Ethics Management Plan

Project deliverable D1.6

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101076963. UK participants in this Horizon Europe Project are supported by UKRI grant number 10139277.

DELIVERABLE ADMINISTRATIVE INFORMATION

DELIVERABLE NUMBER	1.6
DELIVERABLE TITLE	Ethics Management Plan
DELIVERABLE VERSION	Final
WORK PACKAGE NUMBER	1
WORK PACKAGE TITLE	Project Coordination and Management
DUE DATE OF DELIVERY	30/06/2025
ACTUAL DATE OF DELIVERY	27/06/2025
DISSEMINATION LEVEL	PUB
TYPE OF DELIVERABLE	Document, report
EDITOR(S)	Tom Brijs (UH)
CONTRIBUTORS	All Beneficiaries
REVIEWER(S)	Rob Eenink (SWOV), Olivera Rozi (IRAP)
PROJECT NAME	Connected and Adaptive Maintenance for Safer Urban and Secondary Roads
PROJECT ACRONYM	CAMBER

PROJECT STARTING DATE	01/01/2025
PROJECT DURATION	36 months
RIGHTS	**CAMBER** consortium

VERSION HISTORY

Version	Date	Author	Description
0.1	01/05/2025	UH	Draft document created
0.2	14/05/2025	UH	Integration of GDPR checklist results from Beneficiaries
0.3	13/06/2025	UH	Revision based on feedback obtained after internal quality review procedure, with inputs from SWOV and IRAP.
1.0	30/06/2025	EIRA	Final version submitted and copied to the Deliverables folder in the root repository

APPROVED FOR SUBMISSION BY

Name	Organisation	Approval date
Olivera Rozi	EIRA	25/06/2025

LEGAL DISCLAIMER

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101076963. UK participant IRAP is supported by UKRI grant number 10139277. UK participant Agilysis is supported by UKRI grant number 10157029. 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. The information in this document is provided “as is”, and no guarantee or warranty is given that it is fit for any specific purpose. The Camber project Consortium members shall have no liability for

TABLE OF CONTENTS

LIST OF TABLES

PROJECT EXECUTIVE SUMMARY

CAMBER aims to develop and demonstrate improved safety monitoring across urban and secondary rural road networks by using real-time data to inform road maintenance systems and implementing cost-effective, proven interventions.

Performance metrics derived from next-generation data sources will provide road managers with up-to-date information on safety issues, road damage, and maintenance or upgrade needs. Data from telematics, vehicle and smartphone sensors, and road user feedback will inform safety assessment models, identifying necessary measures to ensure safe roads for all users, including minority groups with specific design needs, such as powered two-wheelers (PTW).

CAMBER will address these challenges through research and testing of cost-effective safety interventions and low-impact maintenance techniques, including those tailored for vehicles with advanced driver-assistance systems (ADAS). These approaches will be demonstrated across urban and rural road networks in five European countries (Greece, Portugal, the Netherlands, Croatia and Spain). CAMBER's economically viable solutions and new insights will be shared through established networks to guide European road managers, policymakers, and industry in making informed decisions and investments for safer, more efficient road maintenance.

Social Media:

@camber-project

@CamberProject

For further information please visit camber-project.eu

PROJECT PARTNERS

Organisation	Country	Abb
EVROPSKI INSTITUT ZA OCENJEVANJE CEST - EURORAP	SI	EIRA
STICHTING WETENSCHAPPELIJK ONDERZOEK VERKEERSVEILIGHEID SWOV	NL	SWOV
LABORATORIO NACIONAL DE ENGENHARIA CIVIL	PT	LNEC
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AT	AIT
SVEUCILISTE U ZAGREBU FAKULTET PROMETNIH ZNANOSTI	HR	FPZ
UNIVERSITEIT HASSELT	BE	UH
EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON	EL	ICCS
BE-MOBILE	BE	BMOB
FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	ES	VICOM
EUROPEAN ROAD TRANSPORT TELEMATICS IMPLEMENTATION COORDINATION ORGANISATION - INTELLIGENT TRANSPORT SYSTEMS & SERVICES EUROPE	BE	ERTICO
ANAPTYXIAKI ETAIREIA DIMOU TRIKKAION ANAPTYXIAKI ANONYMI ETAIREIA OTA	EL	ETRIK
MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE	ES	MITMA
INTERNATIONAL ROAD ASSESSMENT PROGRAMME	UK	iRAP
AGILYSIS LIMITED	UK	AGIL

DELIVERABLE EXECUTIVE SUMMARY

Work package 1 sets out the 'ethics requirements' that the project must comply with. The purpose of this Deliverable 1.6 – Ethics Management Plan is to make sure that all legal and ethical issues relevant to the CAMBER Project, as identified by the established Research Ethics Committee (REC), are known, observed and addressed.

Based on a GDPR Checklist and interactions with CAMBER's Beneficiaries, and in alignment with the planned data collection and processing as described in Deliverable 1.5 – Data Management Plan, special attention in the current Deliverable is given to identify and assess which personal data will be collected and processed in the CAMBER project. In addition, an overview of technical and organisational procedures for personal data collection and processing is provided, and responsibilities assigned for each Beneficiary to protect these data. Within the project, a Research Ethics Committee is created that will continuously monitor the ethics requirements during project execution.

It is partners' responsibility to take all the necessary measures to comply with the rules mentioned in this Deliverable and EU/national legislation. Specifically, partners that are active in collecting, harvesting, processing, sharing and retaining personal data confirm that as a company, association, or knowledge institution are compliant with laws and regulations regarding data collection, data protection and data privacy unless otherwise reported following the procedures described. To this end, all partners that will collect or process personal data in their country need to obtain an ethics approval from their respective committees and once it is obtained, submit it to the REC.

LIST OF ABBREVIATIONS AND ACRONYMS

Acronym	Meaning
ASAP	As Soon As Possible
B2B	Business-to-business
B2C	Business-to-Consumer
DMP	Data Management Plan
DoA	Description of Action
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DTA	Data Transfer Agreement
EC	European Commission
EMP	Ethics Management Plan
ERB	Ethics Review Board
GA	Grant Agreement
GDPR	General Data Protection Regulation
KoM	Kick-off Meeting
KPI	Key Performance Indicator
REC	Research Ethics Committee
SC	Steering Committee
WP	Work Package

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Deliverable is **to examine the legal and ethical concerns arising from the project, conducted by the Research Ethics Committee to guarantee adherence to established guidelines and prerequisites.** The deliverable therefore provides a baseline assessment for the CAMBER project on the issues, procedures and tasks related to data privacy, especially with respect personal data.

Personal data means any information with which a natural person can be identified both directly and indirectly (for more info: https://gdpr-info.eu/art-4-gdpr/). Some examples, without being limited to this: name, address, telephone number, e-mail address, IP address, age, gender, origin, image, lifestyle, exam results, location data... In addition to "common" personal data, personal data can also be specific to the physical (f.e. disabilities, medical data (on a vaccination card), psychological, genetic, mental, economic (e.g., financial data), cultural or social identity of a natural person.

Since May 25th, 2018, the privacy legislation of 1992 was replaced by the General Data Protection Regulation (hereinafter GDPR). The GDPR is a set of rules that imposes strict personal data protection on everyone who processes this personal data. More info: https://gdpr-info.eu/ Processing means any operation or set of operations which is performed on personal data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR is built around a number of principles:

- Transparency, including registration of processing (which personal data are processed, why, for how long, legal basis for processing, ...);
- Implementation of privacy measures for the processing of personal data;
- Rights of data subjects

For more info: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

It is the duty of all CAMBER project partners involved in the collection and processing of personal data to respect and comply with the GDPR when dealing with personal data.
More specifically, this Deliverable will deal with the following topics:

- Assignment of a **Data Protection Officer** (hereinafter DPO) for each Beneficiary in the project
- Creation of **a Research Ethics Committee** (REC) for the CAMBER project

- Creation of an **inventory of personal data** collected in the CAMBER project and the **potential vulnerabilities and/or risks involved** in the collection and processing of these personal data
- Creation of **procedures to continuously monitor all data privacy aspects** in the CAMBER project

1.2 DELIVERABLE STRUCTURE

This Deliverable is structured as follows.

Section 2 describes the Ethics structures and processes that are applied in the CAMBER project, including the constitution of a CAMBER Research Ethics Committee, Ethics meetings and procedures, the development of a GDPR checklist, the appointment of Data Protection Officers for all Beneficiaries and how the continuous monitoring and reporting will take place. Section 3 then provides an Ethics assessment of the data collected and processed in CAMBER based on the GDPR checklist that was distributed and filled out by all Beneficiaries in the early stages of the project. Based on the results of this GDPR checklist, an inventory of personal data is made and technical and organisational procedures are reviewed to maintain the highest quality standards for preserving the privacy of staff and volunteers in the CAMBER project. Finally, Section 4 provides the main conclusions of the analysis carried out in this Deliverable.

2 ETHICS PROCESSES

2.1 CONSTITUTION OF A RESEARCH ETHICS COMMITTEE

As a first step in the Ethics management of the project, all Beneficiaries appointed a representative to participate in the Research Ethics Committee (REC). The REC meets at least once per year to revise, approve, and apply the legal and ethical requirements and ensure compliance with the guidelines defined in the Ethics Management Plan (D1.6). The results of these annual meetings will be reported to European Commission (hereafter EC) in periodic reports (e.g. mid-term evaluation, final evaluation). The detailed list of members of the REC with contact details can be requested from the CAMBER coordinator.

2.2 ETHICS KICK-OFF MEETING

After the constitution of the REC, UHASSELT organized an online kick-off meeting (April 1, 2025) with representatives in the REC of each partner in the CAMBER project. During this meeting, all Beneficiaries were invited and important definitions were shared related to data privacy, personal data, data collection and data processing, data controller and data processor. During the meeting, an overview of different data types from the Description of Action (hereafter DoA) were discussed and an essential distinction was made between personal data (e.g. from participants to CAMBER simulator experiments) and non-personal data (e.g. infrastructure attributes, anonymized crash data, traffic volume data, etc.).

Furthermore, it was pointed out that all Beneficiaries receiving data from Third Parties (e.g. non-Beneficiaries such as a local authority) necessary for the execution of their project activities in CAMBER will need to set up a **Data Transfer Agreement** (DTA) or license agreement with this third party to clarify the responsibilities of the different parties in correctly storing and processing the data.

In so far that multiple Beneficiaries are jointly involved in the collection or processing of data, a **Joint Data Processing Agreement** will have to be set up between the Beneficiaries.

In order to ensure that photos of Beneficiaries' staff and of external participants to CAMBER events can be used for public media (e.g. social media, newsletters), **Permission for use and reproduction of photos** should also be obtained and included in procedures by CAMBER event organizers (WP6 leader).

For the CAMBER project website, a **Cookie Policy** and **Privacy Policy** should be made available by the website manager – WP6 leader ''ERTICO'.

Especially when personal data are collected, specific aspects need to be paid attention to:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization

- Accuracy
- Integrity and confidentiality
- Storage limitations
- Accountability

In addition to the **general GDPR regulation**, specific national legislation can be applicable that Beneficiaries will need to verify and comply with in case they collect 'sensitive' personal data (e.g. video recording with cameras, use of dashcams in vehicles, etc). In such case, it is possible that a **Data Protection Impact Assessment** (hereafter DPIA) will have to be initiated.

It was therefore emphasized that all Beneficiaries that are collecting personal data will have to undergo an **Ethics approval procedure** with their institutional/national Ethics Review Board (hereafter ERB), or in the absence of such ERB formally declare compliance with all applicable Ethics regulations, and will have to report their status to the REC. Without the approval by this ERB or compliance report, no personal data collection or processing can be initiated.

In order to carry out an assessment which Beneficiaries will be collecting or processing (personal) data, and whether or not these personal data are of any specific 'sensitive nature', a GDPR checklist was created and filled out by all Beneficiaries.

2.3 GDPR CHECKLIST

The purpose of the CAMBER's GDPR checklist is to make an assessment early in the project of all the planned personal data being collected by the different Beneficiaries in order to evaluate the potential risks and vulnerabilities involved in the collection and processing of these personal data and to follow the necessary legal and ethical procedures.

The GDPR checklist was created by UHASSELT and contains the following main categories of information (the full checklist can be found in Annex 1 of this Deliverable):

- Partner info
- Type of data collected (personal data, or other)
- For personal data:
  - From which persons (inside / outside of Beneficiary's organization)
  - Vulnerable persons involved (types)
  - Categories of personal data (types)
  - Sensitive data involved (types)
  - Legal grounds for personal data collection
  - Information provision
  - Data processing :
    - Data controller / data processor
    - Transfer of data
  - Technical and organizational measures
    - Data storage

    - Data exchange
    - Data access
    - Data retention period
    - Data archiving / deletion
    - Data anonymization / pseudonymization
- Organizational and technical measures
    - Security policy
    - Identity and access management
    - Data classification and encryption
    - Availability control
- Data subject derogations
- DPIA

Answers to the GDPR checklist were entered by all Beneficiaries by April 25 and were processed to identify any issues that need specific attention in the short or longer term. The results of this analysis can be found in Section 3.3.

2.4 LIST OF DATA PROTECTION OFFICERS

Each Beneficiary has appointed a Data Protection Officer (DPO) who is the main organization's contact person for legal and ethical matters with respect to the treatment of (personal) data in the CAMBER project. The DPO is an expert on data protection law and practices and in the position to operate independently within the organization. The primary role of the data protection officer (DPO) is to ensure that her organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. Those Beneficiaries collecting personal data in the CAMBER project will inform the data subjects (e.g. study participants) of the existence of this role and will provide the necessary contact details in case data subjects wish to be informed about specific matters related to their privacy. The detailed list of DPOs with contact details can be requested from the CAMBER coordinator.

2.5 CONTINUOUS MONITORING AND REPORTING

Throughout the project, the REC will meet at least once per year during Project Steering Meetings, or ad hoc whenever necessary to discuss any issues on data privacy that require urgent attention. In any case, the progress towards securing the approval by the Beneficiarie's ERB or formal declaration of compliance with ethics regulations will be the subject of continuous monitoring of the project's Ethics procedures. Members of the REC can contact the chairperson of the REC (Tom Brijs – UHASSELT) for advice on any issues related to data privacy. No collection or processing of personal data can take place in CAMBER without this approval or declaration of compliance with the ethics regulations.

The REC will report to the CAMBER Steering Committee (SC) on a regular basis during SC meetings and during periodic reporting events (e.g., mid-term reporting, final reporting).

3 ETHICS ASSESSMENT

3.1 BENEFICIARIES

In CAMBER the largest part of the data that will be processed or collected concerns non-personal data. More specifically, it concerns the following categories of **non-personal data**:

- Road infrastructure data, such as geometric and physical attributes of the road
- Road asset condition data (e.g., road surface condition, rutting, skid resistance)
- Road safety levels (e.g., road safety star rating)
- Speed and vehicle flow data
- Road maintenance and road safety procedures (documents)
- Road maintenance and safety interventions (e.g., attributes of innovative markings and signs)
- Costs figures of road maintenance and safety interventions
- Georeferenced anonymized crash data (i.e., publicly available road safety data)
- Anonymized vehicle sensor data (e.g., vehicle speed, ADAS activation data, g-force data)
- Probe vehicle data (e.g. g-force data)
- Weather data
- Open Source GIS map data (terrain features, road hierarchy)
- Interferometric Synthetic Aperture Radar data (InSAR) (i.e. radar measurements)
- Surrogate safety indicator data

For **personal data**, the following categories of data have been determined:

- Driving simulator data (e.g., speed, lane position, acceleration, etc.)
- Eye tracking data (e.g., gaze position, gaze duration)
- Survey data (e.g., gender, age, education level, risk attitudes, driver behaviour records)
- Driver telematics data (e.g., vehicle location, speed, acceleration, deceleration)
- Vehicle camera imagery (e.g. faces, license plates of persons not participating in the study)
- Floating car data (e.g., vehicle location, speed, acceleration, deceleration)
- Event participant data (e.g., name, contact details of participants in CAMBER project events)

The general policy in CAMBER for personal data is that volunteers to CAMBER data collection activities will be duly informed about their rights and obligations according to the GDPR and that volunteers will be asked to provide **informed consent** before any personal data is collected. For CAMBER project events, a specific procedure (based on informed consent) will be followed as described in Section 3.3. For some categories of personal data, it is impossible to obtain informed consent since there is no technical or administrative possibility to inform them or obtain consent. This is the case for vehicle camera imagery data where persons in the public space will be filmed without them knowing. In this case, the following measures will be taken to try and inform them to the greatest possible extent, as well as to preserve their privacy. First, an **information notice** will be put up at the location of filming

with a link (QR code) to additional details for random passers-by about the CAMBER project, such as: the purpose of data collection, the type of data collected and how the data is anonymized before further processing by any of the CAMBER partners, contact details of the CAMBER representative responsible for data collection. Second, any imagery data collected that holds potential identification of individuals (e.g. by means of their vehicle's license plate, or people's faces) will be **blurred before analysis**.

It must be highlighted that as part of the CAMBER project additional data can be collected or acquired in a later stage when needed to reach the project goals. It cannot be determined at this point of completing the current Deliverable what the potential data privacy implications are with respect to data that are currently unknown. However, if this happens, Beneficiaries planning to acquire additional data will have to report this to the REC which will then evaluate any potential data privacy issues and to make sure that the correct Ethics procedures are followed. The REC will include the topic of additional data on its yearly REC meeting.

3.2 NON-EU BENEFICIARIES

For the non-EU Beneficiaries in the CAMBER, specific data privacy aspects could be applicable since data privacy regulations might be different in their countries when compared to the EU-wide GDPR. In order to avoid problems with data privacy, as a general rule adopted in the CAMBER project, all data exchanged with these partners (in both directions) will be anonymised prior to data exchange. More specifically it concerns the following data types:

- For iRAP:
    - Anonymised road images, speed data, vehicle counts, etc., for road safety assessment. Includes uploading the coded data into iRAP's processing system to produce risk ratings.
    - Reviewing similar coded data (historically) produced by road authorities in Europe and newly coded data produced by data suppliers to verify accuracy.
- For Agilysis:
    - Agilysis will procure dynamic data from the suppliers directly.
    - Agilysis will also be receiving some data from road authorities and the other Beneficiaries collecting data for the purposes of creating digital twin maps.

3.3 RESULTS FROM GDPR CHECKLIST

In this section, more details will be provided with respect to the personal data being collected and which measures are taken to preserve the privacy of individuals taking part in CAMBER. The following sections describe the results from the GDPR checklist as provided by the different CAMBER Beneficiaries. Before any actual data collection or processing of personal data takes place, relevant Beneficiaries collecting or processing personal data will submit an Ethics assessment and will obtain approval from their local Ethics Review Board or will formally declare compliance with all applicable Ethics regulations (see Section 2.5).

3.3.1 OVERVIEW OF PERSONAL DATA

Based on the results from the GDPR Checklist, it can be concluded that the following Beneficiaries will be collecting personal data (see Table 1 — personal data processed).

TABLE 1 — PERSONAL DATA PROCESSED

Organization	Personal data processed
SWOV	Surveys and (possibly) driving simulator data
UHASSELT	driving simulator data, survey data, eye tracking data, physical well-being
FPZ	vehicle/smartphone telematics data, roadside camera image data, survey data
ALL PARTNERS	Contact information from participants in CAMBER project events (both online and offline)

3.3.2 PERSONAL DATA FROM VULNERABLE PERSONS

None of the Beneficiaries will be collecting personal data from vulnerable persons, which would require specific Ethics procedures to be followed.

3.3.3 CATEGORIES OF PERSONAL DATA

The following categories of personal data will be processed by the Beneficiaries (see Table 2 — Categories of personal data).

TABLE 2 — CATEGORIES OF PERSONAL DATA

Category	Description
Identification details	e-ID, name, username, e-mail, date of birth, IP address, Phone number, LinkedIn profile
Socio-demographic data	Age, gender, driving experience
Location data	home address, GPS locations (from floating car data)
Media data	video, audio, social media

Driver behaviour data (either telematics or simulator-based)	Speed, acceleration, deceleration, overtaking, lane positioning
Driver attitude data	self-reported risk behaviour & past accident involvement, risk perceptions, safety attitudes, qualitative intervention evaluations
Eye tracking data	Gaze location, gaze duration, gaze frequency, saccades
Physical well-being data	Pre-post questionnaire data about driver simulator sickness, cognitive effort (i.e. simulator difficulty level)

3.3.4 PURPOSE AND LEGAL GROUNDS FOR DATA PROCESSING

Beneficiaries have indicated for which purpose the personal data will be collected and on which legal grounds the collection and/or processing of personal data will be based (see Table 3 — Purpose and Legal ground).

TABLE 3 — PURPOSE AND LEGAL GROUND

Category	Purpose	Legal ground(s)
Identification details	To contact CAMBER volunteers, to register participants to CAMBER events, for project dissemination purposes	Informed consent
Socio-demographic data	To carry out sub-group analyses	Informed consent
Location data	To link the location of driver behaviour, vehicle and/or smartphone sensor data to relevant road attributes for identification of maintenance and/or safety issues	Informed consent
Media data	Roadside images collected from video or photographic data: to extract relevant information for road maintenance and road safety research. Event pictures : for CAMBER project dissemination activities (e.g. newsletter, social media)	Informed consent and/or processing needed to fulfill a task of general interest (i.e., road maintenance and road safety research). Only relevant images will be collected needed for the purpose of the research. Other data will be anonymized/blurred.

Driver behaviour data (either telematics or simulator-based)	To evaluate the effectiveness of proposed CAMBER interventions	Informed consent
Driver attitude data	To obtain deeper understanding about the heterogeneity in effectiveness results of CAMBER interventions	Informed consent
Eye tracking data	To obtain deeper understanding about the heterogeneity in effectiveness results of CAMBER interventions	Informed consent
Physical well-being data	To exclude participants from driving simulator analysis in case of simulator sickness	Informed consent

3.3.5 TECHNICAL PROCEDURES FOR PROCESSING OF PERSONAL DATA

All necessary measures will be undertaken by the Beneficiaries in CAMBER to protect personal data from their staff and volunteers taking part in CAMBER data collection. These procedures can be described as follows:

- **Data pseudonymization / anonymization**: all personal data will be pseudonymized during the project duration, and anonymized after project closure. For video data where identifiable personal data are collected unintentionally (e.g., vehicle license plates, faces), the technique of blurring will be adopted to preserve data privacy
- **Data storage and transmission**: data will be stored on secured personal computers/laptops, European-based secured cloud storage, and will be transmitted between Beneficiary staff members using either encrypted USB sticks or encrypted online transmission.
- **Data storage period**: data will be stored no longer than strictly needed for the execution and reporting duties of the project, i.e. no longer than 5 years after project closure (except for UK: 6 years). After this period, any personal data will be deleted or permanently anonymized and archived.
- **Data encryption**: all personal data will be stored using encryption to avoid unintended access to sensitive data
- **Data access**: for each Beneficiary, a list of staff members will be held that have access to the personal data. Data access will be limited to those staff members only that require access to the data for the execution of their project duties.
- **Data security**: all Beneficiaries processing personal data have the necessary data security policies in place (e.g., user authentication, role-based authorization, data access logging and reporting, secured data connection, physical access control, data backup systems, data

recovery plans, antivirus protection, regular software updating procedures, password policies) and have procedures in place to report any data breaches. Within CAMBER a special form was prepared to report any data leakage (see CAMBER Data Leakage Reporting Form.docx)

- **Data supervision**: in each Beneficiary, a person is appointed to deal with the technical procedures of data storage, anonymization and data deletion.

3.4 PERMISSION OF USE AND REPRODUCTION OF PHOTOS

In order to preserve the privacy of individuals, whether they are staff members of CAMBER Beneficiaries, or external participants to CAMBER project events, explicit permission will be asked to use their photos and/or video for reproduction in communication materials of the project.

3.4.1 FOR CAMBER STAFF

For CAMBER project staff members, written consent will be requested to use their photographic materials for purposes of dissemination.

A template (CAMBER_GDPR_ConsentFormConsortium_FINAL.docx) was created to be signed by all CAMBER project staff members in order to enable reproduction of materials.

Permission for use and reproduction of photos

Dear,

CAMBER project wishes to use your photo to communicate about and to visualize project events in its external communication via different channels such as website, social media (Youtube, LinkedIn) and newsletters, organized within the scope of the project. The project started on January 1st, 2025 and will finalize on December 31st 2027. The projects' website, social media channels and newsletters will be online up to 5 years after the project end date.

CAMBER respects the portrait rights and the right to protection of everyone's personal data in accordance with the General Data Protection Regulation (GDPR) and therefore takes the necessary measures for this through this statement.

By signing this statement you therefore agree to the following:

- I hereby give the CAMBER Beneficiaries my explicit and unambiguous permission to take my photo for the aforementioned purposes and always within the framework of the activities organized within the scope of CAMBER.
- I hereby give the CAMBER Beneficiaries my explicit and unambiguous permission to use, publish, multiply and distribute my photo as described above and always within the framework of the activities organized within the scope of CAMBER.
- I do not request compensation for the use of my photo and I agree that these photos can be transferred to third parties, if a CAMBER Beneficiary considers it appropriate and in accordance with the project activities.

I am aware that I can withdraw or change my permission to use these photos at any time without giving a reason. Furthermore, I am aware that I can always ask for more information about the use of the photos or to exercise my right of access, improvement, resistance or transferability. In any of these cases I will contact the CAMBER partner responsible for dissemination (ERTICO) via m.mendez@mail.ertico.com.

The photos are not stored any longer than necessary for the realization of the purposes. As soon as the aforementioned purpose is no longer active or there are new images, the least recent photos will be deleted.

I have read and understood the above information and have received answers to all my questions. I have also received a copy of this document.

Full name:

Affiliation:

Signature:

Date:

Contact details CAMBER partner responsible for dissemination:
EUROPEAN ROAD TRANSPORT TELEMATICS IMPLEMENTATION COORDINATION ORGANISATION - INTELLIGENT TRANSPORT SYSTEMS & SERVICES EUROPE (ERTICO), AVENUE LOUISE 523, BRUXELLES 1050, Belgium,
email: m.mendez@mail.ertico.com, website: https://camber-project.eu/

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 10139277.

3.4.2 FOR EXTERNAL VISITORS

For CAMBER project events where external visitors participate, the following stepwise procedure will be adopted to maintain compliance with the GDPR.

1. Make sure that visitors register for the event beforehand via an online registration form. Include the following box in the form:

> ❑ I hereby give the CAMBER consortium my explicit permission to make photographs and/or videos during this event on which can be depicted. The use of these photographs and/or videos for publicity on the CAMBER website and the CAMBER social media channels (Youtube, LinkedIn).
> ❑ I do not want to have photos and/or videos taken of me
> ❑ Not decided yet
>
> For more information, please check the CAMBER privacy policy.

2. Use the participant list WITH the GDPR notice to mark attendances at the registration desk (see doc on the Teams drive: CAMBER_GDPR_ParticipantList.docx)

3. Foresee a physical GDPR notice (e.g. mini roll-up banner, poster…) at the registration desk of the event and place it next to the registration list. This banner should contain the following info:

> CAMBER wants to inform you that photographs and/or videos can be taken during this event. The use of this material might include (but is not limited to) the use in our printed media, our website and social media, marketing brochures and press releases.
> Do you prefer not to appear in any pictures or videos, then please inform the photographer/cameraman, ask for a sticker at the registration desk and stick it on your name badge. Or you can of course always contact us in writing via camber-privacy@irap.org for any questions or requests.
> More information on how we process data in accordance with GDPR, can be found in our privacy policy on the CAMBER website.

4. Foresee stickers to mark namebadges of people that don't want to appear on photo's/videos. (you can use the camera png icon included on the Teams drive: Camera off)

4 CONCLUSIONS

The largest part of the data collected and processed in the CAMBER project concerns non-personal data (e.g. road maintenance and safety data, road risk data, weather data, anonymized road accident data, etc). To a limited extent, however, personal data will be collected by some Beneficiaries to fulfil the required objectives of the project. These data mainly pertain to driving simulator data, eye tracking data, vehicle telematics data, roaside video data and survey data in order to collect relevant roadside attributes and to evaluate the (simulated) effectiviness of innovative road maintenance and safety interventions. In addition, based on a GDRP checklist created for this project and filled out by all Beneficiaries, an assessment was carried out to evaluate the sensitivity of these personal data and the risk of loss of privacy, as well as procedures and techniques put in place to reduce this risk. As a general principle, informed consent by the subject under investigation will be asked, and in those cases where this is impossible due to the nature of data collection (e.g., roadside observations), all state-of-the-art techniques of information provision and anonymization will be applied (e.g. blurring of video data).

A CAMBER Research Ethics Committee was created to permanently monitor the application of all necessary Ethics procedures (e.g. Ethics approval) in the project and to deal with any new or unplanned Ethics challenges during the execution of the project.

ANNEX 1: GDPR CHECKLIST

GDPR checklist

Scope
Since May 25th, 2018, the privacy legislation of 1992 was replaced by the General Data Protection Regulation (hereinafter GDPR). The GDPR is a set of rules that imposes strict personal data protection on everyone who processes this personal data. More info: https://gdpr-info.eu/

The GDPR is built around a number of principles:
• Transparency, including registration of processing (which personal data are processed, why, for how long, legal basis for processing, ...);
• Implementation of privacy measures for the processing of personal data;
• Rights of data subjects

For more info: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

It is the duty of all CAMBER project partners involved in the collection and processing of personal data to respect and comply with the GDPR when dealing with personal data.

What are personal data?
Personal data means any information with which a natural person can be identified both directly and indirectly (for more info: https://gdpr-info.eu/art-4-gdpr/).

Some examples, without being limited to this: name, address, telephone number, e-mail address, IP address, age, gender, origin, image, lifestyle, exam results, location data...

In addition to "common" personal data, personal data can also be specific to the physical (f.e. disabilities, medical data (on a vaccination card), psychological, genetic, mental, economic (e.g., financial data), cultural or social identity of a natural person.

Definition Processing Processing means any operation or set of operations which is performed on personal data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Compliance to GDPR
The purpose of this questionnaire is to collect the mandatory information:
• to maintain the registry of processes concerning personal data
• to decide whether a "data processing agreement" needs to be added to a basic agreement in a research project.

Project Implementation

1. Name of the project owner in your organization *

2. Who determines the objectives of the research/project? (select one option) *

- ◯ Your organization
- ◯ Your organization together with someone else outside your organization (e.g. other CAMBER project partners).
- ◯ You perform it on behalf of someone outside your organization

3. Are personal data processed within the project? *

Personal data means any information with which a natural person can be identified both directly and indirectly.

- ◯ Yes
- ◯ No

Personal data

If you indicated 'YES' on the previous question: whose personal data are you investigating / processing? Please specify

4. External/outside your organization (e.g., participants to project events, participants to research project, customers, suppliers, entrepreneurs, citizens, prospects...)

5. Internal/within your organization (e.g., staff, guests, applicants, alumni...)

6. Vulnerable persons (e.g., children under 16 years, people with mental disorders, elderly, ethnic minorities, asylum seekers, people with disabilities, pregnant women, the sick and patients...)

7. Categories of personal data

General personal data (multiple answers allowed):

- [ ] Identification details (e-ID, name, username, date of birth, IP address, Phone number..)
- [ ] Location data (Address, GPS locations...)
- [ ] Family situation (Children,...)
- [ ] Lifestyle (Hobby,...)
- [ ] Education (qualifications, CV, ...)
- [ ] Career (work related circumstances,...)
- [ ] Financial data
- [ ] Media (video, audio, social media...)
- [ ] Andere

8. Sensitive personal data

Personal data relating to the following characteristics of the individual: Details of racial or ethnic origin; Political opinions, religious or philosophical beliefs; Trade union affiliation / health details; Information about a person's sex life or sexual orientation; information concerning criminal convictions or offences (multiple answers allowed):

- [ ] Psychosocial and/or medical data
- [ ] Details of racial or ethnic origin
- [ ] Data regarding risk situations and risk behaviour
- [ ] Andere

9. Personal data in detail

List all the data you process about a person.

An important principle in GDPR is data minimization. Data processing should only use as much data as is required to accomplish a given task.

List all the data you process about a person:

Legal grounds

A processing of personal data can only take place based on one of the following legal grounds!
(If your research concerns secondary processing of personal data, you should check with the person who collected the data primarily on what legal basis this was done.)

10. Legal ground (multiple answers possible when multiple data types are applicable)

- [ ] Processing is necessary for the fulfilment of a task of general interest (e.g. speed camera enforcement requires processing of the driver's license plate)
- [ ] Consent of the data subject (e.g., data subject signs an informed consent form and agrees to share his personal data)
- [ ] The processing is necessary for the execution of a contract or agreement (e.g., use of a smartphone navigation app requires user's position data)
- [ ] Legal obligation (e.g. obligatory reporting to tax authorities, etc...)
- [ ] The processing is necessary to protect the vital interests of the data subject or another person (e.g., if there is an imminent danger, but someone is unconscious or mentally incapable of giving consent)
- [ ] The processing is necessary for the representation of a legitimate interest (e.g. fraud prevention,...)

Are the persons concerned been informed of the processing of their personal data?

11. Is or will the necessary information be(en) provided to these persons?

- ◯ Yes
- ◯ No

12. If you have answered no, why not?

Data processing

13. Data controller/data processor

How are the personal data processed? (multiple answers possible when multiple data types are applicable)

- [ ] Your organization takes care of everything relating to the processing of personal data.
- [ ] Your organization receives personal data from a third party and processes it further.
- [ ] Your organization receives personal data from a third party, processes it and shares it with other parties.
- [ ] Your organization processes personal data together with other partners
- [ ] Your organization processes the personal data on location (the personal data are processed outside your organization, if necessary, VPN will be used).

14. Are the collected and/or processed data transferred to other partners?

The "white list", a list of countries can be consulted at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions

- ◯ EU
- ◯ Outside EU, EU-whitelisted country
- ◯ Outside EU, non EU-whitelisted country
- ◯ Andere

15. Specify which partners are involved:

Technical and organizational measures

16. Data storage

    Where will the data be stored? (Laptop/PC, Google/Teams personal or shared drive or any other cloud provider, ...)

17. Define how data will be exchanged (e-mail, download website, webservices, usb-stick, ...)

18. Who has access to the data during processing of the project?

    For example, in addition to the researcher, the following persons also have access: the supervisor and co-supervisor, the entire research group, members of a partner institution, etc....

19. Who has access to the data after closure of the project?

20. How long is the data being kept (retention period)?

    The GDPR provides archiving for the purpose of general interest. This means, however, that the data may no longer be kept in active files and that the access possibilities must be limited. (Usual answer is: 5 years, unless it can be motivated why a longer period is needed)

21. Who will eventually archive and/or delete the data?

22. Data masking

Is the data anonymized? (Anonymization of personal data is the process of encrypting or removing personally identifiable data from data sets so that the person can no longer be identified directly or indirectly. When a person cannot be re-identified the data is no longer considered personal data and the GDPR does not apply for further use)

- ◯ Yes
- ◯ No

23. If yes, please specify the anonymization method and the persons involved in this process (e.g. data masking, data randomisation, data generalisation):

24. Is the data being pseudonymized or coded? (Pseudonymisation' of data (defined in Article 4(5) GDPR) means replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified.)

- ◯ Yes
- ◯ No

25. If yes, note the coding method, the persons involved and who has access to the coding key:

Organizational and technical measures

Which security measures are taken by your organization to secure the data?

26. For the security Policy

	Yes	No
Does your organization have a security consultant/ responsible	○	○
Does your organization have an information security policy	○	○
Does your organization have a continuity plan	○	○
Does your organization have a notification procedure in case of physical/ technical incidents	○	○
Does your organization raise staff GDPR awareness through information and training of incidents	○	○

27. For identity and access management (incl. cloud services)

Which of the following methods are adopted in your organization:

	Yes	No
Authentication (e.g. username, password)	◯	◯
Strong authentication (e.g. e-ID)	◯	◯
Authorization system (role-based access control)	◯	◯
Logging system	◯	◯
Access restrictions for certain IP address ranges	◯	◯
External access only via secure connections	◯	◯
Physical access control to the datacenter	◯	◯
Physical access control to the office	◯	◯

28. Data classification and encryption

Which of the following methods are adopted in your organization:

	Yes	No
Report providing that the technical measures' effectiveness is regularly tested/evaluated and assessed	◯	◯
Information/data classification	◯	◯
Encryption (data at rest)	◯	◯
Encryption (data in transit)	◯	◯

29. Availability control

Which of the following methods are adopted in your organization:

	Yes	No
Regular check of the processing systems and services adequacy	○	○
Recovery plan in case of physical/ technical incidents	○	○
Back-ups	○	○
Anti-virus	○	○
Regular software updates	○	○
Password policy	○	○

30. Remarks

If you've answered NO or not answered a question, please specify reasons or other arrangements at your registry

Data subject rights derogations

31. Is your research seriously impeded if the persons concerned wish to exercise their rights of access, rectification, restriction of processing and right of objection?

- ◯ Yes
- ◯ No

32. If so, please justify the need to derogate from one or more of the above rights:

Data Protection Impact Assessment (DPIA)

When your organization collects, stores, or uses personal data, the individuals whose data you are processing are exposed to risks. These risks range from personal data being stolen or inadvertently released and used by criminals to impersonate the individual, to worry being caused to individuals that their data will be used by your organization for unknown purposes. A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. The questions below help to determine if such DPIA will be necessary or not.

33. What is the expected number of persons whose personal data will be collected?

34. Large scale

    Specify the volume of data and/or the range of different data items being processed as well as the geographical extent of the processing activity. (for example: data processing by a hospital, tracking individuals using a city's public transport system as well as the processing of customer data by banks, insurance companies and phone and internet service providers.)

35. The processing of personal data is likely to involve a high risk of privacy for the data subject.

    E.g. - If personal aspects, based on automated processing including profiling, are systematically and comprehensively evaluated and decisions affecting people are based on them; - sensitive personal data are processed on a large scale - On a large scale, people are followed up systematically in a publicly accessible area (e.g. with camera surveillance)

    - ◯ Yes
    - ◯ No
    - ◯ Andere

36. Motivate why the described processes are necessary to achieve the research objectives.

    Explain that you follow the principle of minimum data processing: the data you process are limited to what is really necessary for the purposes for which they are processed.

37. What are the privacy risks of those involved into the project/process?

    To what extent is there a risk of unlawful access to the data, unwanted modification of the data and loss of data?

38. Motivate why the technical and organizational measures you have taken are sufficient to limit the risks.