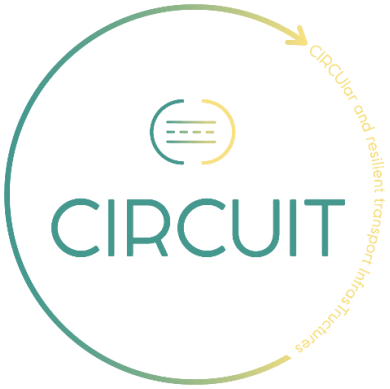
- CIRCUIT -

Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices



– Deliverable 7.2–

Project Quality Assurance, Ethics Manual and Risk Assessment Plan

Project details	
Project reference no.	101104283
Project Acronym	CIRCUIT
Project Fyll title	Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices
Call ID **Topic**	HORIZON-CL5-2022-D6-02 HORIZON-CL5-2022-D6-02-06
Duration	48 Months
Coordinator	Thierry Goger (FEHRL)

	Participant Legal Name	Country
1	FORUM DES LABORATOIRES NATIONAUX EUROPEENS DE RECHERCHE ROUTIERE FEHRLAISBL – FEHRL	Belgium
2	INFRA PLAN KONZALTNIG JDOO ZA USLUGE - INFRA PLAN	Croatia
3	INGEO BV – INGEO BV	The Netherlands
4	ANAS SPA – ANAS	Italy
5	ZAVOD ZA GRADBENISTVO SLOVENIJE – ZAG	Slovenia
6	EUROPEAN UNION ROAD FEDERATION – ERF	Belgium
7	ACCIONA CONSTRUCCION SA – ACCIONA	Spain
8	INSTITUTO ESPAÑOL DEL CEMENTO Y SUS APLICACIONES – IECA	Spain
9	BETON - LUCKO DOO ZA GRADITELJSTVO PROIZVODNJU TRANSPORT I TRGOVINU– BL	Croatia
10	Obcina Crna na Koroskem – CRNA	Slovenia
11	RIGHT-CLICK – RC	Spain
12	UNIVERSIDAD DE CANTABRIA – UC	Spain
13	DIGITALTWIN TECHNOLOGY GMBH – DTT	Germany
14	SVEUCILISTE U ZAGREBU GRADEVINSKI FAKULTET – UNIZAG GF	Croatia
15	Ministerio de Transportes, Movilidad y Agenda Urbana – MITMA	Spain
16	INGEVITY HOLDINGS SRL – NGVT	Belgium
17	ALGORAB – ALGORAB	Italy
18	Hrvatske autoceste d.o.o. – HAC	Croatia
19	Waterschap Hollandse Delta – WSHD	The Netherlands
20	Uberbinder Limited – Uberbinder	United Kingdom

Document Details	
Title	Project Quality Assurance, Ethics Manual and Risk Assessment Plan
Work Package	WP7 - Coordination, Management & Ethics
Date of the Document	21/09/2023
Version of the document	V1.0
Responsible partner	FEHRL – Adewole Adesiyun
Contributing Partner	N/A
Reviewing Partner	N/A
Status of the document	Final
Dissemination level	PUBLIC

Document History			
Version	**Date**	**Comments**	**Author**
01	30-08-2023	Draft 1	Adewole Adesiyun (FEHRL)
1	21-09-2023	Final version	Adewole Adesiyun (FEHRL)

Authors list		
Adewole Adesiyun	FEHRL	adewole.adesiyun@fehrl.org

Disclaimer:
CIRCUIT has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101104283.
This document reflects only the authors' views. The European Commission and CINEA are not responsible for any use that may be made of the information contained therein.

EXECUTIVE SUMMARY

The deliverable D7.2 (Project Quality Assurance, Ethics Manual and Risk Assessment Plan) is prepared in the context of Task 7.2 (Scientific-Technical Coordination, quality & risk management) and Task 7.4 (Ethics). It consists of three key parts, namely the Quality Assurance Plan of the project, the Risk Assessment Plan of the project as well as the Ethics Manual of the project.

The document comprises of the roles, mechanisms and tools to support all the three key core parts. The scope of all of them is to ensure that all project outcomes will be of high quality, having undergone a risk assessment and will be ethics and GDPR compliant. All three aspects are cross-cutting to the upcoming project activities.

TABLE OF CONTENTS

TABLE OF TABLES

1 INTRODUCTION

1.1 PURPOSE AND STRUCTURE OF THE DOCUMENT

The purpose of this Deliverable is to report the establishment of the project Quality Handbook, Risk Assessment Plan and GDPR compliant Ethics Manual. All of them aim to serve as a point of reference for all upcoming CIRCUIT project activities. The aim is to meet the sum of the contractual obligations of the Grant Agreement (GA) in a consistent and effective manner.

In addition to this deliverable, the project is also guided by important reference documents, which define the contractual objectives, the work plan, and the operational procedures of the CIRCUIT project. These documents are as follows:

- The CIRCUIT Grant Agreement (GA) including its Annex I (Description of Action), Annex II (Estimated budget for the action), Annex 3 (Accession Forms), Annex 4 (Model for the financial statements), Annex 5 Specific rules.
- The Consortium Agreement (CA) as signed by all beneficiaries.

This Deliverable encompasses the following structure:

Chapter 1 introduces the overall purpose of the document, the intended audience, and interrelations with other activities of the project.

Chapter 2 presents the quality assurance plan with the establishment of the processes and tools that aim to ensure the efficient monitoring and fulfillment of the contractual commitment of the project and in alignment with the project GA and CA.

Chapter 3 presents the risk assessment plan of the project.

Chapter 4 provides all the principles and mechanisms that constitute the Ethics Manual of the project and the tools that will allow for the project implementation according to it. This Chapter describes the Ethical Code of Conduct for all actions and activities within the project, including gender monitoring and a summary of the ethics controlling process (or ethics compliance monitoring) of the project. The data protection principles and initial policy of the project are included, encapsulating the transparency and accountability principles and demonstrating compliance with the data protection legislation in the EU. The Ethics Board of the project has been established (Annex 7).

Conclusions summaries the next steps and reporting places of the herein described activities follow-up, whilst Annexes of this Deliverable provide the key example reporting templates of the project – available also as standalone documents, the peer review plan of the project with roles allocation per Deliverable, as well as the ethics and GDPR related templates of the project, including the informed consent forms.

1.2 INTERRELATIONS

The current Deliverable is related to the whole project workplan, as the activities described herein refer to horizontal implementation principles and mechanisms (along with the governance described in D7.1: Project inception report [1]).

2 PROJECT QUALITY ASSURANCE

Quality Assurance (QA) is an integral part of project management as a process of verifying quality standards through inspection, to ensure that the outcomes of the project will meet specific standards and quality requirements. This process includes the definition of quality standards for the deliverables along with quality assurance guidelines to secure compliance. The quality assurance policy and measures are introduced through processes based on "project self-assessment/ self-evaluation" before the deliverables are disposed to the European Commission. Measures are planned and coordinated by the Quality Managers of the project (Irina Stipanovic (INFRAPLAN) and Carlos Martin-Portugues Montoliu (ACCIONA)) and supervised throughout all the project activities to make sure that contractual requirements are met, effective quality planning is evident, and the quality system is appropriate. The quality assurance plan of CIRCUIT consists of:

- The guidelines that should be followed by the consortium partners throughout development/conduct, documenting and reporting activities.
- The required measures need to be taken when low quality is detected; and
- The distributed responsibilities of each partner along this process.

The current plan reflects the overall quality policy of the Consortium that is in accordance with ISO 9001:2015 principles, to pursuit continuous improvement, include accountability as well as transparency issues. It is also based on past best practices applied in other and comparable European projects, such as AUGMENTED CCAM Innovation Action [2].

For further details on the governance bodies that are mentioned in the current Deliverable, please refer to D7.1: "Project inception report".

2.1 QUALITY SYSTEM REVIEW

The present Quality System is to be reviewed, if applicable, within the project General Assembly meetings. In any occurring subsequent reviews, the following will be considered:

- the results from project audits.
- the results from internal audits.
- the official project Deliverables (reports and prototypes).
- the corrective action requests.
- the preventive actions taken/proposed.
- any project prototype/solution deficiencies and subsystems/parts problems.
- project participants staff training and adequacy for the tasks undertaken.
- level of used resources per category and adequacy of spent resources for the task.

The outcomes and derived conclusion on the above shall be discussed at the project General Assembly meetings, to assess:

- Satisfaction with the audits, corrective actions and the results of complaints.
- Dissatisfaction and requirements for further auditing or additional corrective actions.
- Satisfaction with the corrective actions taken by the relevant partner(s).

In the agenda of such occurring meetings the following topics should be included:

1. Results of Internal Audits.
2. Corrective actions requests received.
3. Defects in prototypes / demonstrators/ software.
4. Complaints.
5. Results of external audits.
6. Preventive actions.
7. Review of quality policy and objectives.
8. Introduction of new quality plans.
9. Risk assessment plan review (see section **Error! Reference source not found.**).

2.2 DELIVERABLES PREPARATION GUIDELINES

All project results are materialized through 31 Deliverables to be submitted to the European Commission (EC) during the project lifespan.
As such, the core aim of the QA procedure is to assess the quality and content of each deliverable planned, which must be submitted under contractual obligations to the EC. Each deliverable has one project beneficiary appointed as the lead author to ensure that:

- Content is consistent with the objectives and descriptions reflected in the GA and being already further elaborated in the project Inception Report (D7.1).
- Quality of presentation (style, typing errors, presentation, etc.) and content (i.e. quality of writing) is of a high standard and according to the principles defined in the current Chapter.
- There are no missing parts, references and content is readable and comprehensible by the readers.

To ensure optimal, smooth and timely delivery but also consistent presentation of each Deliverable, this Chapter defines the structure, the layout of project report Deliverables as well as the procedure to be used for their development. The full list of Deliverables in this project is presented in DoA (Part A) of GA but also in Annex 2 along with the Peer Review plan defined as an inherent part of the Quality Assurance.

2.3 DELIVERABLES TYPE AND CONFIDENTIALITY

All deliverables of the project are classified in the GA and the participant portal as "R — Document, report" apart from D2.1 (Digital Platform) classified as "DEM - DEMONSTRATION" and deliverables linked to the Data Management Plan i.e., D7.3, D7.4, D7.5 and D7.6, classified as "DMP - Data Management Plan". Nevertheless, these deliverables will also be submitted as reports. Each document deliverable will be written in Microsoft Word and the final submitted version for the participant portal will be converted into a .pdf format. There are two confidentiality levels anticipated in CIRCUIT, to be clearly stated on the front page of each Deliverable (as it is the case for the current Deliverable). The PUBLIC (PU) level implies that the document is fully open and may be read by everyone interested, while SENSITIVE (SEN) restricts the content for members of the consortium and the European Commission Services.

2.4 FILE NAMING CONVENTION

The file naming in the CIRCUIT project will follow the convention below.

"CIRCUIT_Document Type - ID_short name_versioning ID_Status.extension"

Table 1: Deliverable file naming convention

Element	Naming convention	Case
CIRCUIT	Standard initiating element	Upper
Document Type & ID	"D" for deliverable, together with its ID number (e.g. D6.1), as defined in the G.A. • "Periodic report" for interim reports to the European Commission together with the identification of the period it refers to (i.e. M0-M18). • ""ID & Type of meeting" Agenda" for meeting agendas. • ""ID & Type of meeting" Minutes" for meeting minutes. • "Task_IR" for the internal reports. • "PR" for the peer review report of Deliverable.	Upper
Short name	Short name of the deliverable/meeting/report	Lower
Versioning ID	According to versioning given in templates (see Annex 1)	Lower
Status	One of {DRAFT, FINAL, SUBMITTED, APPROVED}	Lower

The objective of the naming convention is to simplify and to make the identification of a document produced in the project self-explanatory and allow an automatic versioning system. This naming convention is applicable to the official documents defined in the Grant Agreement and in the DoA (Deliverables, Periodic and Final reports to the European Commission), as well as to internal documentation of the project (i.e. that one related to project meetings, internal reports, etc.). The document naming convention is formed by the above elements, separated by "_". For instance, the final version of the current document in PDF format, ready to be submitted in the participant portal, is as follows:

"CIRCUIT_D7.2 – Project Quality Assurance, Ethics Manual and Risk Assessment Plan_v1.0_final.pdf"

SUBMITTED status is applied to documents that have been formally delivered to the EC.

APPROVED status is applied to documents that have been formally delivered to the EC and accepted by the EC's reviewers in a review process.

2.5 DELIVERABLES & OTHER DOCUMENTS FORMAT & LAYOUT

The official templates for deliverables, project meeting agendas, project meeting minutes are provided in Annexes 1 and 3 respectively. Any other template that will occur in the project will follow similar principles. Presentations template will be dealt with in WP7,

as part of the branding of the project. Those templates are all available as standalone template in the internal (Microsoft Teams) repository. All of them define a common structure for each case and specify the formatting for most of the commonly used elements in the respective type of reports.

In addition to the formatting and structure issues, all of them must adhere to some rules of good practice as follows:

- The document should be coherent and limited in size, avoiding verbosity. Although there is no rule in size of Deliverables; still, excessive verbalism should be avoided. Analytical information that goes in depth in one topic should be put in an Annex and only a summary of them should be included in the main body text.
- Language to be used is UK English.
- Deliverables should include all the outcomes of all associated tasks to them. It is upon the responsibility of the Lead Author (as assigned in the DoA and also repeated in Annex 2) to collect from other beneficiaries their input, evaluate their quality and, if needed, ask for revised versions and critically synthesize them in order to reach the expected goal.
- Dissemination rules should be respected, thus acknowledgment to the EC should be included in the cover page as follows:

2.6 QUALITY ASSURANCE

The beneficiary acting as Lead Author, according to the DoA, is responsible to coordinate all inputs from other involved partners and to prepare the draft deliverable according to the predefined general format and quality assurance standards defined above. The Lead Author is also responsible to define the key methodological approach, propose and finalise the document structure and coordinate all contributions required among the respective beneficiaries, setting intermediate versions and respective deadlines to reach and deliver the expected outcome.

The Quality Control Board (QCB) is responsible to conduct the peer review of each deliverable before submission. It consists of the following partners:

- The Project Coordinator (FEHRL).
- The Technical & Innovation Managers (Ms Irina Stipanovic (INFRAPLAN) and Mr. Carlos Martin-Portugues Montoliu (ACCIONA)), acting also as the Quality and Risk Managers of the project.
- Two (2) experts coming from Consortium beneficiaries (appointed in Annex 2).

A peer review template will be used for this purpose. Some deliverables, such as the current one, are excluded from peer review due to their nature (managerial or dissemination Deliverables). The full peer review plan of the project and the allocation of the roles among the beneficiaries respectively is provided in Annex 2. As it can be seen therein, FEHRL, INFRAPLAN and ACCIONA are permanent QCB members apart from the cases they are authors of Deliverables.

2.6.1 The Quality Manager

The Quality Managers are responsible for managing and overviewing all processes regarding quality assurance. For CIRCUIT, the appointed Quality Managers are Irina Stipanovic (INFRAPLAN) and Carlos Martin-Portugues Montoliu (ACCIONA).

The Quality Managers have the following key tasks:

- Quality control of all key project produced outcomes, such as deliverables, public reports, key dissemination material, project demonstrators, etc. according to the defined specifications and time schedule defined in the DoA. In addition, management of all the relevant quality processes in this context (i.e. peer review of Deliverables);
  - For the deliverables, the Quality Managers will ensure that all defined herein standards are met (document information & identification, style & formatting, language and content check), documents have been subjected to internal peer review according to the plan of Annex 2 and submitted before the deadline date.
- Overview and timely recognition of outcomes non-conforming to quality control processes, provision of respective guidance to meet the original standards and commitment and monitoring until problems' resolution and verification of solutions' implementation.

Specifically for Deliverables, the final consolidated review of each Deliverable will be conducted by the Quality Managers. They will be responsible for collecting all feedback from all individual (internal and external) peer reviews, consolidate them in one consolidated form for the author(s) that will be sent to them for finalising their Deliverable and addressing the comments listed, providing for each revision made according to them an answer.

During this consolidation process, the Quality Managers will also focus on the following aspects:

- Assurance that the Deliverable meets the original commitment as being reflected in the DoA, in terms of goal, objectives and expected outcome.
- Respect to the style and format according to the principles defined in the Deliverable template and in this document.

In addition, the Quality Managers are responsible for checking/ensuring that the final Deliverable returned by the author(s) upon the peer review comments conform to the

consolidated peer review comments and, if not, a proper justification is provided in the author(s) response part of the form.

2.6.2 Peer Review (internal & external experts)

The assigned peer reviewers (see Annex 2) are appointed to review the deliverable across the following aspects:
Provide general comments for

- Deliverable content thoroughness and structure
- Innovation level
- Correspondence to project and programme objectives

Provide specific comments -if necessary- for

- Topic A: Relevance
- Topic B: Methodological framework soundness
- Topic C: Quality of achievements
- Topic D: Quality of presentation of achievements

The peer review document will clearly state the overall evaluation outcome, which can be one of the following ratings:

- Accepted
- Conditionally accepted
- Rejected

2.6.3 Consolidated Peer Review to be conducted by the Quality Manager

Irina Stipanovic (INFRAPLAN) and Carlos Martin-Portugues Montoliu (ACCIONA), acting as the Quality Managers, consolidate the results coming from the individual peer review reports, identify and resolve conflicting comments and will provide one consolidated peer review form to the Lead Author(s) requesting for the final Deliverable from the side and the answer to the consolidated peer review form, where they will explain how the comments have been addressed.

2.6.4 Review by the Project Coordinator and submission

The final stage before submission of the Deliverable is its final check by the Project Coordinator (FEHRL) upon receipt by the author and confirmation by the Quality Managers (INFRAPLAN and ACCIONA) that it is ready for submission.
The Coordinator will quickly review the document and if it has no objection, will proceed with the submission of an electronic copy to the EC via the online Participant Portal within the appropriate timeframe and in the necessary format.
FEHRL will also archive backups and originals; circulation of electronic copies to all project partners via the project internal repository (denoting the SUBMITTED and later the APPROVED Deliverables).

2.7 DELIVERABLE PEER REVIEW PROCESS

To ensure that all the requirements and principles described in the current document are met, a strict framework of serial actions will be followed for the quality assurance of project Deliverables. As of the start of the implementation and until the submission of the Deliverable, those are as follows and in the appointed order:

1. The Deliverable Lead Author issues the provisional Table of Contents (ToC) of the Deliverable and uploads in the respective folder of the project repository, 4 months before the final deadline provided in the G.A., notifying the PMT, the respective Task and WP leader.
2. As soon as the ToC is agreed among the above members, the Deliverable main Author shares responsibilities among participants/Co-Authors and monitors progress of contributions along with the respective Activity and WP leaders, with a frequent update to the PMT regarding the progress of the Deliverable.
3. The Deliverable Lead Author, in agreement and collaboration with the other Co-Authors, iteratively and progressively updates purpose, audience and ToC as well as content.
4. Two months before the official deadline of Deliverable, a complete draft is sent out by the Deliverable Lead Author for internal (to the WP) comments and revision with a notification to the Project Management Team (PMT).
5. One month before the official deadline of the Deliverable, the Deliverable Lead author uploads the draft Deliverable for peer review in the respective folder of the internal project repository and notifies respectively the Quality Manager.
6. The Quality Managers inform respectively the internal and external peer reviewers that the peer review process can start, giving 15 calendar days for completing their reviews.
7. All assigned peer reviewers must return the peer review form with their comments in the given timeframe and the Quality Manager consolidates them using the respective form and provides them to the Lead author.
8. The Lead Author is responsible to return the Deliverable back together with all the contributing authors' response to the comments in one week time (Annex 4) acknowledging to the PMT.
9. The Quality Managers check conformity in two calendar days and acknowledges the Coordinator.
10. The Coordinator reviews in one calendar day and proceeds with submission, acknowledging to the whole Consortium the submission of the Deliverable.

If a non-conformity issue is noticed in steps 9 and/or 10, the Quality Managers/Coordinator request the author(s) for corrective actions before closing the Deliverable.

2.8 ESSENTIAL SOFTWARE TOOLS

This section defines the software tools which are considered as a basic requirement to achieve a good level of interoperability and cooperation between consortium partners. These are:

- Operating Systems: Windows 10, Mac OS X 10.10 or later, Linux stable distributions
- MS Office 2010 or later for
  - Documents (MS-Word)
  - Worksheets (MS-EXCEL)
  - Presentation tools (MS-POWERPOINT)
- Google Docs and OneDrive (latest version)
- Adobe reader or other suitable applications able to view and publish in the latest format of Portable Document Format (PDF).
- ZOOM
- GoToMeeting
- GoToWebinar
- Microsoft Teams
- Microsoft SharePoint

All operating systems and tools compliant with the aforementioned.

3 PROJECT RISK ASSESSMENT

The risk management of the project falls under the responsibility of the Project Executive Group (PEG) that, monthly, will evaluate the foreseen risks and present relevant mitigation measures applied (if any) etc. A key aspect of the procedure will be the implementation of a risk register, in which risks and mitigation actions will be identified. The risk register will be updated throughout the project.

A six-month review cycle will then be performed by the General Assembly. The goal is to review whether certain areas have not progressed enough, to identify any potential risks that could arise during the development of the remaining tasks of the project and discuss and agree the corrective measures required to prevent their appearance.

Major project risks and contingency measures have already been identified as described in Table 2. Likelihood and severity (L/S) of each risk are expressed according to their significance: low (L), medium (M), high (H).

Table 2: Critical risks for implementation

Description of risk	L/S	WP(s)	Proposed risk-mitigation measures
Management Risks			
Defaulting/withdrawing partners or missing expertise of a specific sector, leading to biased/ incomplete outcomes	M/L	**7**	Consortium encompasses multiple entities with similar expertise (both SMEs and Research/Academia), allowing in case of a defaulting party, the shift of responsibility and resources to other entities for addressing the same objectives.
Deliverables do not achieve the expected quality or are not delivered in time	M/ M	**7**	Through the iterative quality procedure regarding Deliverables preparation and submission and the establishment of the Quality Board that will be managed by the Technical Manager, such occurrences (if any), will be mitigated to lead to the most high quality possible outcomes.
Technical Risks			
Lack of availability engagement within the expert group may affect the baseline assessment and inputs for holistic approach development.	L/M	1	Mix of expertise in the consortium and Advisory Board, as well in the association networks (FEHRL, ERF, IECA) will ensure high level input. Although very unlikely to be required, replacement expertise will be obtained from within road stakeholders, agencies and industry.
Lack of data as an input for building up models and demonstrators in the tools	L/M	1, 2	Engagement of road and motorway owners (ANAS, MITMA, HAC), and industry partners involved in pilot projects as well as several research organizations that have already developed collaborations with the owners, will ensure access and collection of input of data. Partners already possess lots of data.
Poor understanding of the digital technology and its intended use	L/M	2	Industry partners involved in the project are direct users of the technology which is developed and

Description of risk	L/S	WP(s)	Proposed risk-mitigation measures
			upgraded. Further dissemination will demonstration workshops which will act as an face-to-face and online teaching aid to help the initial development of the digital tunnel twin and its application and usage in the processes.
Lack of availability engagement within the expert group may affect the baseline assessment and inputs for holistic approach development.	L/M	1	Mix of expertise in the consortium and Advisory Board, as well in the association networks (FEHRL, ERF, IECA) will ensure high level input. Although very unlikely to be required, replacement expertise will be obtained from within road stakeholders, agencies and industry.
New binders developed do not meet the requirements as expected.	L/M	3	This risk is reduced through the involvement of highly experienced researchers, up-to date in the project's domain and with a huge know-how on a specific technology. In addition, some of the materials are commercially available, so they are designed for this purpose.
Results of CRS facility are not significant	M/L	3	There are not significant differences in the results of the CRS tests among the technologies. In this case, more weight will be given to the environmental and economic impact in the selection of the best technologies for the demo.
3DCPsafety wall: Printability issues with mix formulations utilizing secondary materials.	M/M	3	Start material characterization and selection early. If all else fails, use a printable mix without secondary materials.
3DCP safety wall: Negative results in the proof-of-concept tests.	M/M	3	Conduct simulations and small-scale tests during the design stage.
Up-scaling of asphalt mixtures incorporating new binders in local asphalt plants with no experience or lack of specific equipment (pilot 1).	M/H	5	Both HMPB and biobinders are designed for their use in conventional asphalt plants. Technical advice will be provided by task leaders to the asphalt plant to ensure quality.
Poor quality of GRS abutments (pilot 3).	M/M	5	ZAG will conduct laboratory tests on reclaimed infill material and will provide quality control personnel on-site during construction work to ensure adequate compaction.
Limitations in the adaptation of commercial electrochromic glass to pre-tunnel requirements (pilot 4).	L/M	5	The transparency factor of the electrochromic glass will be changed at a discrete rate as a function of the external luminance value.
Hybrid generators malfunctions (pilot 4).	L/L	5	The lighting poles will be also connected to the electric power grid so that any faults wouldn't cause safety problems to road users.
Logistic & Coordination Risks			
Reclaimed girder: No girders found on the market (the market with secondary components is not yet established).	H/H	3/5	ZAG is collecting bridge components for research purposes and some of these could be reutilised.

Description of risk	L/S	WP(s)	Proposed risk-mitigation measures
Lack of involvement regarding the questionnaire.	L/M	4	Involvement of ERF and FERHL in various working groups and organizations at European and international level will ensure good level of participation in the surveys. In addition, the consortium includes public bodies from five member states offering an important contribution from transport authorities
Quality of the responses from public bodies.	L/M	4	Public bodies involved in the consortium are committed to provide quality data and information towards a modernisation of their national GPP methodologies in line with EU climate neutrality objectives.
Prefabricated slabs : Slovenian Technical Approval not awarded on time.	M/H	5	Start the process early.
Political, legal or technical obstacles in launching GPP/IPP	M/H	5	Preparatory actions will be carried out from the beginning of the project to early look for solutions to possible obstacles. If all fails, XXXX
No tenders received in GPP/IPP call for the innovation partnership.	M/H	5	Local firms will be alerted before the call is published to ensure that at least one tender is submitted.
Delay or denial from the Italian Energy Manager to electrically connect the hybrid generators to the electric power grid (pilot 4).	M/L	5	Contact with the Italian Energy Manager will start at the beginning of the project so that any delay or denial to connect the hybrid generators can be solved with the creation of mini-grids
Delays related to possible appeals by participants in the tender following the related outcome (pilot 4).	M/M	5	ANAS will define clear award criteria that prevent any misinterpretation. Furthermore, during the tender phase, ANAS will be available to provide all the necessary clarifications to make the tender proceed smoothly.
Dissemination & Communication, IPR & Exploitation Risks			
COVID-19 outbreak prevents stakeholders' activities	L/M	6	Due to COVID-19 uncertainty or other major global disturbances, the consortium will work or the identification of appropriate methodological alternatives that ensure that participatory and D&C activities are not brought to a complete standstill and the project can continue producing results
Low stakeholders' engagement	L/H	6	Each of the responsible partners has significant experience working in the construction sector with extensive network in the field. The robust methods for recruitment, will ensure sufficient stakeholders are engaged. Where there proves to be local difficulties in recruiting, in the first instance, this will be overcome through assistance and advice from other partners.
Capacity building activities ineffective. The helpdesk is not useful	M/L	6	User research in WP4 will allow to build training materials adapted to user needs with tailored content. Different formats will be produced (live

Description of risk	L/S	WP(s)	Proposed risk-mitigation measures
			sessions, videos, workshops and other material…) to ensure it is adapted to different audiences and needs.

4 ETHICS & GDPR

4.1 PURPOSE OF THE ETHICS MANUAL

The current Chapter aims to provide an overview of the ethics principles and data protection principles to be followed in the project, as consolidated with the reformed legal framework in the EU. Along with ethics, the General Data Protection Regulation (GDPR) is a guiding document, together with other complementary legislative documents. The Chapter discusses the ethics manual in depth, as complemented by the compliance monitoring procedures, the informed consent procedures, the gender equality monitoring, the dedicated data protection policy, the enumeration and obligations of data controllers and processors in CIRCUIT that will be further elaborated in the course of the project, the appointment of data protection officers (DPOs), and lastly, the data protection impact assessment procedure (DPIA) to be followed in the project.

The purpose of the Data Protection Policy is to describe how personal data are processed, the purposes of processing, the data subjects' rights and the processing obligations arising in CIRCUIT. Such policy focuses mainly on compliance with mandatory data protection regulation regarding personal data in national or EU level and complementary local data protection requirements, if not entirely uniform in the EU level. The aim is to protect individuals as participants whenever these are involved in the evaluation activities at the pilot sites yet including any project activity involving humans. The Data Protection Policy is expected to be continuously revisited in the project to reflect the emerging needs along with the evolution of project activities.

At the same time, data controllers or data processors are accountable whenever conducting personal data know, as per their obligations described in the DPIA. The data protection policy provides guidance accordingly, along with templates for carrying out the assessment in a compliant manner.

The templates for the informed consent forms to be used in tests within CIRCUIT are provided in Annex 9 of this Deliverable. Those aim to serve as the baseline template for the further case specific templates to emerge depending on the respective test scope and target audience. They also go along with information sheets of CIRCUIT for the participants in language and terms intelligible for the participant.

Partners are expected to carry out any work and activities within the lifetime of CIRCUIT in compliance to the principles and processes described in the herein enclosed Ethics Manual. The application of the Ethics Manual principles will be monitored by the Ethics Manager of the project (FEHRL) supervising and collaborating with the full Project Ethics Board (PEB) of the project. The application of the highest standards of research integrity, the relevant international, European and national legislation and ethical principles will be monitored regularly, throughout the lifecycle of CIRCUIT.

Although the current version of this document stands for the first and final official version of the Ethics Manual, the Ethics Manual, across all its layers, is intended to be a "living document" to which references can be made throughout the duration of the project. Any potential updates of it but also the further elaboration of the data protection policy as well as the DPIA conduct will follow-up in WP7 and more specifically in the following Deliverables: D7.3: Data Management Plan (M6); D7.4: Data Management Plan – 1st Revision (M18), D7.5: Data Management Plan – 2nd Revision (M36) and D7.6: Data Management Plan – 3rd Revision (M48.)

Nevertheless, the utmost objective of this Chapter is to provide an established basis for the principles, processes, mechanisms and bodies that will be assigned in the project with the task to successfully monitor the implementation of ethics principles in the implementation and, mainly, the validation and other user related activities anticipated. To this end, the ethics manual is to be read in conjunction with the data management plans (DMP) that are going to be issued in the aforementioned Deliverables.

4.2 ETHICS MANUAL

4.2.1 Aim

The current Section discusses the Ethics Manual and more specifically a series of ethics obligations which are closely connected with the proper application of ethics principles during the CIRCUIT project. The Ethics manual is supervised by the Project Ethics Board (PEB), the Local Ethics Representatives (LERs) and the Data Protection Officers (DPO), as provided in the corresponding Annex of the current document. The Ethics Manual gives further clarifications about the inner workings of the PEB and the relations between the local ethics representatives and the partners of CIRCUIT. The Ethics Manual may also touch upon issues concerning ethics in relation to children, incidental findings, incentive schemes and gender.

4.2.2 Legislative instruments

For the preparation of work of the Ethics Manual, several legislative and non-binding instruments have been collected and consulted. An overview of this legislation is presented in the following table, as has been considered by the CIRCUIT Ethics Board.

Table 3: Legislation and non-binding instruments to be considered by CIRCUIT's Ethics Board

Ethical & social issue	Area of law	Legislation, Case law and Guidelines
Human Dignity and integrity	Fundamental (human) rights	• Universal Declaration of Human Rights (United Nations) Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe) • European Charter of Fundamental Rights (European Union)

		• Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe) • European Court of Justice case law about fundamental rights in the EU
Privacy and Autonomy	Right to personal data protection and new technologies	• The Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) (replacing the Directive 95/46/EC of the European parliament and the Council (1995)), on the protection of individuals about the processing of personal data and on the free movement of such data. • Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector. Take into account developments of Reform of the legislative framework for personal data protection (In January 2012, the European Commission proposed a reform of the Directive 95/46/CE, which constituted until now the basic instrument for personal data protection, in the form of a global Regulation on data protection 2012/001 (COD), supplemented by Directive 2012/0010 (COD) concerning the processing of personal in the area of police and judicial cooperation in criminal matters. • Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. • Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. • Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. • Proposal for a Regulation of the European Parliament and of the council on European data governance (Data Governance Act). • Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

		• Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). • Directive 85/374/EEC on liability for defective products as amended by Directive 1999/34/EC. • Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. • European Data Protection Board (EDPB) opinions and guidelines.

4.2.3 Partners' role and responsibilities

Within the project evolution the following regulations related to compliance, approvals, privacy, personal health information and collaboration should be applied for all partners involved in user related activities, such as evaluation activities, focus/ stakeholder groups, surveys and general data collection and processing.

Each party shall be responsible for ensuring its own compliance with all laws and regulations applicable to its activities. Such laws include, but are not limited to, those in respect of rights of privacy, data protection, non-discrimination, safety, intellectual property rights and healthcare.

Any party which provides any data or information to another party in connection with the project will not include any personal information relating to an identified or identifiable natural person or data subject.

To this end, the providing party will anonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, only from the anonymised data and any other available information, deduce the personal identity of individuals, and thus trigger the applicability of personal data legislation.

Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for their performance.

Partners supplying special data analysis tooling, shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

4.2.4 Ethics Code of Conduct

Code of Conduct for research integrity

ALLEA is the European Federation of Academies of Sciences and Humanities, representing more than 50 academies from over 40 EU and non-EU countries [3]. ALLEA has created the European Code of Conduct for Research Integrity. The Code serves the European research community as a community as a framework for self-regulation. The European Commission has recognised the Code as a reference document for research integrity for all EU-funded research projects and as a model for organisations and researchers across Europe.

The members and third parties of CIRCUIT are therefore obliged to ensure that the conditions for research Integrity set out in the Code are fulfilled. The Code will be used as a framework for dealing with ethical and professional issues within CIRCUIT.

Good research practices, according to the Code, are based upon the following fundamental principles of research integrity:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- Respect for colleagues, research participants, society, ecosystems, cultural heritage, and the environment.
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision, and mentoring, and for its wider impacts.

Code of Conduct for various ethical issues

The procedures and criteria that will be used to identify/recruit participants in the pilot test sites will be kept on file and submitted on request. Furthermore, the informed consent procedure as detailed in Annex 9 of this document will be implemented for the participation of humans and will be kept on file and submitted on request.

The members of CIRCUIT shall especially focus on the following:

- Abide to the Ethics Manual and Data Protection Policy of CIRCUIT.
- Protect private and sensitive information and ensure that participants will not be harmed during the pilots. The Data Protection Policy is found in the same document.
- Respect participant's free will and treat them as intelligent beings who decide for themselves about any type of gathered data that are indeed outcomes of their participation.
- Inform in full about which data will be collected and how data will be collected, processed, shared, and disposed before signing the consent form (Annex 9).
- Communicate ethical issues to the Project Ethics Board and the project management team to ensure these issues will be timely and effectively addressed, managed and resolved.

- Ensure ethics approval (wherever is applicable) is obtained on time and relevant documents are shared with the PEB.
- Communicate results their findings through open-access journals to other researchers and academic communities (especially true if it is requested by the funder). Personal data, unless separately agreed with the person, will not be published.
- Ethics control and monitoring within CIRCUIT is carried out by the PEB.

Transparency at each pilot site or any other site performing other activities involving humans should explain the following to recruited participants:

- general scope of CIRCUIT and short reference to its objectives,
- scope and short description of the pilot and the respective study,
- value of participation (benefits for the participant and the public in general),
- acknowledgement of research results, and
- role of participants in the activity (pilots, etc.).

Acknowledgement to the participants of CIRCUIT studies will be done by the local to each site evaluation teams. The evaluation team members will during testing ensure that the participants feel comfortable and not coerced or tired. Questions are allowed during testing, in designated times. Participants should be informed about this possibility beforehand. The contact person details will be provided to the participant along any information and contacts in case the participants have any questions after the end of the testing session.
Communication with participants should abide with fundamental rights principles. Participants should not feel coerced, threatened, or stressed by researchers. The researchers must make sure that their behaviour towards participants is not deceitful and that the participants has been given sufficient information about the project. The concept of deception and debriefing is discussed below.

Deception: researchers do not deceive by any means prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress. Researchers explain any deception that is an integral feature of the design and conduct of an experiment to participants as early as feasible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data. No deception will take place in CIRCUIT demonstrations and the user will be informed at all evaluation stages about the objectives and the procedures related to the pilots and how their data will be handled, processed, and stored. In the case a functionality of a service is emulated, they will be informed beforehand (in the context of "Scope and short description of the Pilot and respective study"), but they will be asked to perform and react as the situation was real.
Debriefing: Researchers provide a prompt opportunity for participants to obtain appropriate information about the nature, results and conclusions of the research, and they take reasonable steps to correct any misconceptions that participants may have of which the researchers are aware.

4.2.5 The CIRCUIT Ethics Board

4.2.5.1 Overview

In general, the Consortium shall implement the research project in full respect of the legal and ethical national requirements and code of practice. The Local Ethics Representatives (LER) will be used as a contact point to achieve this aim.
Thus, the Project Ethics Board (PEB) consists of the Chair/ Ethics and Legal Manager (FEHRL), the Coordinator (FEHRL), the Technical, Innovation and Quality Manager (INFRAPLAN, ACCIONA) and one representative of each pilot test site of the project. The PEB will be assisted, whenever necessary, by the Project Executive Group (PEG). The latter comprises the project coordinator, the WP leaders, the technical and innovation managers and the ethics manager. The PEG makes executive decisions on strategic issues. Major decisions concerning overall technological, innovation and exploitation direction of the project policies, standards, quality and IPR/knowledge management are within its competence.

4.2.5.2 Main responsibilities

The main responsibilities of the Project Ethics Board are as follows:

- Ensure the CIRCUIT project's ethics policy complies with European and national legislation.
- Ensure all project activities are conducted in line with CIRCUIT Ethics Manual and Data Protection policy.
- Resolve potential ethics issues, related conflicts and mitigate risks.
- Raise ethics issues related to CIRCUIT's research direction and resolve them in collaboration with pilot site responsible partners.

The CIRCUIT Ethics Board will be responsible for the project's ethics management and will act as supervisors of the ethical conduct of activities in the project. They will do so considering both European and national ethical and legal requirements. They will also collaborate with external members (e.g. regional/municipality authorities) to ensure the Board is making decisions that are in harmony with the ethical profile and agenda of the cities and areas that will act as pilot sites.
The PEB shall act in conformity with the national and European legislation and code of practices and must fully support and scrutinize any plans, operational documents, and research protocols to guarantee that the ethics policy is applied in all activities and foremost when and where users are involved. Partners should ensure timely submission of research protocols based on their previous experience with relevant bodies to avoid any delays in the pilot's instantiation.

4.2.6 Local Ethics Representatives (LER)

The profile of a member of the LER is defined as follows:

- Responsible for a pilot site.
- Experience in data collection and/or data management with humans involved.

- Experience in preparation and submission of ethical proposals and handling of approvals including compliance to GDPR.

The LER are required to report to the Ethics Board about all relevant activities, their compliance as well as any problems that may arise. The means to do so will be the Ethics Controlling Reports, according to the templates provided in Annexes 4 and 5, designed for this purpose. A summary for each pilot site will be obtained, and the information will become the Ethics profile of each pilot site. In addition to the CIRCUIT Controlling Report, ethical approvals will be obtained in the pilot test sites on city/national/ entity level, if they have obligation to do so.

The LER at each pilot test site will be the main contact point for any ethics related issues (e.g. submission of research/test protocols for approval, by the Institutional/National Ethics Committees, GDPR in collaboration with the designated DPO, etc.) from the specific pilot site point of view. Their role will be to comply with the Ethics Manual and report back before and after each round of the iterative and implementation plan (see D7.1 inception report for more) using the templates of Annexes 4 and 5 and which tackle with user involvement, ethical and data protection issues. In addition, one of the main tasks of the nominated persons will be to coordinate and be responsible for obtaining approval by the local/regional/institutional ethics and GDPR regulatory committees before any pilot-related activities take place (e.g. even before recruitment starts), if needed. Any required or requested authorisations and approvals remain official project documents at any time.

4.2.7 Risk assessment and mitigation strategy in ethics

The risk assessment includes the plans to ensure no harm will be brought upon the participants and pre-testing activities will ensure that this will stay the case. None of the pilot-related activities is anticipated to have any (side-) effects on the physical or mental integrity or health of the participant, other than the ones existing in their everyday activities. As diverse user groups are expected to be formed, (e.g., travellers including potentially people with disabilities, older citizens, young people, and various stakeholders) all sites will internally review the pilot/experimental plans of each phase and will reach a decision on the inherent risks for all addressed user groups.

To minimise risk, the LER ensure that the participants have received proper information. Also, when there are safety related issues, all necessary precautions will be taken. In all cases, the pilot sites will abide with the internal and/or national safety regulations applying in their sites. All the pilot site leaders have established internal company quality assurance procedures, which will be adopted to guarantee high level quality in CIRCUIT activities.
It is impossible to conceive a procedure, investigation, or process which would be riskless. One of the most important factors in the assessment of risk is the perception of the prospective participant of the importance of risk. The participant's life situation may substantially influence the way in which a risk is perceived. The end point of the process

is the consent given by the person to be part of the research project, having considered all aspects of the process and asked all relevant questions.
All relevant information will be given to the participants. This means that the project CIRCUIT will be carefully explained. The choice that is made and the consent that is given will be without coercion or undue pressure being applied. Categories of risk take into consideration:

- Physical risks (or material risks) stemming from traffic safety issues will be minimised and is expected to be at the same level as that experienced by the average traveller throughout their daily driving when in a hurry, fatigued, stressed, etc.
- Psychological consequences (or non-material risks) will be carefully examined and considered.
- Social inconveniences will be minimised (no additional stress or different from stress experienced during daily living/driving/travelling conditions, cost reimbursement for additional transport costs, etc.).

Table 4: Preliminary considerations regarding Ethical Risk Management in CIRCUIT

Ethical & Social risks	Description	Ethical Risk Management in CIRCUIT
Application of an overarching Ethical and legal framework	All relevant legislation, regulation and ethical codes will be taken into consideration; they are defined how they are met in terms of processes, timing and responsibilities.	CIRCUIT PEB will oversee the ethical issues in the project and the ethics approval processes at project level. The required Annexes include the information required to be addressed and included in an Ethics application form partners will be required to obtain prior any evaluation takes place.
Transparency and consent of the travellers	The informed consent administration ensures that the user accepts participation and is informed about the project and demonstration/evaluation objectives. Written consent, if needed, is obtained after participants are informed. Information provided is clear and understandable about their roles (tasks and rights), research objectives and methods applied, duration of study and participation (if they differ), confidentiality, safety and risk related issues as well as the benefit for them and the project.	The basic parts of the CIRCUIT informed consent, as per the requirements of the GDPR, include: • The possibility to decline the offer and to withdraw at any point of the process (and without consequences) • Information about the data controllers, processors and data processing in general • Contact person identification.
Privacy and data protection	Only anonymised or at least pseudonymised data will be processed and used in the evaluations and, therefore, no personal data will be processed in	In general, the project identifies which data protection rules apply and establishes a list of risks and potential solutions; taking due account of the following: what kind

	relation to a specific user. The name will not be connected to other characteristics (e.g. age, gender, nationality, health and/or mobility profile). To avoid risks related to the processing of personal data such as identity theft, discriminatory profiling or continuous surveillance, the principle of proportionality has to be respected. Data can be used only for the initial purpose, or compatible purposes, for which they were collected. Anonymisation or pseudonymisation is a way to prevent violations of privacy and data protection rules. Processing has to be limited to what is truly necessary, while less intrusive means for realising the same end have to be considered.	of data will be processed; what is the purpose of the processing; will the data exceed the purpose of the study; are there procedures ensuring that data is processed only for the originally identified purposes; who is the data controller; is personal data connected to other information; will data be commercially exploited; what is the duration of the storage of the data; where will the data be stored and according to which national legislation; who will have access to the data; will the user be recorded; which metrics will be implemented; who will supervise the application of the data protection principles.
Participants' engagement	Evaluation is expected to be inclusive and representative of different participant types, especially in a dynamically shaped real-life context. The selection and recruitment of participants is a crucial part of the involvement process, as it will impact on the quality of the outcomes and the sustainability of the research outcomes. At this stage a satisfactory number of users and combination of participants' characteristics is sought (i.e. to reflect and accommodate certain needs; gender balance and equality are addressed.	CIRCUIT will target specific participants' groups. Adequate number of participants will ensure sample representativeness, even at pre-Demonstration level, including: i) different age groups, ii) balanced female/male ratio iii) various social, cultural, and socio-economic (SES backgrounds). The PEB will oversee the selection of participants. Participant engagement will be governed by the guidelines defined by the Responsible Research and Innovation Framework[1].

4.2.8 Ethics in relation to participants

All research activities are organized in conformity with the data protection policy of CIRCUIT. If needed, participant groups and involved stakeholders will be recruited and invited, respectively, to participate in dedicated and controlled activities during the carrying out of the pilot tests. All participants should have the competence to understand

[1] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

the informed consent information. Recruitment of participants will take place during both pre-demonstrations and demonstrations.
The substantial number of users will ensure a wide trial perspective, including: i) different age groups, ii) balanced female/male ratio, and iii) various social backgrounds. The PEB of CIRCUIT will oversee the selection of participants when it is applicable (i.e. in stakeholder interviews, in the specific cases that passengers will be recruited).

4.2.9 Ethics in research with children

According to the United Nations Convention on the Rights of the Child, the term child refers to every human being under the age of eighteen years unless under the law applicable to the child, majority is attained earlier. Children are not addressed as a user group within CIRCUIT as such. They will not be recruited in the context of any evaluation or other user-related activity.

4.2.10 Not included in CIRCUIT

CIRCUIT will not touch any of the following fields of research:

- research activity aiming at human cloning for reproductive purposes.
- research activity intended to modify the genetic heritage of human beings which could make such changes heritable.
- research activities intended to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer.

Furthermore, CIRCUIT does not include any research involving:

- the use of human embryonic tissue, human foetuses, human foetal tissue, other human tissues
- genetic information
- pregnant women
- animals
- children
- users with special needs and mental disabilities

4.2.11 Incidental findings

The term 'incidental findings' refers to anticipated or unanticipated findings that are not in the scope of what is actively looked for in the research.
'Anticipated' incidental findings are findings that are known to be associated with a specific test or procedure. These findings do not have to be common or likely to occur. The defining characteristic is that the possibility of finding them is known.
'Unanticipated' incidental findings are findings that could not have been anticipated given the current state of scientific knowledge. Researchers cannot plan for these types of findings specifically. However, researchers can consider in advance what they might

do if a particular kind of unexpected finding arises, for example, one that could be actionable or lifesaving.
These 'incidental' or otherwise unintended or unexpected findings may include indications of criminal activity, abuse, domestic violence, bullying etc. Thus, they may have significant implications to welfare, safety, and security not only for the participants in the research activities but also for other people and for society.
In other words, they are defined as the findings that may be by-products or outcomes of the study that were not necessarily collected to answer the main research questions and objectives but could be of importance for the physiological, psychological, and metal wellbeing of the participant. The number and type of incidental findings could be different for each site and valuable for both the person and the other stakeholder groups.
The CIRCUIT project, like any social science and humanities research, relies on methods that may unintentionally produce findings outside the scope of the original research questions. Field work such as pilot tests and the observation therein may result in becoming aware of information that goes beyond the scope of the research design. Hence, it is likely that incidental findings occur during some testing and pilot phases.

4.2.12 Reimbursement

The pilot (mainly) participants may receive a reimbursement (incentive) as compensation for their participation. The incentive will be in line with the performing partners' general practice.
As commitment is essential for the success of the project, recruited participants might receive some form of reimbursement. In the event of recruiting employees, incentives are not used as people are already paid for their time. Participants should be informed of the presence/absence of incentives when recruited and a statement needs to be added in the consent form. In case of legal restrictions or policies, the ethics responsible at each pilot site should inform the PEB. An alternative to cash is using vouchers; sometimes it is easier for evaluation moderators to carry/use and they should be representative of the demographics (i.e. have an added value for older citizens). It is upon the discretion of each partner to decide the incentive scheme to use (or to not use). Other options include sharing the results of the study, making charitable donations, creating prize draws and offering nonmonetary gifts. The PEB will oversee and approve (or not) the incentive schemes chosen by each pilot site (including the sites that will perform driver simulation activities).

4.2.13 Gender monitoring

The gender level of participation within the CIRCUIT activities will be monitored. Equal opportunities and equal treatment between men and women shall be guaranteed.
Over the years, the European Parliament has supported and called for measures to improve the position of women. This work continues through the activities of the Women's Committee. In detail, several specific European and UN Policies have been adopted to promote the equity of gender. Those will be fully respected within the project. The monitoring of the gender level of participation within the project activities is important for CIRCUIT.

Gender and equity issues will be monitored to guarantee equal (to the maximum extent) representations of genders, age groups, mobility limitations and socio-economic groups, to the extent applicable in the project planned activities. The safeguarding of the right to non-discrimination will be materialized through continuous monitoring of research groups and their gender representation in the project. Specific templates will be used, when necessary, inspired from the work of Horizon Europe Guidance on Gender Equality Plans (European Commission, Directorate-General for Research and Innovation, Horizon Europe guidance on gender equality plans, Publications Office of the European Union, 2021). The Gender Equality Plan will concern, among others, the publications, the dedicated resources, the data collection and monitoring, as well as the training of personnel. It should consider how the gender dimension will be incorporated in the contents of research or educational activities and outputs of the organisation. Content-wise, the plan will pay particular attention to the work-life balance and organizational culture as well as the gender balance in leadership and decision-making, among others. Most of all, in the context of equity principles, the project will try to ensure as much as equal representation of genders in the tests planned, even though test samples in the project will be small, making it rather challenging to achieve a gender equilibrium in every single test. This will be the case for the pilot tests. Summing up, CIRCUIT will ensure that during all its phases, and as much as possible, equal gender participation will be maintained, this addresses research and development phases, as well as evaluation phases. The gender will be one of the test/evaluations participants' characteristics that will be tracked and statistically processed (to come up with any correlations if applicable). Each pilot site, along with its LER and assistance from the PEB, is responsible to choose its own gender balance and justify its selection, if asked for.

4.3 ETHICS COMPLIANCE MONITORING

4.3.1 Overview

A "Questionnaire on ethical and legal issues" of the respective Annex has been prepared and is expected to be completed with the supervision by each LER (Local Ethics Representative) for each pilot site respectively with a twofold scope: a) to capture the current status of ethical aspects/issues at each pilot site of the project, and b) to serve as a checklist reminding the researchers/conductors to consider all relevant ethical aspects before conducting any evaluation activities within CIRCUIT, in view of the upcoming pilot phase.
The form itself is divided into several subsections (e.g. participants and informed consent, ethical control instruments, privacy, safety, risk assessment and reimbursement).
During the period of the pilot sites activities, it is expected that all collected data will be kept entirely confidential and their anonymity will be protected in full across all sites, as dictate by the CIRCUIT Ethics Manual. Field trials data management will be carried out at all pilot sites according to the General Data Protection Regulation (GDPR) (Regulation EU 2016/679) and the project data management procedures as will be identified in the Data Management Plans of WP7. Furthermore, it is the LERs in continuous collaboration with their entity's Data Protection Officer (DPO), when existing and when applicable,

who will guarantee the compliance of the project data related activities with the GDPR regulations.

4.3.2 Participants and informed consent

The GDPR sets a high standard for consent, while also all of the five (5) CIRCUIT pilot sites are also obliged according to their national/regional/institutional regulation to obtain the consent of pilot activities participants. This means that there might be slight differences (usually procedural) among the sites when it comes to the relevant lawful basis for personal data depending on the type of organization. Still, all relevant information will be given to the participants of all pilot sites in CIRCUIT.
Each pilot site will edit the required templates of the informed consent forms and information sheets, according to their main research objectives per demonstration phase and will define the procedures regarding the collection, storage, and protection of personal data, in compliance with the European and national legislation and the project established processes and mechanisms, but also in relation to the local logging processes, to the extent applicable. The signed forms, whenever required, will be kept locally and will be available upon request.
All pilot sites representatives will ensure that the informed consent will be provided/translated in a manner comprehensible by all, while also all participants will be given sufficient time to reflect their decision of giving or withholding consent. Other than that, it is a project decision to not include in the testing (or any other activities) individuals who will not be having the necessary cognitive capacity and/or ability to consent (children and users with special needs and mental disabilities). The informed consent form will be translated into the national language of all pilot sites. Following the approval of the informed consent by respective bodies, its translated version will be used with a small group of project participants to validate that the included information and the chosen form of presentation is appropriate and understood by all types of participants.
The controller must also have a valid lawful basis to process personal data. Among the five (5) CIRCUIT sites that will participate, they all acknowledge an international or national legislation (or institutional regulation), which they must follow when performing tests within CIRCUIT project, involving healthy human participants, and that there is a respective legislation/regulation for the involvement of participants with cognitive impairments/learning difficulties.

4.3.3 Ethical control instruments

In the five (5) pilot sites there could be the case that a controlling body or controlling committee needs to be contacted and get approval from (on national/regional/local/institutional level) for the experimental procedures prior to the evaluation activities. Another option could be an internal review board on human research which may take over. Out of the ones that there will be a local ethics controlling committee/ controlling body that their organisation is usually obliged to get approval from it is not necessary for them to obtain this approval for CIRCUIT specifically, as the informed consent form process fulfils the requirement.

However, the Local Ethics Responsible (LERs) will be contacted by the CIRCUIT Ethics Board to ensure that the processes are conducted in line with the project's ethics policy and that no further action is necessary to be taken in relation to ethics approvals from regional bodies.
For those sites that Ethics approval is required at any level (institutional, national, etc.), the corresponding forms will be collected (the process has started already) and reserved internally in the project to be available upon request.

4.3.4 Privacy and data protection

The pilot sites operators acknowledge the processing of personal data during the CIRCUIT field testing. In case and to the extent this gets anticipated by the data collection requirements of the project, the collected data will be made anonymous and with no association enabler to retrieve them. There might be cases that for the accommodation of project services there will be data storage of personal data; in those cases, data will be however anonymously stored in a coded form as will be instructed in the context of the project data processing mechanisms so that no traveller identities are revealed.
The Local Ethics Responsible are the a priori identified persons and will be the only contacts having access to full contact details of the participants as well as to their consent forms that will be signed in all cases. Moreover, all sites have stated that there is a Data Protection Authority on national/regional level.

4.4 DATA PROTECTION ONLIGATIONS

4.4.1 In general

The CIRCUIT project aims to develop a holistic approach supported by digital solutions and guidelines to foster the introduction of innovative engineering practices in the whole construction supply/value chain enabling circular, sustainable resilient and smart transport infrastructure and a wider deployment of Green Public and Innovation Procurement. To that end, personal data of natural persons are expected to be processed, both in pilot sites and during the research studies. The parties to CIRCUIT will follow all applicable data protection laws, whether national or European, and adapt routines continuously so that the processing of personal data for which the parties are responsible does not violate the fundamental rights and freedoms of individuals.

Personal data which will be processed by partners or by external stakeholders during CIRCUIT may fall in the scope of one of the following categories:

- Personal Data collected in the context of participation in a research study,
- Contact information such as name, address, telephone number and email address,
- Banking and other financial information for payment or invoicing purposes,
- Information about websites, for the purpose of making them more user-friendly, such as cookies,
- Information about participation in conferences or courses, and

- Personal data needed for employment purposes.

The European Commission requests that the consortium abides by the data protection legislation, and in particular the implementation of the data protection principles. For instance, how personal data processing is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle) is one of the principles explained below. In addition, a systematic description of security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing is necessary, as well as a description of the anonymisation / pseudonymisation techniques that will be implemented. A detailed information on the informed consent procedures about data processing operations annexed to this document conceptually follows the content of this section.

4.4.2 Kay actors and concepts

For the purposes of this section, the European-level General Data Protection Regulation (GDPR) is considered. The Regulation, founded in the three pillars of lawfulness, fairness and transparency, has reformed the data protection framework in the EU and has created a more robust accountability regime for involved actors. Specifically, it recognizes five parties:

- Data controller 'means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.
- Data processor 'is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.
- Data subject 'is a natural person whose personal data is processed by a controller or processor'.
- Data protection officer (DPO) is an enterprise security leadership role to oversee data protection strategy and implementation to ensure compliance with GDPR requirements. The DPO assists the controller or the processor in all issues relating to the protection of personal data of data subjects.
- Data protection authority is an independent public authority responsible for monitoring the application of the Regulation and vested with specific tasks and powers.

The most important concept, however, is the definition of personal data as such. According to the GDPR, personal data means 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. The definition is quite broad, ensuring a large scope of application and extensive protection to the data subjects.

4.4.3 Data protection principles

The Regulation sets forth several cornerstone principles which aim to ensure proper and effective implementation of data protection law. These principles are the following:

- Lawfulness, fairness, and transparency: three fundamental principles in data protection law jointly act as the starting point for the more detailed provisions on processing. Largely, these concern the data controller.
  - To process personal data, the data controller must have a lawful basis to do so. This basis functions as an enabler for processing personal data within the scope of the purposes identified. Lawful processing requires the consent of the data subject, or one of the five other legitimate grounds provided in the data protection legislation. It also implies that the data controller has reviewed the purposes of the processing activities and has selected the most appropriate lawful basis (or bases) for each activity.
  - Personal data must be processed fairly. This means that processing must be done in ways that people would reasonably expect, and not in ways that have unjustified adverse effects on them, or in ways that could mislead them. This does not mean, however, that every processing that would negatively affect an individual should be considered 'unfair'.
  - The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Among other things, the following information is provided beforehand: the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended, and the legal basis for the processing, the legitimate interests pursued, the legitimate interests, the period for which the personal data will be stored, etc. Transparency in processing facilitates the exercising of the data subject's rights.
- Purpose limitation: this means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, any processing of personal data must be performed for a specific well-defined purpose, and if this happens for additional purposes, these must be specified and compatible with the original one. Its objective is primarily legal certainty, along with predictability and user control. Neither processing personal data for undefined or unlimited purposes is lawful, nor is processing based on the assumption that it may be useful at some point in the future. It is the data controller who defines the purposes of processing. In assessing the compatibility of the initial specific purpose with any additional ones, the controller shall take the following into consideration: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected; the reasonable expectations of data subjects; the nature of the personal data; the consequences of the processing for data subjects; the existence of appropriate safeguards.

- Data minimisation: this principle means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. All these three words, 'adequate, relevant and limited' are subject to the discretionary power of the data controller. The criteria for the assessment of necessity of processing are not straightforward, and neither is the extent to which the purpose of the processing can be reasonably fulfilled by other means. What is deemed 'appropriate' in the case of extensive processing systems is not listed, in order to avoid prescriptiveness and to allow greater conformity with technological advancements. The data controller shall proceed to an assessment of the measures adopted, to ensure that data processing does not entail a disproportionate interference in the fundamental rights and freedoms.
- Data accuracy: a data controller must ascertain that data are accurate and kept up to date by guaranteeing that data that are inaccurate are erased or rectified without delay. The data subject shall have the right to restriction of processing by the controller when the accuracy of the personal data is contested.
- Storage limitation: the data controller shall ensure that personal data are deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected. Personal data shall be kept in a form that permits identification of data subjects for no longer than what is necessary for the purposes for which the personal data are processed. Storage limitation functions in conjunction with purpose limitation, since these both allow for the same exception of further processing solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. Data subjects must be appropriately informed about the standard retention periods through the privacy policy. This principle enables compliance with individuals' requests for erasure under 'the right to be forgotten'.

4.4.4 Data subject rights

The Regulation bestows several rights to the data subjects:

- The right to be informed: The transparency principle requires that any personal data processing should generally be transparent to individuals. To this end, the data controller is obligated to provide information to the data subjects. This holds whether personal data are collected from the data subject directly or have not been obtained from the data subject, but instead from third parties. Such an obligation does not depend on a request from the data subject. Rather, the controller must proactively comply with the obligation, regardless of whether the data subject shows an interest in the information or not.
- The right to access one's own data: a pivotal right and also set out as one of the elements of the fundamental right to the protection of personal data in the Charter of Fundamental Rights. The right of access gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps data subjects to understand how and why the data controller is using their data, and check whether this is being done lawfully.

- The right to rectification: EU law provides for a right to rectification of personal data. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. This right includes completing data which were previously incomplete, or inaccurate personal data, which must be rectified without undue or excessive delay.
- The right to erasure: Data subjects have the right to have their own personal data erased, pursuant to the principle of data minimisation. This is applicable, for instance where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent, or the data has been unlawfully processed.
- The right to restriction of processing: Data subjects are entitled to obtain from the controller restriction of processing of their personal data where the accuracy of the personal data processed by the data controller is disputed or is unknown, the processing itself is unlawful, the processing of personal data is not necessary for the purposes intended, or the data subject has objected to the processing.
- The right to data portability: Applying the right to data portability essentially means that data subjects are entitled to have their personal data transmitted directly from one controller to another if this is technically feasible. This involves receiving the personal data in a structured, commonly used and machine-readable format and then transmitting that data to another controller without hindrance.
- The right to object: Data subjects have the right to object to the processing of their personal data in certain circumstances, such as where a task is carried out in the public interest, or in the exercising of official authority or legitimate interests.
- Right not to be subject to automated decision-making, including profiling: In principle, data subjects must not be subject to automated decisions that give rise to legal or similarly significant effects. This right is passive, in the sense that it equates to a general prohibition and does not require the data subject to proactively seek an objection to such a decision. Automated decision-making based on profiling may take the form of analysing or predicting aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, etc. If such processing is conducted, it must be accompanied by adequate safeguards for the data subject, such as the right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision.

4.4.5 Lawfulness of processing

Pursuant to the principle of lawfulness, personal data may be lawfully processed if they meet one of the following criteria (lawful grounds):

a. Consent: the data subject has given consent to the processing of their personal data for one or more specific purposes. Consent is considered freely given if the data subject has genuine or free choice or can refuse or withdraw consent without detriment. It shall be as easy to withdraw as to give consent, at any time.

b. Contract: processing is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering a contract.
c. Legal obligation: processing is necessary for compliance with a legal obligation to which the controller is subject. For instance, employers must process data about their employees for social security and taxation reasons, and businesses must process data about their customers for taxation purposes.
d. Vital interests: processing is necessary in order to protect the vital interests of the data subject or of another natural person. An illustration would be when monitoring epidemics and their development, or where there is a humanitarian emergency, for instance in an accident.
e. Public interest: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is most relevant to public authorities, and the underlying task, function or power must have a clear basis in law.
f. Legitimate interest: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, where the data subject is a child. In this respect, the legitimate interests of the controller are first identified, and then a balancing exercise must be conducted between those interests and the interests or fundamental rights and freedoms of the data subject.

4.4.6 Security of processing

The principle of data security is probably the most complicated and disputed one. It is connected to a data protection principle, that of integrity and confidentiality. It requires that the security, integrity and confidentiality of personal data is guaranteed, so as to prevent adverse effects for the data subject. Measures adopted could be either of a technical or organisational nature. The appropriateness of security measures must be determined on a case-by-case basis and be reviewed regularly.
Criteria for such choice are 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.
Measures that are deemed technically appropriate, among others, are: the pseudonymisation and encryption, the confidentiality, integrity, availability and resilience of processing systems and services, restoration of the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
Measures that correspond to good organisational rules could be: regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations, clear distribution of responsibilities and a transparent outline of competences in matters of data processing and ensuring that authorisations to access personal data have been assigned by the competent person and require proper documentation.

4.4.7 Data protection by design and by default

Data protection by design and by default refers to the effective implementation of data protection principles and appropriate technical and organisational measures to safeguard data subjects' rights and freedoms. The concept is an evolution of what was previously known as privacy by design and is currently a legal requirement.
Data protection by design applies to the development of new services, systems, processes or products that involve personal data processing. It involves implementation of appropriate technical and organisational measures designed to implement the data protection principles, and the integration of safeguards into the processing necessary to fulfil the legal requirements and protect data subjects' rights. This way, privacy and data protection are guaranteed at the design phase of any system, service, product or process, and then throughout the lifecycle.
Data protection by default requires that the data controller ensures processing of the data that is necessary to achieve a specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation. A misunderstanding could be that it requires the adoption of a 'default to off' solution, but this is not true; this principle translates as the need to specify the personal data before the processing starts, to appropriately inform individuals, and to only process the data that are needed for the purpose.

4.4.8 Data breaches

One additional accountability mechanism is that relating to data breaches. A personal data breach refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to processed personal data. Data breaches can be highly detrimental to the data protection rights of individuals who, because of the breach, lose control over their personal data. They are subsequently exposed to risks, such as identity theft or fraud, financial loss or material damages, loss of confidentiality of personal data protected by professional secrecy, and damage to their reputation. When a personal data breach is detected, and if it is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The notification must include a description of the nature of the data breach, of data subjects affected, and a description of the possible consequences. If the data breach is likely to result in high risks for the data subjects, then the data controller must inform the data subjects in clear and plain language. At the same time, the controller is responsible for informing the supervisory authorities.

4.4.9 Data transfers

The level of protection of personal data is deemed to accompany them in function of the country that the personal data are. Data protection law regulates transfers of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation. In other words, if and whenever personal data are transferred outside the EU (and EEA), then they are subject

to specific rules in processing. Regarding the principle of free movement of personal data in the EU, this shall be neither restricted nor prohibited for reasons connected with the protection of natural persons regarding the processing of personal data. Depending on the recipient of personal data, there are different tools to frame the data transfers. The strongest, but also the least common, is the adequacy decision. A third country may be declared as offering an adequate level of protection, under a European Commission decision, meaning that data can be transferred to another company in that third country without the data exporter being required to provide further safeguards or conditions. If an adequacy decision has not been signed, then data controllers can transfer personal data based on binding corporate rules, which are legally binding to every member of the group. Alternatively, they can use standard contractual clauses approved by the European Commission; lastly, it is possible to adhere to a code of conduct or certification mechanism.

4.4.10 Data protection impact assessment (DPIA)

The requirement to conduct data protection impact assessments (DPIAs) in several innovative laws around the world is not coincidental. The recently reformed personal data protection law in the EU introduced a requirement for data controllers to assess the impacts of data processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons" with regard to the protection of personal data. The level of risk varies depending on the nature and scope of processing. Large-scale operations and those involving the processing of sensitive data present much higher risks for data subjects compared to smaller-scale data controllers who processes their employees' personal phone numbers. The Regulation foresees a list of processing operations that are considered high-risk and for which a prior impact assessment is necessary: where there is systematic and extensive evaluation of personal aspects (profiling), where special categories of data or personal data relating to criminal convictions or offences are processed, and where processing involves the large-scale, systematic monitoring of publicly accessible areas. The content of the impact assessment shall include, among other things, an assessment of the necessity and proportionality of the processing operations and the possible risks to the rights of individuals, as well as mitigation measures for the risks identified. To demonstrate compliance, data controllers must maintain a record of the processing activities carried out under their responsibility. The consortium of CIRCUIT, having identified a list of processing operations and risks stemming therefrom, proceeds to such assessment, as described below, in another Section of this Chapter. A tailored-down framework, method and template for the DPIA are also provided in this Chapter.

4.4.11 Pseudonymisation and anonymization

The process of pseudonymisation of personal data aims to reduce the risks to the data subjects by helping the data controller, as a mitigation measure, to demonstrate the accountability principle. Pseudonymisation is a technique that replaces or removes information in a data set that identifies a natural person. Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for

example, a reference number. The controller (or the processor) may tie that reference number back to the individual if they have access to the relevant information. This additional information shall be held separately and without easy access to everyone. However, pseudonymised personal data do still fall within the material scope of the Regulation and are treated as such. An additional measure towards mitigating the risks involved with processing, is the encryption (i.e. pseudonymisation and coding) to the extent reasonably possible, so that individual cannot be identified. Pseudonymisation is thus preserved by consistently coding participants with unique identification codes.
On the other hand, anonymization is the process of removing every trace or information which would relate back to a natural person, therefore rendering the nature of information as non-personal. Anonymisation is a method of limiting risk to the data subjects while processing. Anonymising data wherever possible is therefore encouraged and preferred over pseudonymization. While the GDPR applies in pseudonymized data, it does not apply to personal data that has been anonymised, i.e. 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 no longer identifiable.
To be truly anonymised under the GDPR, the data controller must remove all elements from personal data which would identify an individual. However, if the controller or the processor could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data would effectively not have been anonymised, but would have been merely pseudonymised.

4.4.12 Specifically: the informed consent procedure

The CIRCUIT project develops under WP7 -ethics requirements – a procedure to obtain informed consent for the participation of humans in the project (ethical requirement to conduct scientific research making sure researchers reach an agreement with individuals about whether they wish to participate in the research) and a procedure to obtain informed consent from participants for processing their personal data (to streamline the legal requirement under the General Data Protection Regulation).
The consent procedure for the pilot use case realisation at each of the selected pilot sites will be obtained through a two-stage procedure. Initially, each pilot leader will verbally present the pilot to people that will be involved, carefully describing the level of personal data processing and privacy infringement that the execution of each of the pilot realisation involves. Secondly, after a few days, participants will be required to read and sign an informed consent form that will explain in both plain English and in local language what the trial leader has already verbally explained, in a form that is intelligible to the participant.
CIRCUIT research will be continuously monitored by the Project Ethics Board of the consortium and through its local interfaces (LERs). All national legal and ethical requirements of the relevant Directives where the research is performed will be fulfilled. Personal data of participants will be strictly held confidential at any time of the research. Several consent forms have been developed, which will be available for the partners and test site pilot leaders to use as appropriate. Some of these are: the informed consent procedure for the participation of humans in the project; the consent form to participate in the CIRCUIT research; the consent form for dissemination purposes; the informed

consent procedure in connection to data processing according with GDPR • Information sheet on the CIRCUIT project.

4.5 DATA PROTECTION POLICY

4.5.1 Overview

Personal data must be processed in compliance with applicable data protection laws. The exact requirements and due diligence for the processing of personal data need to be scoped and defined within the relevant jurisdictions.
All parties and third parties to CIRCUIT must comply with all applicable data protection laws and adapt routines continuously so that the processing of personal data for which the parties are responsible does not violate the rights and freedoms of individuals. Each one is responsible for complying with the CIRCUIT data protection policy.
Throughout this data protection policy, a party or third party to CIRCUIT which is processing personal data will be referred to as controller and/or processor.
For identifying the minimum obligations of controllers and processors, templates and checklists are attached from the Information Commissioner's Office, in English. These are expected to help the controllers and processors to meet the obligations for compliance under the GDPR. In case of uncertainty concerning the controllers/processors ability to meet the requirements of the GDPR, it is recommended that the controller/processor use these checklists. Be aware that there might be other regulations to comply with as well, for example complimentary national regulations to the GDPR.
The personal data that is or will be processed with in CIRCUIT will fall into one of the following categories:

- Personal data collected in the context of participation in a research study,
- Contact information such as name, address, telephone number and email address,
- Banking and other financial information for payment or invoicing purposes,
- Information about how one uses websites, for the purpose of making them more user-friendly, for example via cookies,
- Information about participation in conferences or courses, and
- Personal data needed for employment purposes.

The Data Management Plan, across its consecutive issues in WP7, for CIRCUIT will further explain how the parties must process information to fulfil their obligations.

4.5.2 Terminology for Data Protection Policy

Anonymisation: the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR.

Data Protection laws: EU Data Protection legislation and, to the extent applicable, the data protection or privacy laws of the pilot site country.

Data Protection Policy: the current Section, as a comprehensive document of the data controller obligations, data subject rights and specification of data protection principles.

DPO: the Data Protection Officer

DPIA: the Data Protection Impact Assessment

GDPR: the General Data Protection Regulation (EU) 2016/679

ICO: the Information Commissioner's Office

Pseudonymisation: the act of processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special category of personal data: any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health (also known as sensitive data).

The terms, "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Third countries", "Processing", "Processor" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
A party in processing of personal data in this data protection policy is referred to as a controller or a processor, depending on whether the party defines the means and purposes of processing or is merely following the instructions of other parties, without engaging in the decision-making.

4.5.3 Data Protection Officer

In general, each controller is obliged to appoint a Data Protection Officer (DPO) unless the duty is not mandatory under the GDPR. It is a necessity to appoint a DPO if a DPIA must be carried out before a lawful processing of personal data can begin. Below are the tasks and role of the DPO, as suggested by the ICO [3].

Position of the DPO per applicable partner in the Consortium (see more in section 4.6).

- The DPO reports directly to the highest level of management (PMT through LER) and is given the required independence to perform their tasks.
- The DPO is involved, in a timely manner, in all issues relating to the protection of Personal Data.
- The DPO is sufficiently well resourced to be able to perform their tasks.
- The DPO is not penalized for performing their duties.
- We ensure that any other tasks or duties we assign the DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

- The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, the data protection policies, awareness-raising, training, and audits.
- The advice of the DPO should be taken into consideration as well as the information they provide on data protection obligations.
- When carrying out a DPIA, the advice of a DPO who also monitors the process, is sought.
- The DPO acts as a contact point for the Supervisory Authority. They co-operate with the Supervisory Authority, including during prior consultations under Article 36, and will consult on any other matter.
- When performing their tasks, the DPO has due regard to the risk associated with data processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

- The DPO is easily accessible as a point of contact for all involved employees, individuals and the Supervisory Authority.
- The contact details of the DPO have been published and communicated them to the Supervisory Authority.

4.5.4 Record of processing activities

Unless the duty is not mandatory under the GDPR, each controller is obliged to keep a record of personal data processing activities under its responsibility. The data should be stored for 5 years after the end of the project closure.

4.5.5 Rights for individuals

The rights for individuals under the GDPR:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict Processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Each controller must ensure that the requirements regarding these rights are met, for example when processing personal data related to participants.

4.5.6 Principles

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of each controller and processor´s approach to processing personal data.

4.5.7 Lawfulness, fairness and transparency

Each controller must identify valid grounds under the GDPR (known as a lawful basis) for collecting and using personal data and ensure that there is not a breach of any other laws while processing the data. Each controller must use personal data in a way that is fair. This means not to use data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. Each controller must be clear, open and honest with individuals from the start about how personal data is processed.

Guidelines (ICO)

Lawfulness

- We have identified an appropriate lawful basis (or bases) for our processing.
- If we are processing special categories of personal data or criminal offence data, we have identified a condition for processing this type of data.
- We do not do anything generally unlawful with personal data.

Fairness

- We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- We only handle individual's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- We do not deceive or mislead individuals when we collect their personal data.

Transparency

- We are open and honest and comply with the transparency obligations of the right to be informed.

4.5.8 Purpose limitation

The controller must from the start decide the purpose of processing is, keep a record of the purpose and specify the purpose in the controller´s privacy information for individuals.

It is only allowed to use the personal data for another purpose if either this is compatible with the original purpose, or the controller needs to acquire the consent again, or there is an obligation or function set out in law.

4.5.9 Data minimisation

The controller must ensure that the personal data that is being processed is adequate, relevant and limited to what is necessary. With "adequate" means that the data processing is sufficient to properly fulfil the defined purpose of the processing (see purpose limitation above). With "relevant" means that the data Processing has a rational link to the defined purpose for the processing. With "limited to what is necessary" means that the controller is not allowed to hold more personal data than is needed for the defined purpose for the Processing.

4.5.10 Accuracy

The Controller should take all reasonable steps to ensure the personal data that is processed is not incorrect or misleading as to any matter of fact and if deemed necessary keep the data updated.

Guidelines (ICO)

- We ensure the accuracy of any personal data we create.
- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep note of any challenges to the accuracy of the personal data.

4.5.11 Storage limitation

The Controller/Processor must not keep personal data for longer than needed.

Guidelines (ICO)

- We know what personal data we hold and why we need it.
- We carefully consider and can justify how long we keep personal data.
- We have a policy with standard retention periods where possible, in line with documentation obligations.
- We regularly review our information and erase or anonymise personal data when we no longer need it.

- We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
- We clearly identify any Personal Data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

4.5.12 Integrity and confidentiality (security)

The Controller must ensure that there are appropriate security measures in place to protect the personal data that is being processed. Security measures means technical and organisational actions. The security measures of personal data include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This means that each controller must have proper security to prevent personal data to accidentally or deliberately be compromised.
The controller must choose employees with relevant professional qualifications providing enough guarantees in terms of technical expertise and personal integrity to ensure such confidentiality.
Note that information security is more than just cybersecurity (the protection of your networks and information systems). It also covers, and therefore requires, other actions like physical and organisational security measures.

Guidelines (ICO)

- We undertake an analysis of the risks presented by our Processing and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of Personal Data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the Personal Data we process.
- We make sure that we can restore access to Personal Data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

Pseudonymisation and Encryption

- Encrypted data transfer through server (SSL).

- Pseudonymisation of personal data for both development, integration, and testing.
- Protective measures against infiltration.
- Physical protection of core parts of systems and access control.
- Logging of systems and mechanisms as well as appropriate auditing of the peripheral components.

Confidentiality

- Access to data is restricted and password protected.
- Access is documented and system controlled with permission and with potential for access removal.
- Anti-virus software protected with automated updates and firewalls usage of systems and solutions.
- Automatically activated and password-protected computer locking.
- Password-protected access to all data and to a limited number of partners.
- Prevention of forced password entry attempts.
- Restriction to account access.
- Logging of all access attempts and those who failed to data storage.
- Separated data handling.

Integrity

- Detailed tracking of accessing and interacting with data (e.g. uploads, changes, versions, access times, etc.).
- Frequent backups to ensure data is not corrupted.
- Ensuring applications and systems involved are regularly updated and properly configured.

Availability and Resilience

- Deletion procedures are established and documented.
- The controller has a clearly defined process of data handling.

Restoring data access

- Documented and regularly tested failover procedures.

4.5.13 Accountability

The accountability principle requires the controller to take responsibility for what is being done to personal data and how the controller demonstrates compliance with the other data protection principles. There must be appropriate measures and records in place to be able to demonstrate such compliance.

Compliance

- We take responsibility for complying with the GDPR, at the highest management. level and throughout our organization.
- We keep evidence of the steps we take to comply with the GDPR.

Technical and organisational measures

- Adopting and implementing data protection policies (where proportionate).
- Taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations.
- Putting written contracts in place with organisations that process Personal Data on our behalf.
- Maintaining documentation of our processing activities.
- Implementing appropriate security measures.
- Recording and, where necessary, reporting personal data breaches.
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.
- Appointing a data protection officer (where necessary).
- Adhering to relevant codes of conduct and signing up to certification schemes (where possible).

4.5.14 Lawful processing

The controller must have a valid lawful basis to process personal data. Before collecting data, the participants have the right to be informed about relevant lawful basis. It is good to know that the GDPR sets out six lawful bases (consent, contract, legal obligation, vital interest, public task, and legitimate interest). At least one must be applicable whenever a controller processes personal data. Most lawful bases require that processing is 'necessary' for a specific purpose. If the controller can reasonably achieve the same purpose without processing, the controller cannot claim to have a lawful basis at hand. The controller must determine which lawful basis is applicable before beginning processing. The decision should be documented.

The lawful bases we need to follow in CIRCUIT are the following:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

4.5.15 Consent

The GDPR sets a high standard for consent. But the controller often may need consent. If consent is difficult, it is recommended to look for a different lawful basis. If the controller deems consent to be the best option for lawful basis, it should be kept in mind that the requirement is strict.

Guidelines (ICO)

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.

- We have made the request for consent prominent and separate from our terms and conditions.
- We ask individuals to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third-party controllers who will be relying on their consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We do not penalise individuals who wish to withdraw consent.

4.5.16 International Transfer of Personal Data

It might be necessary for a controller to transfer personal data to a third country, although it should be avoided if possible. The controller must take special care to ensure compliance with the GDPR before the transfer takes place. The transfer is not allowed if the controller is unable to make the transfer in accordance with GDPR.
The GDPR applies to controllers located in the European Economic Area (EEA) with some exceptions. Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA. On that basis, the GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. A transfer of personal data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.

Guidelines (ICO)

- Q1: Are we planning to make a restricted transfer of Personal Data outside of the EEA?
  - If no, you can make the transfer.
  - If yes go to Q2
- Q2: Do we need to make a restricted transfer of Personal Data in order to meet our purposes?
  - If no, you can make the transfer without any Personal Data.
  - If yes go to Q3
- Q3: Has the EU made an 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver?
  - If yes, you can make the transfer.
  - If no go to Q4
- Q4: Have we put in place one of the 'appropriate safeguards' referred to in the GDPR?
  - If yes, you can make the transfer.
  - If no go to Q5
- Q5: Does an exception provided for in the GDPR apply?
  - If yes, you can make the transfer.
  - If no you cannot make the transfer in accordance with the GDPR.

If we reach the end without finding a provision which permits the restricted transfer, we will be unable to make that restricted transfer in accordance with GDPR.

4.5.17 Data protection impact assessment

A data protection impact assessment (DPIA) is a process to help the controller identify and minimise the data protection risks of a project. The DPIA helps identify the risks, foresee problems and bringing forward solutions. The controller(s) shall conduct a DPIA if the processing is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

In CIRCUIT, in the context of WP7 and specifically Task 7.3: Data Management, the Consortium will issue the DPIA in a cross-cutting level for the project, also addressing specificities of its pilot sites using the template provided in Annex 6 [4] that is designed upon the GDPR principles.
In parallel, there will be an exploration if there is a need that the controller of each site and according to the local processes as mandated by the local DPO is required to perform an additional to that DPIA. This requirement is expected to be mainly associated with the processing of personal data originating from the PDI infrastructure (surveillance systems, digital twins, etc.) of each site. The first issue of DPIA of the project will be reported in D7.3: Data Management Plan for M6. This issue will also report any updates occurring until then regarding the ethics matters of the project. Also, any revisions made in the DPIA template and the ethics related documentation will be also documented therein.

Some basic guidelines for DPIA are as follows:

Guidelines (ICO)

DPIA awareness

- We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- Our existing policies, processes and procedures include references to DPIA requirements.
- We understand the types of processing that require a DPIA and use the screening checklist to identify the need for a DPIA, where necessary.
- We have created and documented a DPIA process.
- We provide training for relevant staff on how to carry out a DPIA.

DPIA screening

- We consider carrying out a DPIA in any major project involving the use of personal data.
- We consider whether to do a DPIA if we plan to carry out any other:
  - 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.
- We always carry out a DPIA if we plan to:
  - use systematic and extensive profiling or automated decision-making to make significant decisions about individuals.
  - 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 of personal 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.
- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- If we decide not to carry out a DPIA, we document our reasons.

DPIA process

- We describe the nature, scope, context and purposes of the processing.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our DPO.
- We check that the processing is necessary for and proportionate to our purposes and describe how we will ensure compliance with data protection principles.
- We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- We identify measures we can put in place to eliminate or reduce high risks.
- We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We implement the measures we identified and integrate them into our project plan.
- We consult the supervisory authority before processing if we cannot mitigate high risks.
- We keep our DPIAs under review and revisit them when necessary.

5 CONCLUSIONS

The current Deliverable provides the Quality Assurance principles, mechanisms and roles of the project, core part of which is the structured peer review process of project Deliverables, the Risk Assessment Methodology and plan of the project as well as the first version of the Ethics manual, tackling also with the key GDPR principles that the project has to abide by.

The Quality Assurance principles will apply in a cross-cutting way and across the full lifespan of the project as is equally the case for the Ethics and GDPR related matters.

Still, updates of the Ethics Manual, as applicable, and the in-depth and progressive elaboration of all data management and protection issues will be reported in the relevant upcoming WP7 Deliverables, as follows:

- D7.3: Data Management Plan (M6)
- D7.4: Data Management Plan – 1st Revision (M18)
- D7.5: Data Management Plan – 2nd Revision (M36)
- D7.6: Data Management Plan – 3rd Revision (M48)

In specific, and apart from the DPIAs conduct that is one of the clear objectives of the above Deliverables, the data protection policy of the project, as enclosed in the current document, will be revisited and be more specific to the project activities as soon as their concise nature and in-depth relation to personal data processing will be acquainted. Data controllers and processors initially identified in the current issue will also be revisited as more in-depth knowledge will be acquired during the project. Also, the ethics profile that will be basically formulated via the use of the Annex 4 checklist will be reported in D7.3 along with any revisited version of all the ethics and data management related tools (Annex 4, Annex 5, Annex 6).

Finally, the project risk assessment will be a continuous living activity, performed on an annual basis and reported in a respective Chapter of the project progress reports. In each annual iteration round, the risk assessment process will reveal the past risks that have been materialised and resolved in the meanwhile.

REFERENCES

[1] FEHRL, "Deliverable D7.1: Project inception report, "CIRCUIT Project (GA 1011042830), 2023
[2] D1.2: AUGMENTED CCAM Project Quality Assurance, Ethics Manual and Risk Assessment Plan, "AUGMENTED CCAM project, GA 101069717
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.
[4] K. Dariusz (2020), "Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process," d.pia.lab Policy Brief, Brussels: VUB, https://doi.org/10.31228/osf.io/7qrfp.

ANNEX 1 – DELIVERABLE TEMPLATE

CIRCUIT -

Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices

– Deliverable 1.1–

Name of the Deliverable

Project reference no.	101104283
Deliverable no:	1.1
Work Package no:	
Status	Draft
Version:	01
Author:	Name, surname (organisation)
Date:	Date Month Year
Nature:	Report
Dissemination level:	Public

	Participant Legal Name	Country
1	FORUM DES LABORATOIRES NATIONAUX EUROPEENS DE RECHERCHE ROUTIERE FEHRLAISBL – FEHRL	Belgium
2	INFRA PLAN KONZALTNIG JDOO ZA USLUGE - INFRA PLAN	Croatia
3	INGEO BV – INGEO BV	The Netherlands
4	ANAS SPA – ANAS	Italy
5	ZAVOD ZA GRADBENISTVO SLOVENIJE – ZAG	Slovenia
6	EUROPEAN UNION ROAD FEDERATION – ERF	Belgium
7	ACCIONA CONSTRUCCION SA – ACCIONA	Spain
8	INSTITUTO ESPAÑOL DEL CEMENTO Y SUS APLICACIONES – IECA	Spain
9	BETON - LUCKO DOO ZA GRADITELJSTVOPROIZVODNJU TRANSPORT I TRGOVINU– BL	Croatia
10	Obcina Crna na Koroskem – CRNA	Slovenia
11	RIGHT-CLICK – RC	Spain
12	UNIVERSIDAD DE CANTABRIA – UC	Spain
13	DIGITALTWIN TECHNOLOGY GMBH – DTT	Germany
14	SVEUCILISTE U ZAGREBU GRADEVINSKI FAKULTET – UNIZAG GF	Croatia
15	Ministerio de Transportes, Movilidad y Agenda Urbana – MITMA	Spain
16	INGEVITY HOLDINGS SRL – NGVT	Belgium
17	ALGORAB – ALGORAB	Italy
18	Hrvatske autoceste d.o.o. – HAC	Croatia
19	Waterschap Hollandse Delta – WSHD	The Netherlands
20	Uberbinder Limited – Uberbinder	United Kingdom

Authors list		
Name, surname	Organisation	email
Reviewer: Name, surname	Organisation	email

Document History			
Version	**Date**	**Comments**	**Author**
V0.1	02/07/2023		Name (organisation)
V0.2	02/07/2023		Name (organisation)
V0.9	02/07/2023		Name (organisation)
V1.0 (/Final; if no peer review is applicable)	02/07/2023	• Version submitted for peer review, if peer review is applicable • Final version towards submission, if no peer review is applicable	Name (organisation)
V2.0 (/Final; if peer review is applicable)	02/07/2023	• Final version towards submission, if peer review is applicable	Name (organisation)

Disclaimer:
CIRCUIT has received funding from the European Union's Horizon research and innovation programme under Grant Agreement No 101104283.
This document reflects only the authors' views. The European Commission and CINEA are not responsible for any use that may be made of the information contained therein.

TABLE DES MATIERES

Aucune entrée de table des matières n'a été trouvée.

ANNEX 2 – PEER REVIEW PLAN

Del. ID	Deliverable name	WP ID	Lead Author	Delivery date	Standard QCB members	1st additional reviewer	2nd additional reviewer
D1.1	Holistic circularity framework	WP1	INFRA PLAN	M10	ACCIONA, FEHRL	UC	DTT
D1.2	Up-stream and down-stream supply-chain actors needs	WP1	IECA	M12	INFRAPLAN, ACCIONA, FEHRL	INGEO	NGVT
D1.3	Circularity analytics tool	WP1	INFRA PLAN	M18	ACCIONA, FEHRL	UC	DTT
D2.1	Digital platform	WP2	DTT	M24	INFRAPLAN, ACCIONA, FEHRL	UNIZAG	UC
D2.2	Digital product passport	WP2	IECA	M36	INFRAPLAN, ACCIONA, FEHRL	BL	DTT
D2.3	Supply – chain matchmaking tool	WP2	DTT	M40	INFRAPLAN, ACCIONA, FEHRL	UC	UNIZAG
D2.4	Real-time traffic management on smart mobility systems	WP2	UC	M24	INFRAPLAN, ACCIONA, FEHRL	ZAG	DTT
D2.5	Transport infrastructure assessment based on the integration of traffic and driving simulators	WP2	UC	M36	INFRAPLAN, ACCIONA, FEHRL	BL	HAC
D3.1	Report on the innovative solutions developed for the	WP3	UC	M36	INFRAPLAN, ACCIONA, FEHRL	UBERBINDER	ZAG

Del. ID	Deliverable name	WP ID	Lead Author	Delivery date	Standard QCB members	1st additional reviewer	2nd additional reviewer
	recycling pillar						
D3.2	Report on the innovative reuse solutions	WP3	ZAG	M30	INFRAPLAN, ACCIONA, FEHRL	UNIZAG	CRNA
D3.3	Report on the developed solutions in the Energy Pillar	WP3	ANAS	M30	INFRAPLAN, ACCIONA, FEHRL	UBERBINDER	ZAG
D4.1	Manual for a successful deployment of GPP in CIRCUIT pilots	WP3	ERF	M16	INFRAPLAN, ACCIONA, FEHRL	ANAS	CRNA
D4.2	Novel Governance models and Innovation and GPP guideline	WP4	ERF	M36	INFRAPLAN, ACCIONA, FEHRL	RIGHT-CLICK	UNIZAG
D4.3	Organisation of the CIRCUIT helpdesk and European Innovation and GPP competition	WP4	FEHRL	M42	INFRAPLAN, ACCIONA, FEHRL	RIGHT-CLICK	NGVT
D5.1	Demo 1: Report on Pilot 1 in Croatia and validation of the digitalization solutions	WP5	INFRA PLAN	M46	INFRAPLAN, ACCIONA, FEHRL	INGEO	ANAS
D5.2	Demo 2: Upscaling and implementation report	WP5	MITMA	M48	INFRAPLAN, ACCIONA, FEHRL	ZAG	BL

Del. ID	Deliverable name	WP ID	Lead Author	Delivery date	Standard QCB members	1st additional reviewer	2nd additional reviewer
D5.3	Demo 3: As-built plans and test report	WP5	INGEO	M48	INFRAPLAN, ACCIONA, FEHRL	HAC	UBERBINDER
D5.4	Demo 4: Slovenian pilot report: Bistra Creek bridge construction	WP5	ZAG	M48	INFRAPLAN, ACCIONA, FEHRL	DTT	NGVT
D5.5	Demo 5: As-built plans and final tests report	WP5	ANAS	M48	INFRAPLAN, ACCIONA, FEHRL	UC	MITMA
D5.6	Impact assessment report	WP5	INFRA PLAN	M48	ACCIONA, FEHRL	NGVT	WSHD
D6.1	Communication strategy, monitoring and materials	WP6	RIGHT-CLICK	M48	INFRAPLAN, ACCIONA, FEHRL	ERF	IECA
D6.2	CIRCUIT Dissemination & Exploitation Plan	WP6	FEHRL	M4	INFRAPLAN, ACCIONA, FEHRL	ALGORAB	ERF
D6.3	CIRCUIT Final Dissemination & Exploitation Plan	WP6	RIGHT-CLICK	M48	INFRAPLAN, ACCIONA, FEHRL	BL	ZAG
D6.4	CIRCUIT Guidelines and replication strategy	WP6	ERF	M48	INFRAPLAN, ACCIONA, FEHRL	INGEO	RIGHT-CLICK
D6.5	CIRCUIT Dissemination & Exploitation Plan – 1st update	WP6	RIGHT-CLICK	M18	INFRAPLAN, ACCIONA, FEHRL	BL	ERF

Del. ID	Deliverable name	WP ID	Lead Author	Delivery date	Standard QCB members	1st additional reviewer	2nd additional reviewer
D7.1	Project inception report	WP7	FEHRL	M2	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A
D7.2	Project Quality Assurance, Ethics Manual and Risk Assessment Plan	WP7	FEHRL	M3	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A
D7.3	Data Management Plan	WP7	FEHRL	M6	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A
D7.4	Data Management Plan 1st rev.	WP7	FEHRL	M18	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A
D7.5	Data Management Plan 2nd rev.	WP7	FEHRL	M36	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A
D7.6	Data Management Plan 3rd rev.	WP7	FEHRL	M48	INFRAPLAN, ACCIONA, FEHRL	N/A	N/A

Partner no.	Short name	Number of Dels to review
1	*FEHRL (Coordinator)*	*25*
2	INFRA PLAN	25
3	INGEO BV	3
4	ANAS	2
5	ZAG	5
6	ERF	3
7	ACCIONA	25
8	IECA	1

Partner no.	Short name	Number of Dels to review
9	BL	5
10	CRNA	2
11	RIGHT-CLICK	4
12	UC	5
13	DTT	5
14	UNIZAG GF	4
15	MITMA	1
16	NGVT	3
17	ALGORAB	1
18	HAC	2
19	WSHD	1
20	UBERBINDER	3

ANNEX 3 – MEETING AGENDA TEMPLATE

- CIRCUIT -

Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices

– Title of the –

Time and place

Project details		
Time	**Item**	**Who**

Font : Century Gothic

Title 1

Subtitle

Text

TABLE OF CONTENTS

Aucune entrée de table des matières n'a été trouvée.

ANNEX 4 – ETHICS CHECKLIST TOOL

Name of the investigator responsible for this project

- Name:
- Email address:

Ethics Checklist	
Question item	**Answer & Justification**
Who is conducting the pilots?	
Title of the study?	
What is the purpose of this research study?	
Who can take part in this study?	
Why should a person consider joining this study?	
If a person joined the study, can he/she change his/her my mind and drop out before it ends?	
What exactly will be done to with a person, and what kinds of treatments or procedures will he/she receive?	
What kinds of harm can a person experience in this study, and what will the investigators do to reduce the risk of harm?	
What will the investigators do to make sure that the information collected on persons will not get in wrong hands?	
What kinds of benefits can a person expect from taking part in this study?	
What kinds of benefit to others can come out of this study?	
Will the persons get paid for taking part in this study?	
Will the person(s) health insurance company be charged for any of the costs of this study?	
What can a person do if he/she wants to find out more about the study, or to complain about the way he/she is treated?	
Will personal data be shared with any other partner of third party?	
What will happen to any information given by a person and how will it be stored?	
How long will personal information be stored?	
Will the data possibly be commercially exploited?	
Has the CIRCUIT data protection policy been consulted?	
Is there any obligation to conduct a DPIA?	

Questions about the ethics procedure	Please indicate as necessary	
Is there a need for ethical approval?	Yes	No
If yes, has it been approved?	Yes	No
If yes, has it been documented and communicated to the consortium?	Yes	No
Is the proposed research adequately designed, so that it will be of informational value?	Yes	No
Does the research pose risks of physical or psychological harm to participants by using deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?	Yes	No
If risks exist, does the research adequately control these risks by including procedures, such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	Yes	No
Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?	Yes	No
Have I, as part of the project, informed the Ethics Board about the ethical issues I have identified and of which I am aware?	Yes	No

ANNEX 5 – QUESTIONNAIRE ON ETHICAL AND LEGAL ISSUES

This questionnaire on ethical and legal issues is to be filled in by the LERs (Local Ethics Representatives), responsible for supervising, from the ethics compliance point of view, the pilot trials involving human participants. It is a checklist reminding the researcher to consider all relevant ethical aspects, as they are delineated in the ethics manual of CIRCUIT Deliverable 7.2 (Chapter 4), before planning and then after conducting any data collection activities within CIRCUIT. The questionnaire is divided into the following subsections: Informed consent, Ethical control instruments, Privacy, Safety, Risk assessment and Reimbursement.

A) Participants and informed consent

1. **Are you (so far) obliged according to national / European regulation to obtain the consent of pilot activities participants?**

❑Yes ❑ No

If ***yes***, briefly explain which specific aspects of trials you currently obtain informed consent for:

_____

2. **Do you intend to conduct pilots in CIRCUIT with individuals who might not understand the informed consent forms that will be used in CIRCUIT?**

❑Yes ❑ No

If ***yes***, briefly explain the procedures you currently follow in order to obtain informed consent in such cases:

_____

3. **Is there is any doubt about the anticipated CIRCUIT pilot trials individuals' cognitive capacity to consent (if known already)?**

❑Yes ❑ No

If ***Yes***, please clarify who will provide consent in such instance:

_____

4. **a) Will the informed consent, provided in common language, be understood by "the man/woman in the street" (or layperson)?**

❑Yes ❑ No

If ***no***, why not?

_____

b) Will the participant be given sufficient time to reflect on their decision of providing consent?

❑Yes ❑ No

If ***no***, why not? Please indicate the time to be given to the participant.

_____

5. **Do you believe that any of the participants will be unable to consent in any way for any reason?**

❑Yes ❑ No
If ***yes***, **no experiment should be performed since these participants are excluded from CIRCUIT trials. Please list here each excluded case.**
_____

6. **Do you believe that there will be participants, for any reason, unable to read the form by themselves (there is a range of people who are unable to read the consent form; these include those who have severe visual impairments, e.g. cataract, glaucoma, but perhaps also illiterate and children)?**

❑Yes ❑ No
If ***yes***, be advised that any participant that will not be able to read must give oral consent which has to be witnessed at least by one person. If that will be the case, please ensure that you will record the name of the witness when recording the individual's grant of consent.

7. **Do you believe that there will be illiterate participants?**

❑Yes ❑ No
If ***yes***, be advised that an illiterate participant has to give oral consent which has to be witnessed at least by one person. If that is the case, please name the witness (in case of controlled trials):

8. **Has the oral consent of an illiterate participant been given in the presence of a witness, in accordance with your national legislation (and/or institutional protocols, if any)?**

❑Yes ❑ No

9. **Is there an international or national legislation, which you must follow when performing tests within CIRCUIT project?**

a) involving healthy human participants?
❑Yes ❑ No
If ***Yes***, please give details (reference number and short description of how you will assure compliance):
_____

b) involving participants with cognitive impairments / learning difficulties?
❑Yes ❑ No
If ***Yes***, please give details (reference number and short description of how you will assure compliance):
_____

c) involving *illiterate* or *with co-morbid conditions* participants?
❑Yes ❑ No
If ***Yes***, please give details (reference number and short description of how you will assure compliance):
_____

d) involving *children*?
❑Yes ❑ No
If ***Yes***, please give details (reference number and short description of how you will assure compliance):
_____

B) Ethical control instruments

10. Is there a local ethics controlling committee or controlling body (on national/regional/local/institutional level) from which your organisation will be obliged to get approval for the experimental procedures before beginning with the experiment, and how will you obtain this approval?

❑Yes ❑ No
If ***Yes,*** will you **obtain this approval?**
❑Yes ❑ No
If ***Yes,*** please give details of the relevant body and shortly describe the specific procedure:
If ***No***, please explain what is your current practice respectively:
_____

11. At which level of your organization / enterprise, *ethical controls* are audited?
❑ laboratory or workgroup
❑ division or department
❑ institution
❑ regional
❑ national

12. If there is an established ethical control procedure which you must follow before performing tests, please explain how you will assure compliance when performing tests with:
a) healthy participants:
b) participants with cognitive impairments/ learning difficulties:
c) illiterate or with co-morbid conditions participants:
d) children:
_____

C) Privacy

13. What personal data of pilot participants will be recorded as part of the trials? Please list them here and explain how they will be recorded:
_____

14. Is there any Data Protection Authority on national/regional level?

❑Yes ❑ No
If Yes, please provide its name and url to it (if any):
_____

15. If there is an established Data Protection Authority issuing procedures / standards you must follow before performing tests with human participants and their personal data:

a) Please state if they are applicable for CIRCUIT trials:

❑Yes ❑ No

b) If *Yes* above, please explain here how you will assure compliance (according to current practice):

c) If *Yes* above, please give a url to them (if any) and provide a short summary of them:

d) If *No above*, explain why they are not applicable in CIRCUIT case and how you plan to deal with data protection issues (according to current practice):

_____

16. If there is an appointed Data Protection Officer at your organization, please share here the contact details (name, position, e-mail) of that person:

_____

17. If there is not an appointed Data Protection Officer at your organisation, please explain why it is the case:

_____

18. Will you follow or are you aware of any official national or international guidelines on protecting privacy?

❑Yes ❑ No

If ***Yes***, please give a brief outline and provide references:

_____

19. Do you intend to clarify to the CIRCUIT participants that all data collected in the activities they are participating in will be kept entirely confidential and that their anonymity will be protected in full?

❑Yes ❑ No

20. Will you identify persons (in your entity) and their professions/positions who are authorised to have access to the data collected and / or who have access to any data storage devices, both, paper-based and digitally?

❑Yes ❑ No

If *Yes*, please give a list of those persons contact details (names, position, e-mails):

If *No*, please explain why you are not doing so:

_____

D) Safety

21. Will you provide information to the CIRCUIT participants about any participant's illness that is detected (if relevant)?

❑Yes ❑ No

22. Will the pilot implementation at your site be evaluated for any side-effects?
❑Yes ❑ No
If ***Yes***, please give a brief outline of it:

23. Will you have written procedures for safety for employees and volunteers within your own group or institution?
❑Yes ❑ No
If ***Yes***, please give a brief outline of it:
If ***No***, please explain the reasons briefly or what corrective actions you take:

_____

E) <u>Risk assessment</u>
24. Will you perform a risk-assessment concerning breach of privacy and / or breach of safety at your site?
❑Yes ❑ No
If ***Yes***, please give a brief outline of it:
If ***No***, please explain the reasons briefly refer to any corrective actions you will take:
_____

25. Is your organisation insured against risks as a result of breach of privacy and safety?
❑Yes ❑ No
If ***Yes***, please give a brief outline of it and state the insurer, if possible:
If ***No***, please explain the reasons briefly and state who would cover any insurance-related costs:

_____

26. For conducting research and manage the risk, do you need to involve other organisations (entity, unit, division, department, etc.) that might influence your research activities and/or your ethical and legal conduct?
❑Yes ❑ No
If ***Yes***, please give a brief outline of it:

_____

F) Reimbursement
27. Are reimbursement practices allowed in your country/region/institution?
❑Yes ❑ No

28. If *Yes*, will financial / in kind payments (including reasonable expenses and compensation for time of participation) be offered to participants for participating to your demonstration trials in the context of CIRCUIT (applicable only for pre-demonstration phase or in-depth controlled trials part of final demonstration phase)?
Another factor that may cloud the judgement of a potential participant when deciding whether or not to participate in research is whether money or payments in kind (e.g. gift vouchers) will be offered. It is reasonable for expenses and compensation of time to be offered. However these should not be so large that a participant is more concerned

about what s/he will be receiving rather than the risks involved with the research. If children are involved, then the researchers might consider the fact that what an adult considers to be a reasonable expense/compensation might be very different from a child's perspective (i.e. a child may consider 10 Euros to be a huge reward and, therefore, the 10 Euros might unduly influence a child's decision as regards whether or not to participate).

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

_____

ANNEX 6 – DPIA TEMPLATE

COVER PAGE

CIRCUIT	
Name, contact details and other identifying details of:	
border control authority deploying the initiative	
data controller(s)	
data processor(s), if applicable	
person(s) in charge of the initiative	
assessor(s)	
data protection officer(s) (DPO), if appointed	
chief information security officer, if appointed	
quality control body supervising the assessment process, if appointed	
data protection authority/ies (DPA)	
research ethics committees at public or private organisations	
national ethics committees or councils	
groups of *ad hoc* recruited ethics experts	
anyone else involved, as practicable	
Version of the assessment report	
Level of confidentiality of the assessment report	□ Public □ Confidential □ Specific [explain]
Date and place of compilation of the report	

Executive summary

[Summarize the most significant information concerning the outcomes of each step of the integrated impact assessment process.]

Phase I: Preparation of the assessment process

Step 1: Screening (threshold analysis)

Step 1a: Preliminary description of the envisaged initiative

Overview of data protection aspects	***Contextual description***	**What?**	
		How much/how many?	
		Where?	
		Why?	
	Technical description	Overview of personal data and processing operations	
		Infrastructure	
		Actors	
Overview of privacy aspects			
Overview of ethical aspects			
Overview of social acceptance aspects			
[other, explain]			

Step 1ba: Personal data protection screening (threshold analysis)

Positive criteria	***Legal provision***	***Applicable?***	***Explanation***
Criterion 1: The envisaged processing operations are likely to result in a high risk to the rights and freedoms of natural persons (general)	35(1)	☐	
Criterion 2: Processing operations deemed highly risky			
2a. Processing operations entailing 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	35(3)(a)	☐	

Positive criteria	*Legal provision*	*Applicable?*	*Explanation*
concerning the natural person or similarly significantly affect the natural person			
2b. Processing operations regarding special categories of data, or personal data relating to criminal convictions and offences on a large scale	35(3)(b)	☐	
2c. Processing operations entail a systematic monitoring of a publicly accessible area on a large scale	35(3)(c)	☐	
Criterion 3: Processing operations included in the public list of processing operations that require a data protection impact assessment compiled by the DPA(s) to which jurisdiction(s) the data controller is subject	35(4)	☐	
Criterion 3bis: Processing operations that require a DPIA as included in a code of conduct to which the data controller is subject	40	☐	
[other, cf.* Step 2a: Benchmark*; explain]		☐	
DECISION		☐	**required**
		☐	**not required**
Negative criteria	*Legal provision*	*Applicable?*	***Explanation***
Criterion 4: Processing operations included in the public list of processing operations that DO NOT require a data protection impact assessment compiled by the DPA(s) to which jurisdiction(s) the data controller is subject	35(5)	☐	

Positive criteria	*Legal provision*	*Applicable?*	*Explanation*
Criterion 5: Whereas the legal basis for the processing operations is the compliance with a legal obligation to which the controller is subject or the performance of a task carried out in the public interest, on the basis of EU or member state's law, and an impact assessment satisfying the conditions of DPIA under the GDPR has already been performed	35(10)	☐	
Criterion 6: Processing operations concerning personal data from patients or clients performed by an individual physician, other health care professional or lawyer	Recital 91	☐	
Criterion 6bis: Processing operations exempted from a DPIA by a code of conduct to which the data controller is subject	40	☐	
[other, cf.* Step 2a: Benchmark*; explain]		☐	
DECISION		☐	**exempted**
		☐	**not exempted**

Step 2: Scoping
Step 2a: Benchmark
Personal data protection

Applicable laws and regulations		**Applicable?**	**Explanation**
lex generalis	General Data Protection Regulation (GDPR)	☐	
	National law(s) supplementing/implementing the GDPR	☐	
	National data protection laws (extra-EEA)	☐	
	National exclusion/inclusion list(s) (Art. 35(4)-(5) GDPR)	☐	
	Codes of conduct	☐	

Applicable laws and regulations		Applicable?	Explanation
	Certificates (Art. 42 GDPR)	☐	
	Technical standards	☐	
	Laws from extra-EU jurisdictions	☐	
	[other, general sources for personal data protection, explain]	☐	
by-laws	Data protection policies	☐	
	[other, explain]	☐	

Scope of the assessment process			Applicable?	Explanation
Personal data protection principles		Art. 5	☐	
Legal basis for processing		Art. 6	☐	
Data subject rights		Art. 15-22	☐	
Obligations of data controller and processor		Art. 24-39	☐	
Data transfers outside EU/EEA		Art. 46	☐	
Specific processing situations		Art. 85-91	☐	
Other fundamental rights	Private and family life, home and communications	Recital 4	☐	
	Freedom of thought, conscience and religion		☐	
	Freedom of expression and information		☐	

Scope of the assessment process		Applicable?	Explanation
	Freedom to conduct business	☐	
	Right to an effective remedy and to a fair trial	☐	
	Cultural, religious and linguistic diversity	☐	
[other, explain]		☐	

Step 3: Planning and Preparation

Specific objectives of the assessment process

Objective	Applicable?	Explanation
Protection of individuals	☐	
Compliance with the law	☐	
[other, specify]	☐	

Criteria for the acceptability of negative impacts

Objective		Applicable?	Explanation
Necessity and proportionality (Article 35(7)(b))		☐	
Human rights limitation criteria (Article 52(1) CFR)		☐	
Risk assessment (qualitative, quantitative) (risk criteria)	Likelihood scale	☐	
	Severity scale	☐	
	Point of acceptability	☐	

[other, specify]	☐	

Phase II: Assessment

Step 4: Systematic (detailed) description of the initiative

A succinct description of the envisaged initiative

[Explanation]

Personal data protection

			Explanation
Contextual description	**Nature** *(what types of processing operations? e.g. collection, storage, erasure, etc.)*		***1***
			2
			…
	Scope	**Scale** *(how much? how many? how far?)*	
		Time *(when? how long?)*	
	Context *(in what circumstances?)*	**Internal** *(concerning the controller)*	
		External *(concerning individuals, groups, society, etc.)*	
	Purpose of processing operations, including, where applicable, legitimate interest (why?)		
	Benefits of processing operations	for individuals, including data subjects	
		for the data controller	
		for society as a whole	

	Drawbacks of processing operations	for individuals, including data subjects	
		for the data controller	
		for society as a whole	
Technical description	Categories of personal data (what?) special categories of personal data personal data of vulnerable people (e.g. children) data of a highly personal nature		
	Means of processing (infrastructure) (by what means?)		
	Envisioned data flows (where to where? whom to whom?)		
	Data security (how is it ensured?)		
	Jurisdiction/market (where?)		
	Actors in the 'supply chain' (who?)		
	[Other, explain]		

Diagram of personal data flows and/or other visualisations

[Insert a diagram]

Step 5: Appraisal of Impacts & Step 6: Recommendations
Step 5aa: Data protection: Necessity and proportionality of the processing operations
Personal data protection principles

		ID of a processing operation **Type of a processing operation**	
Step 5 Appraisal of impacts		**Step 6 Recommendations**	

Principle		Legal provision	Applicable?	Satisfied?	Explanation		Response plan, if principle not satisfied: Measures in place	Measures to introduce	Responsible person	Priority	Deadline
Lawfulness	Consent	6(1)(a)	☐	☐							
	Contract	6(1)(b)	☐	☐							
	Legal compliance	6(1)(c)	☐	☐							
	Vital interests	6(1)(d)	☐	☐							
	Public interest	6(1)(e)	☐	☐							
	Legitimate interests	**6(1)(f)**	☐	☐							

Principle		Legal provision	Applicable?	Satisfied?	Explanation		Response plan, if principle not satisfied: Measures in place	Measures to introduce	Responsible person	Priority	Deadline
Fairness Transparency		5(1)(a)	☐	☐							
			☐	☐							
Purpose limitation	Specific	5(1)(b)	☐	☐							
	Explicit		☐	☐							
	Legitimate		☐	☐							
	Not processed further		☐	☐							
	(Exceptions)	89(1)	☐	☐							
Data minimisation	Adequate	5(1)(c)	☐	☐							
	Relevant		☐	☐							
	Limited		☐	☐							
Accuracy	Accurate	5(1)(d)	☐	☐							
	Up-to-date		☐	☐							
Storage	Necessar	5(1)(	☐	☐							

Principle		Legal provision	Applicable?	Satisfied?	Explanation		Response plan, if principle not satisfied: Measures in place	Measures to introduce	Responsible person	Priority	Deadline
limitation	y	e)									
	(Exceptions)	89(1)	☐	☐							
Data security	Integrity and confidentiality	5(1)(f)	☐	☐							
	Security of processing	32	☐	☐							
Data protection by design		25(1)	☐	☐							
Data protection by default		**25(2)**	☐	☐							

Step 5ab: Data protection: Risk to the rights and freedoms of natural persons

STEP 5 APPRAISAL OF IMPACTS **STEP 6 RECOMMENDATIONS**

RISK IDENTIFICATION			RISK ANALYSIS				RISK EVALUATION										
							Risk response					*Response plan*					
ID	Risk	*Description (risk source, risk owner, etc.)*	Likelihood [probability] of occurrence L[P]	Severity of conseauence(s) if risk S	Risk level (score) R = L[P] * S	Explanation	Type	Description	*Revised risk level (score) (Any residual risk?)* *L[P]*	*S*	*R*	Measures in place	Measures to introduce	Responsible person	Priority	Deadline
1	*[Specify]*															
2																
3																
4																
5																

Risk matrix

Before recommendations	*After recommendations*
[Insert a diagram]	*[Insert a diagram]*

Phase III: Ex post (eventual) steps

Step 7: Prior Consultation

Data protection	**Competent DPA(s)**	
	Date of submission	
	Date of receipt of the response	
	Inquiry (summary)	
	Response (summary)	
	Decision of the controller after consultation	
Ethics	Ethics committee and/or competent authority	
	Date of submission of application for approval	
	Date of receipt of the response	
	Response (summary)	
	Decision of the sponsoring organisation after consultation	
[other, explain]		

Step 8: Revisiting

	Criterion		Change?	*Explanation*
Contextual description	**Nature** *(what types of processing operations? e.g. collection, storage, erasure, etc.)*		☐	
	Scope	**Scale** *(how much? how many? how far?)*	☐	
		Time *(when? how long?)*	☐	
	Context *(in what circumstances?)*	**Internal** *(concerning the controller)*	☐	
		External *(concerning individuals, groups, society, etc.)*	☐	
	Purpose *of processing operations, including, where applicable, legitimate interest (why?)*		☐	
	Benefits of processing operations	for individuals, including data subjects	☐	
		for the data controller	☐	
		for society as a whole	☐	
	Drawbacks of processing operations	for individuals, including data subjects	☐	
		for the data controller	☐	
		for society as a whole	☐	

	Criterion	Change?	Explanation
Technical description	Categories of personal data (what?) special categories of personal data personal data of vulnerable persons (e.g. children) data of a highly personal nature	☐	
	Means of processing (infrastructure) (by what means?)	☐	
	Envisioned data flows (where to where? whom to whom?)	☐	
	Data security (how is it ensured?)	☐	
	Jurisdiction/market (where?)	☐	
	Actors in the 'supply chain' (who?)	☐	
	[Other, explain]	☐	

Overall suggestion

What should be done with the assessment process?		When?	Decision of the sponsoring organisation and its justification
☐ **revise**	☐ entirely	*[Specify]*	
	☐ in part *[Specify]*	*[Specify]*	
☐ **do not revise**	***[Specify why]***		

Ongoing Steps
Step A: Stakeholder involvement
Internal stakeholders

Category of stakeholder	What information has been communicated to stakeholders?	What input have the stakeholders provided (e.g. opinion)?	How was their input included? Why was it rejected?
Data processor(s)			

Category of stakeholder	*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g. opinion)?*	*How was their input included? Why was it rejected?*
Data protection officer(s) (DPO)			
Recipient(s) (Article 4(9))			
Third parties (Article 4(10))			
Representative(s) (Article 27)			
Information security officer(s)			
Legal service			
Employees, trade unions, contractors, etc.			
[*other, specify*]			

External stakeholders

Category of stakeholder		*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g. opinion)?*	*How was their input included? Why was it rejected?*
Individuals whose rights and freedoms are affected by the initiative and their representatives	Data subjects, including: Minors Vulnerable people *[other, specify]*			
	Representative(s) of data subject(s)			
	Individuals who are not data subjects			
	Representative(s) of individuals who are not data subjects			
Public sector stakeholders	Supervisory authority(ies) (DPA)			

Category of stakeholder		*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g. opinion)?*	*How was their input included? Why was it rejected?*
	Policy makers			
	Local stakeholders			
Private sector stakeholders	Technology providers			
	Transportation companies			
Experts	Research Ethics Committees, at public or private organisations			
	National ethics committees or councils, at EU or Member States' level			
	Groups of *ad hoc* recruited ethics experts			
	Scientific experts			
	[Anybody else affected, etc., specify]			

Step B: Quality control

Quality control body	*What feedback was received?*	*How was the feedback implemented? Why was it rejected?*
Data protection officer(s) (DPO)		
Supervisory authority (DPA)		
[Other, specify]		

Step C: Documentation

Attachment			*Confidentiality level*	*Appended?*	*Comments*
Step 1 Step 4	Data protection	Record of processing activities		☐	
				☐	
Step 2		Approved codes of conduct		☐	
		Certificates		☐	
		Binding corporate rules (BCRs)		☐	
		Standard contractual clauses (SCCs)		☐	
		Data protection policies		☐	
		Professional codes of conduct		☐	
		Data sharing agreement(s)	confidential	☐	
Step 3		A copy of a service contract (in the event that the impact assessment is outsourced)		☐	
	Stakeholder involvement	A list of stakeholders to consult and their contact details		☐	
		Stakeholder consultation plan	confidential	☐	
Step 7	Data protection	Request for prior consultation with a supervisory authority		☐	
		Response from a supervisory authority		☐	
		Response from a supervisory authority		☐	
Step A	Stakeholder involvement	Technical briefing(s) for stakeholder consultation		☐	
		Stakeholder consultation (reports)		☐	

Attachment			*Confidentiality level*	*Appended?*	*Comments*
	Data protection	DPO opinion (report)		☐	
[Reports from other evaluation techniques; specify]				☐	
[other, explain]				☐	

Closing Page Endorsements

Responsibility	Name	Remarks	Date	Signature
Assessor(s)				
Data protection officer				
Data controller(s)				
[other, explain]				

ANNEX 7 – ETHICS BOARD

Project Ethics Board (PEB) – Core members		
Role	**Responsible person**	**Email**
Coordinator	Thierry Goger	thierry.goger@fehrl.org
Project Ethics & Legal Manager	Adewole Adesiyun	adewole.adesiyun@fehrl.org
Technical and Innovation managers	Irina Stipanovic Carlos Martin-Portugues Montoliu	irina.stipanovic@infraplan.hr carlos.martinportugues.montoliu@acciona.com

ANNEX 8 – DATA PROCESSING – RECORD KEEPING TEMPLATE

The information presented here is in line with the requirement to maintain data processing records of processing operations, under the GDPR, and is specific to personal data. All data controllers and processors must also keep records of data set descriptions according to the latest Data Management Plan and DPIA process. Where applicable, this information shall be verified by the organizational Data Protection Officer.

i. Data controller

Contact details of the data controller	
Email	
Company address	
Telephone	
Purpose of processing	
Description of categories of data subjects and of the categories of personal data	
Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations	
Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization	
Where possible, the envisaged time limits for erasure of the different categories of data	

Where possible, a general description of the technical and organizational security measures for • the pseudonymisation and encryption of personal data; • the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; • the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident • a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

ii. Data processor

Contact details of the data controller	
Email	
Company address	
Telephone	
Purpose of processing	
Description of categories of data subjects and of the categories of personal data	
Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations	
Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization	

Where possible, the envisaged time limits for erasure of the different categories of data
Where possible, a general description of the technical and organizational security measures for • the pseudonymisation and encryption of personal data; • the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; • the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident • a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

ANNEX 9 – INFORMATION SHEETS FOR OBTAINING VALID CONSENT

A. Informed consent procedure for the participation of humans in the project

The CIRCUIT project and consortium attach a high priority to the ethical conduct of research. The Ethical and Legal Manager together with the Project Coordinator and, as the case maybe, the LEAR and/or the test/study conductors, will explain and make sure that research participants have understood: what the CIRCUIT research is about; what their participation in the project will entail; any risks that may be involved, and; request their written consent through the 'consent form' In the absence of the Ethical and Legal Manager and the Project Coordinator due to geographical distance or language barrier, in particular during the preliminary testing phases taking place before the pilots, the independent role to obtain consent from participants will be carried out by a staff member of the consortium partner, other than the end-user (employer), with sufficient practice or expert knowledge within its organisation to carry out this procedure.

How to obtain informed consent from research participants for the participation in the project?

Prior to any tentative involvement in the test and demonstration, the information to be provided to the participants in the pilot sites should be the following:

- A statement that the study involves research subjects (that is the person deciding to participate in a research study) and an explanation of the purposes of the research.
- The expected duration of the subject's participation.
- A description of the procedures to be followed and of the technology that is going to be tested, and an identification of any procedures which are experimental.
- A statement that participation is voluntary and that they can withdraw at any time, without any negative consequence.
- Information about who is organising and funding the research.
- A description of any reasonably foreseeable risk, discomfort or disadvantages.
- A description of any benefits to the subject or to others which may reasonably be expected from the research avoiding inappropriate expectations.
- A description of rights such as the right to ask questions, the right to opt out (not wishing to participate in the pilot after being duly informed) or the right to withdraw at any time from the research without consequences, as guaranteed by the GDPR and the EU Charter of Fundamental Rights.
- A statement describing the procedures adopted for ensuring data protection/confidentiality/privacy including duration of storage of personal data.
- A description of how incidental findings are handled, that is results that arise that are outside the original purpose for which the test or procedure is being conducted.
- Insurance coverage should be mentioned.

- A reference to whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject.
- An explanation of what will happen with the data or samples at the end of the research period and if the data/ samples are retained or sent/sold to a third party for further research.
- Information about what will happen to the results of the research.

The above information will be provided orally and in written form, through an 'information sheet' and a 'consent form' which will be kept on file.

After conveying the previous information, the Ethical and Legal Manager together with the Project Coordinator, will seek to obtain the consent from the research participants through the signature of the 'consent form' [Articles 4(11) and 7 of the General Data Protection Regulation]. All signed consent forms will be kept on file. In the absence of the Ethical and Legal Manager and the Project Coordinator due to geographical distance or language barrier, in particular during the preliminary testing phases taking place before the pilots, the independent role to obtain consent from participants will be carried out by a staff member of a partner of the consortium, other than the pilot site leader, with sufficient practice or expert knowledge within its organisation to carry out this procedure.

*** *** ***

B. Consent form to participate in CIRCUIT research

The CIRCUIT Project Consortium attaches a high priority to the ethical conduct of research. We therefore ask you to consider the following points before signing this form which will act as a written record of your consent. For further queries in relation to your participation you can contact the project's Legal and Ethical Manager (LEM) Adewole Adesiyun [email: adewole.adesiyun@fehrl.org] or [name of the responsible person for organising the respective pilot/research/study].

I, undersigned [name + last name] [contact details: email address or phone], declare that:

1. Have been informed that the CIRCUIT project (Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices), with Grant Agreement Number: 101104283 run under the European Union Horizon programme (HORIZON-CL5-2022-D6-02) and authorized by the European Climate, Infrastructure and Environment Executive Agency. The Project Coordinator is FEHRL (FORUM DES LABORATOIRES NATIONAUX EUROPEENS DE RECHERCHE ROUTIERE FEHRLAISBL), Belgium ("Coordinator").

2. Have been informed about the purposes of the Project. I have had all my questions answered to my satisfaction.

3. Have been informed that I can address any ethical questions or concerns arising from this research to the Project Ethics Board by means of contacting the Project Coordinator or the pilot site leader.

4. My participation in the research will include [describe in a sufficient detail the personal data processing]. Information obtained during the research will be used by members of the CIRCUIT research consortium for research purposes and by the European Commission in the context of the CIRCUIT project. The data controller guarantees that:

a. All personal data will be processed in line with European and national data protection law.

b. All personal data will be kept securely and stored no longer than necessary for the purposes for which it was collected subjected to appropriate safeguards, such as pseudonymisation.

c. All personal data will be destroyed once it is no longer needed for the research purposes.

d. It will be made available only to the members of the CIRCUIT Research Consortium and subcontractors and to the European Commission.

5. Understand that no further use of my personal data in the course of the project is foreseen.

6. [Require/do not require my participation to remain anonymous, i.e. all possible efforts would be made to prevent the identification of myself and I will not be identified in any research results.]

7. Understand [I will / I will not] be paid for my participation.

8. Give this consent fully informed, freely and voluntarily and understand that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences. I can also request the deletion of any personal data that may pertain to me. Such a request may be made without any consequences or penalties in return.

9. The relevant laws of [country] shall apply.

Therefore, I hereby consent to take part in the research carried out by the CIRCUIT Research Consortium.

AUDIO/VIDEO/SENSOR CONSENT:

I do not allow / I allow the recording of images and audio-visual content for research and scientific publication purposes. I understand that the content might be used for scientific publication, video explanations of the experiment and research dissemination but will NOT be used for any commercial purposes. [please strike bar what is not applicable].

I allow my face image to be disclosed / I understand that my face image will be blurred [please strike bar what is not applicable]

I allow /I do not allow the use of wearable devices (sensors) for research purposes. [please strike bar what is not applicable]

Participant Signature: .....

Name: .....

Date: .....

I confirm, for the project team, my agreement to participate in this research study.

COMMITMENT FORM OF RESEARCH AND SIGNATURE:

I certify having explained the subject the terms of the present form of consent, having answered to his/her questions related to the experiment, having clearly stated that he/she can retire from the experiment at any time, and that he/she will receive a signed copy of this formulary.

Researcher Signature: .....

Name: .....

Date: .....

Organisation: .....

*** *** ***

C. Consent form for dissemination purposes

Request on behalf of the Consortium

Dear participant,

We would like to ask for your consent to take photographs and videos of you during […], to be held on […], at […].

The photos/videos taken during the event may be:

- used as record of the activity or the event;
- inserted in a report of the activity or event that will be viewed by CIRCUIT partner organisations and by the European Commission as co-founder of the project;
- inserted in material for further activities or events that are compatible with the nature and the scope of CIRCUIT activities;
- inserted in the project website and leaflets, articles published in popular media and/or academic articles.

The processing of your image will take place in accordance with the EU General Data Protection Regulation (GDPR). This means, inter alia, that your picture will not be sent to third parties or posted in social media, with the exception of the project's own social media channels and solely for the purpose of dissemination. You have the right to refuse to be photographed and do not sign the consent form below. In this case, you will still be able to participate in the activity and we will not use your image. You have the right to ask, at any time, the deletion of pictures that make you identifiable. This request should be forwarded to:

[…].

I hereby irrevocably grant each CIRCUIT consortium member, jointly, together with each of their successors, assigns and licensees, all consents necessary, to all usage of the photographs, films and voice recordings, in perpetuity, on a royalty-free basis, throughout the world and at each CIRCUIT consortium member's discretion, to exhibit, edit, distribute, sell, lease and exploit the photographs, films and voice recordings, for use in the CIRCUIT project and related research, publications, presentations, exhibitions, conferences, marketing and advertising materials and for any publicity and promotions relating thereto and for any commercial or non-commercial purposes in all and any media (whether now existing or yet to be invented), including, without limitation, in each CIRCUIT consortium member's online and hard copy materials relating to the CIRCUIT project.

I waive any and all moral rights in the photographs, films and voice recordings, to which I might be entitled in any country and hereby assign with full title guarantee to each CIRCUIT consortium member, jointly, all present and future copyright and any other rights in the photographs, films and voice recordings, throughout the world, for the full period of copyright. I agree and understand that the CIRCUIT consortium members are not obliged to take, use, keep or exploit the photographs, films or voice recordings, nor shall they be obliged to: (a) provide a credit or acknowledgment to me in any way when

exploiting the photographs, films and/or voice recordings; or (b) submit the photographs, films, voice recordings or any other materials relating to the CIRCUIT project to me for any approvals.

None of the CIRCUIT consortium members shall be liable to me for any distortion or illusionary effect or adverse result to myself resulting from the publication or other use of the photographs, films and/or voice recordings. I acknowledge that each CIRCUIT consortium member shall store copies of the photographs, films and voice recordings for the purpose and/or store my contact details on their databases in case they need to contact me. Any such use of my personal information shall be in accordance with the terms of the CIRCUIT data protection policy.

Declaration of consent

I, undersigned [name + last name] [contact details: email address or phone], declare that:

Have been informed that the CIRCUIT project (Holistic approach to foster CIRCUlar and resilient transport InfrasTructures and support the deployment of Green and Innovation Public Procurement and innovative engineering practices), with Grant Agreement Number: 101104283 run under the European Union Horizon programme (HORIZON-CL5-2022-D6-02-06) and authorized by the European Climate, Infrastructure and Environment Executive Agency. The Project Coordinator is FEHRL (FORUM DES LABORATOIRES NATIONAUX EUROPEENS DE RECHERCHE ROUTIERE FEHRLAISBL), Belgium ("Coordinator").

Have been informed about the purposes of the project and have had all my questions answered to my satisfaction.

Have been informed that I can also address any ethical questions or concerns arising from this research to the Legal and Ethical Manager, Nikolaos Ioannidis (email: Nikolaos.Ioannidis@vub.be).

Confirm that I possess all rights necessary to grant this permission for and in connection with the purpose.

Confirm that I am voluntarily giving consent and have been informed that I can at any time request that my picture is deleted.

This media release is governed in accordance with the European General Data Protection Regulation (GDPR). Therefore, I hereby give my consent to the CIRCUIT Research Consortium Project to:

- Record my participation and appearance on digital photography and video.
- Use my image taken in connection with this event only in or for CIRCUIT written, electronic and web publications, including the project's social media dissemination purpose.
- Reproduce my image in print, electronic or any other medium, in academic publications and in popular media exclusively for purposes compatible with CIRCUIT core activities.

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

Participant Signature: .....

Name: .....

Date: .....

Researcher Signature: .....

Name: .....

Date: .....

Organisation: .....

*** *** ***

D. Informed consent procedure in connection to data processing according with the GDPR

How to obtain informed consent from research participants (to the test sites) according with the General Data Protection Regulation (GDPR)?

1. The Ethical and Legal Manager together with the Project Coordinator, will seek to obtain the consent from the research participants through the signature of the 'consent form' (Articles 4(11) and 7 of the GDPR). All signed consent forms will be kept on file. In the absence of the Ethical and Legal Manager and the Project Coordinator due to geographical distance or language barrier, in particular during the preliminary testing phases taking place before the pilots, the independent role to obtain consent from research participants will be carried out by a staff member of the consortium partner, other than the pilot site leader, with sufficient practice or expert knowledge within its organisation to carry out this procedure.

2. The consent is 'informed' if the data subject is aware of the following:

- the identity of the data controller and, where applicable, the contact details of the DPO.
- the specific purpose(s) of the processing for which the personal data will be used, and that the data will be shared with research partners for research purposes. In case of secondary use, that is for projects or purposes other than the present research, the data subjects must be given the opportunity to opt out of the further processing operation(s). In case of significant changes to the methodology or processing arrangements having a bearing on the data subjects' rights or the use of their data, data subjects will be made aware of the intended changes, and their express consent sought.
- the subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority.
- information as to whether data might be shared with or transferred to the relevant European Commission services and to the national data protection supervisory authority for contractual and legal purposes.
- how long the data will be retained before being destroyed.
- any potential risks to the data subjects' rights and freedoms.
- the personal data gathered and processed within and for the purposes of the project will not be disclosed to anybody nor any entity outside the consortium.

3. Workers' personal data will be safeguarded as follows:

- No unnecessary data collection activities will be performed (data minimisation).

- Personal data that have been collected for analysis will be handled discretely and with anonymity.
- No personal data will be collected without express authorisation from the research participant.
- Every personal data collected throughout the project will be treated with respect to the protection of fundamental human rights (e.g. separating general and personal data, handling encrypted personal data and identities, erasing irrelevant personal data).
- The participants will be granted with the right to access their personal data.

Template for informed consent for pilot participation

Pilot name: _____ (the "Pilot")

Researching entity: _____

Researching entity's address:_____

Who we are and what is the CIRCUIT project?

The overall objective of CIRCUIT is to develop a holistic approach supported by digital solutions and guidelines to foster the introduction of innovative engineering practices in the whole construction supply/value chain enabling circular, sustainable resilient and smart transport infrastructure and a wider deployment of Green Public and Innovation Procurement. This will be achieved by: i. developing and deploying an innovative open-source digital platform (with advanced Circularity analytics and Supply/value chain matchmaking tools) interoperable with traditional engineering/design (BIM, Digital Twinm LCC, LCA) and traffic simulation tools; ii. introducing modular solutions, ecodesign and reusing concepts as alternative to traditional designs; iii. maximizing the use of biobased, Secondary Raw Materials (SRM) and Secondary Construction Elements (SCE) as alternative to traditional ones; iv. including in the decision-making process of transport infrastructures design and route planning, information from updated traffic simulation tools to reduce incidents, accidents, congestion and future scenarios with autonomous vehicles). New elements and technologies for Circular, Smart, Resilient and Sustainable transport will be included in the design process to facilitate infrastructures upgrading and a quick adaptation to smart mobility and operations. CIRCUIT will also provide knowledge and technical solutions by exploiting the potential of four strategic pillars: Digitalisation, Recycle, Reuse and Energy. Different technologies will be validated in each of the pillars to deliver a holistic approach suitable for different transport modes,

the urban and interurban environment, and the different stages of the life cycle of infrastructures.

As part of the research project, the CIRCUIT consortium will work together to advance the CIRCUIT project. Various Research Partners will conduct pilots to research: [main objective of specific Phase/Round]. By signing the Consent Form below, you agree to participate in the Pilot, as named at the top of this page and detailed below.

What is the purpose of this Pilot?

The purpose of our Pilot is to further the research objectives of the CIRCUIT project, by… [To be completed by the relevant pilot entity before submitting to the users].

Who is conducting the Pilot?

[Please insert details of the pilot entity, insert entity name] is conducting the Pilot as part of CIRCUIT Research Partners. Information collected during the Pilot Personal information collected from you during the pilot will be processed in accordance with our privacy policy, here [insert link].

Who will my personal information be shared with?

We may share information with the EU Commission to assist with the objectives of both the Pilot and the CIRCUIT project. We will not transfer your personal data outside of the EEA. [Please consider whether anyone outside your pilot organisation may be assisting with reviewing/interpreting the data or assisting with the plot conduction.]

What will my participation in the Pilot involve?

[To be inserted by the relevant pilot entity before submitting to the users]. You will be required to take part in testing sessions as part of the Pilot. [Add ONLY if it is relevant: These testing sessions will be audio recorded and filmed to assist us in our research.]

What value can a participant bring to the CIRCUIT project?

[To be inserted by the relevant pilot entity before submitting to the users].

What will happen to any information I give you and how will it be stored?

[To be reviewed and updated in accordance with each pilot's storage process] We will comply with all applicable laws and regulations when it comes to collecting, storing, using and sharing your personal information. Where possible, data will be pseudonymised and stored on a password protected computer. Further information on how we use your personal information can be found in our privacy policy, here [insert link].

How long will you store my personal data for?

We will only keep your personal data for as long as is necessary to assist us in the purposes of our research and for no longer than 5 years. Any data held by us during this period will be stored in accordance with our privacy policy, here [insert link].

Will the data possibly be commercially exploited?

Personal data collected during the pilot will not be commercially exploited.

How long will the Pilot last?

Each pilot entity should [insert the estimated duration of their pilot here before submitting to the users].

Who should I contact in relation to the Pilot?

If you have any queries or complaints relating to the pilot, please contact [Each pilot entity should insert the relevant contact's details here before submitting to the users].

What will happen to the results of the Pilot?

The results of this Pilot will be anonymised. You will not be identifiable by these results. These anonymised results will be used by us and shared with the European Commission at national and international conferences and exhibitions and published in peer-reviewed scientific and academic journals; with a focus on open-access journals.

What are the possible benefits of taking part in the Pilot?

[To be inserted by the relevant pilot entity before submitting to the users – please note that this may be different for each pilot.]

Are there any risks?

[To be inserted by the relevant pilot entity before submitting to the users. Please note that this may be different for each pilot.]

Photographs [add ONLY if relevant/applicable]

During your participation in the Pilot, we would like to photograph the user testing session that you participate in as part of the Pilot, for CIRCUIT research, publications, conferences, exhibitions and CIRCUIT social media activities. For example, we would like to include photographs from pilots to accompany related CIRCUIT social media posts and publicised research. We will only take your photograph if you consent to us doing so by ticking the corresponding box in the Participant Consent Form. If you do not consent, you can still take part in the Pilot, but we will not take your photograph. If you do consent to us taking your photograph, you may withdraw this consent at any time. For further information on how we use and store the photographs that we take during the Pilot, please see our privacy policy, here [insert link].

My rights

You can withdraw from the experiment at any time and without having to give a reason for withdrawing. Please also read CIRCUIT's privacy policy (below) for further information regarding your rights in relation to the personal information we collect about you.

CIRCUIT's Data Protection Policy

Please read our data protection policy which is available [insert link]. Our protection policy contains information about the personal data that we collect from you, and how we collect, store, use and share your personal information. It also sets out your rights to control personal information we hold about you.

Consent Form

Researcher's Name: _____

Participant's Name: _____

Participant's Unique Reference Number: _____

Place of Pilot: _____ _____

This part will be filled in by the participant.

The original will be kept be the Researcher; a copy will be given to the participant.

I confirm that I have read, and I understand the Documentation of Consent form in full and understand the information in relation to this Pilot.	☐
I have had the opportunity to consider the information provided to me and to ask questions about the Pilot and my participation in the Pilot.	☐
I was informed about whom to contact for questions or complaints about the research and my rights.	☐
I understand that other Research Partners will have access to my information.	☐
I have spoken to: Dr./Mr./Ms. ……	☐
I understand that I am free to withdraw from the experiment • at any time; and • without having to give a reason for withdrawing.	☐
I have read CIRCUIT's privacy policy (link to the web), which contains further information about how CIRCUIT Research Partners collect, use and store my personal information and about my rights relating to my personal information.	☐
I voluntarily agree to participate in the Pilot.	☐
I consent to my photograph being taken during the Pilot and for it to be used by CIRCUIT for CIRCUIT research, publications, conferences, exhibitions and CIRCUIT social media activities.	☐

Participant:

Name of Participant: _____

Signature: _____

Date: _____

Researcher:

Name of Researcher: _____

Signature: _____

Date: _____

Thank you for taking part in this pilot.

Your contribution is very much appreciated.

*** *** ***