- 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 7.3–

Data Management 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	Data Management Plan
Work Package	WP7 - Coordination, Management & Ethics
Date of the Document	22/01/2024
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	18-01-2024	Draft 1	Adewole Adesiyun (FEHRL)
1	22-01-2024	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 current document stands for D7.3 – Data Management Plan of the CIRCUIT project, prepared in the context of Task 7.3: Data management. In this document the first summary of the key project data is presented as they are defined at this early stage. Moreover, the first cross-cutting to the project DPIA is performed and presented. Finally, updates to the CIRCUIT Ethics and the Data Privacy Policy are included in this document with regards to their original definition in D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan [1].

There will be three revisions of the Data Management Plan scheduled to be released in months 18, 22 and 48, as D7.4, D7.5 and D7.6 respectively. It is expected that the three versions will provide many updates on the current content included in this deliverable as all the project activities related to the CIRCUIT's data will be at much more advanced stages and the details surrounding their data will be better defined.

TABLE OF CONTENTS

TABLE OF TABLES

1 INTRODUCTION

1.1 PURPOSE AND STRUCTURE OF THE DOCUMENT

The purpose of this Deliverable is to provide the first version of the Data Management Plan of the CIRCUIT project. The Data Management Plan aims to describe the data the Consortium expects to generate or acquire during the lifecycle of CIRCUIT, how this data will be managed, disseminated, analyzed and stored. It also aims to describe the mechanisms that will be used to share those data. It is evident the Data Management Plan is a living document that will be iterated upon as the related project activities advance during the project.

The DMP includes the following Sections:

Section 1 provides the purpose of Deliverable, its intended audience and interrelations with the various activities of the project.

Section 2 provides the CIRCUIT data overview.

Section 3 provides the FAIR data principles and how CIRCUIT is going to implement them.

Section 4 presents the first Data Protection Impact Assessment.

Section 5 provides updates to the Data Privacy Policy, that has also been a subject of discussion firstly in Deliverable 7.2, in regard to the project's official website privacy policy.

Section 6 concludes the Deliverable.

Annex 1 provides the DPIA template and Annex 2 the updated Ethics Questionnaire.

1.2 INTENDED AUDIENCE

The intended audience of this Deliverable is the scientific community. Of course, as the DMP is a public document, it can be of interest to anyone wanting to observe the data scope, progress and expected results of the CIRCUIT project.

1.3 INTERRELATIONS

This Deliverable is related to most of the activities of WPs 1, 2, 3, 4 and 5 as they are related to some extent -some more than others – with data definition, generation, utilization, processing and storage. It is also related to WP7 in the sense that it includes updates to the Ethics and Data Privacy Policies of the CIRCUIT project.

2 CIRCUIT DATA SUMMARY

The following data clusters are identified with regards to the data collection within the project:

- Experimental numerical and imaging data will be collected to be used in the digital platform.

- Textual data will be collected from interviews and discussions with stakeholders in, for instance, industry, public authorities, and end-users (building materials and waste database) – this is required to understand, for example, barriers in legislation, standards, and attitudes to use such materials.
- A combination of textual and numerical data will be collected or generated to evaluate the circular economic feasibility of the value chain and commercial exploitation possibilities of the SRMs and SCEs.
- Personal data which will be processed by partners of the consortium or by external stakeholders during CIRCUIT.
- Other subjective data collected during user surveys and workshops.
- Dissemination data which are the data related to the communication and dissemination of the project's news and results.

3 FAIR DATA PRINCIPLES

3.1 MAKING DATA FINDABLE INCLUDING PROVISIONS FOR METADATA

According to the principle of making data discoverable in CIRCUIT, all the data to be made publicly available (to be specifically defined later in the project) will have rich descriptive metadata which will support findability, citation, and re-use. Standard metadata schemes (e.g. Dublin Core) will be used to provide important context for the interpretation and automated analysis of the data.
Furthermore, all the datasets will have persistent identifiers, like Digital Object Identifiers (DOIs), to facilitate the identification and citation of the data. Those data will be deposited in trusted repositories, like Zenodo, where DOIs will be assigned to them.

3.2 MAKING DATA ACCESSIBLE

Based on the as open as possible, as closed as necessary principle, the consortium will ensure the widest possible dissemination of data/research outputs to facilitate their potential re-use while considering legitimate concerns to restrict data sharing. Such concerns include privacy concerns related to personal data, Intellectual Property concerns such as patents which may require an embargo period before open access and any other sensitive information that will be identified during the project. Complete justification will be provided for the reasons why data/research outputs will not become openly accessible.
The shared data and their associated metadata will be deposited in an Open Data repository, like Zenodo. A Zenodo account will open soon in the coming period to host all datasets that will be agreed to be shared.
In addition, project data – different sets in each case - will be available for sharing and re-use via the dissemination and the management/administration portals of the project. Those portals will be the means for exchanging data either among the partners of the project or between the consortium and third parties.

3.3 MAKING DATA INTEROPERABLE

The produced CIRCUIT data will be made interoperable, meaning that they can be integrated with other data, applications, and workflows, by using common formats and standards, controlled vocabularies, keywords, thesauri, or ontologies where possible. The data files generated will be processed and submitted to the Open Data repositories following standard universal formatting. To that end, metadata vocabularies, standards and methodologies will depend on the repository to be hosted.

3.4 INCREASE DATA RE-USE

To increase re-usability of data and research outputs, the consortium will publish relevant documentation along with data/research outputs to make them comprehensible for third parties. All the information of the generated data will be documented in README files, which will include a) a short description of what data includes; b) for tabular data: definitions of column headings and row labels, data codes and measurement units; c) any data processing steps that may affect interpretation of results; d) a description of what associated datasets are stored elsewhere, if applicable and e) contact information. The data description formal will align with the related GDPR provisions.
Furthermore, the open data/research outputs will be published with clear licenses and data origin information. Creative Commons licenses will enable open access and re-use of data. More specifically, the Attribution (CC BY) license and Creative Commons Zero (CC0) will be used by the CIRCUIT project. Different licenses could be evaluated depending on the case.

4 DATA PRODUCTION IMPACT ASSESSMENT

In this section, the first cross-cutting to the whole CIRCUIT project Data Protection Impact Assessment (DPIA) is prepared and presented. Consequently, the provided version stands as the current and very early version of the project DPIA. Still, DPIA is an evolving process in the project and will be continuously updated when it is needed based on and following the corresponding developments in the project.
In this version of the Data Management Plan we will not be using the DPIA template provided in D7.2 as that version would be more useful for the final revision of the Data Management Plan to be released on month 48 of the CIRCUIT project, when all the exact details of the project's data and processing procedures will be available and agreed upon. Instead since this is the first DPIA performed during the project, we opt to use a higher-level GDPR approved template [3], included in Annex 1 – DPIA template.

4.1 INTRODUCTION

The Data Protection Impact Assessment is required under Article 35 of the GDPR (EU) 2016/679. A PIA is a process which helps assess data protection and privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. For the DPIA in CIRCUIT, we have

followed a respective GDPR compliant template, tailored-down to the needs of the project.
In addition to the GDPR obligation to carry out a DPIA in occasions where the processing of personal data is likely to result in a high risk, we set out below reasons for performing a DPIA.

Why should I do a PIA?	***When should I start a PIA?***
• *To identify privacy risks to individuals.* • *To identify privacy and data protection compliance liabilities for your organisation.* • *To protect your reputation.* • *To instil public trust and confidence in your project/product.* • *To avoid expensive, inadequate "bolt-on" solutions.* • *To inform your communications strategy.*	*DPIAs are most effective when they are started at an early stage of a project, when:* • *the project is being designed;* • *you know what you want to do and how you're going to do it;* • *you know who else is involved.* *But ideally it should be started before:* • *decisions are set in stone;* • *you have procured systems; and* • *you have signed contracts/ MOUs/agreements.*

4.2 IS THERE A NEED FOR A DPIA?

Determining if you need to do a DPIA - screening questions
*Answering yes to **any** of these questions indicates that a DPIA is necessary.*

- Will the project involve the collection of new information about individuals?
  Yes.

- Will the project compel individuals to provide information about themselves?
  In the context of focus groups, workshops, user surveys and interviews, the project will ask information about participants that are not personal. The objective will not be to collect personal information, but rather views on the acceptance of the solutions tested/ experienced. Individuals will be notified of any personal data which is being collected and processed about them, together with further information relating to that processing, in accordance with the GDPR, prior to any such collection/processing. This information will also be available in CIRCUIT's privacy policy. In addition, participants will sign an informed consent, prior to any participation to experiments, where they will be explained about the purpose of the testing activity and the type of data that will be collected during it.

- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
  Any information about individuals will be disclosed only to the defined LER's and persons defined to be granted access. Other organisations and persons, part of the Consortium or not, will not have access to any information relevant to users' profiles, apart from aggregated anonymise datasets of them. Any access to personal data will be in accordance with the GDPR.

- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
  Yes, subjective feedback data will be used for evaluation of the CIRCUIT solutions, which has not happened before.

- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
  No. In case of video or other type of facial recording during any type of tests or activities, users will be/have been asked to complete a consent form. Moreover, no video feeds are planned to be stored in the system and all the information will be processed in real-time.

- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
  No.

- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
  No.

- Will the project require you to contact individuals in ways which they may find intrusive?
  No. In the case that this emerges as an instance and despite all the precautions taken, any user is free to withdraw at any point from the project activity.

4.3 STEP 1: IDENTIFY THE NEED FOR A DPIA

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents. Summarize why you identified the need for a DPIA.
1. Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. *CIRCUIT is a 48 months duration project, funded by the EU's Horizon program. CIRCUIT is a Horizon Europe project (May 2023 – April 2027) aiming 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.*

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents. Summarize why you identified the need for a DPIA.

The project will deliver circular, sustainable resilient and smart transport infrastructure (both at urban and interurban level) and foster wider deployment of GPP and IP. This will be achieved by:

- *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 and Digital Twins tools and with open-source LCC, LCA, traffic simulation tools;*
- *introducing modular solutions, ecodesign and reusing concepts as alternative to traditional designs;*
- *maximizing the use of biobased, Secondary Raw Materials (SRM) and Secondary Construction Elements (SCE) as alternative to traditional ones;*
- *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 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.*

2. **You may find it helpful to link to other relevant documents related to the project, for example a project proposal.**
   Relevant documents are namely the Grant Agreement of the project, all project documentation released so far, but especially D7.1 - Project inception report and D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan.
3. **Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).**
   A PIA is performed in CIRCUIT as among the data that will be collected and processed during validation activities, like user testing, at the pilot sites, personal information might be collected for creating user profiles. Individuals will be notified of any personal data which is being collected and processed about them, together with further information relating to that processing, in accordance with the GDPR, prior to any such collection/processing.

4.4 STEP 2: DESCRIBE THE PROCESSING

Describe the nature of the processing:

1. **How are you collecting, using, storing and deleting data?**

The data collected, used and stored in CIRCUIT are described in section 2 of this document.

2. **What is the source of the data?**

The different sources of data are presented in sections 2. Some additional to those data sources will be questionnaires, survey forms etc.

3. **Will you be sharing data with anyone?**

Sharing purposes of data collected are defined in section 3.

5. **What types of processing identified as likely high risk are involved?**

No high-risk data processing is involved.

Describe the scope of the processing:

1. **What is the nature of the data, and does it include special category or criminal offence data?**

No, it does not include any special category of criminal offence data.

2. **How much data will you be collecting and using?**

Only necessary data will be collected. During the lifetime of the project, various levels of data– system data included-will be collected from users, through user surveys, workshops, all types of tests, focus groups and technical validation activities.

3. **How long will you keep it?**

Any personal data, if collected locally, will be kept in a local database only for the duration of the project trials and will be in any case deleted one month before the end of the project. Access will be granted to LERs and the additional persons defined in this issue. Anonymized/pseudonymized data collected will be kept for 5 years after the end of the project. All other data - apart those adhering to IPR restrictions - will be shared. With regards to the external groups, as GDPR has already been implemented, participants will be able request access to their data even after their participation has been completed, while they can also ask us to delete the data we hold for them at any time.

Describe the context of the processing:

1. **What is the nature of your relationship with the individuals?**

Not all the field trials will require external to the beneficiaries human participants. The users that will participate in the field trials that do need participants will be internal employees of the project testing entities. If the internal pools do not suffice, external to the entities users will be recruited.

2. **How much control will they have?**

As already stated above GDPR will be implemented, participants can request access to their data even after their participation has been completed. They can also ask us to delete the data we hold for them at any time. Users are not under any obligation to share their data. Also, they can withdraw at any time, without prior notice from the trials. All this will be reflected in the informed consent forms they will sign.

3. **Would they expect you to use their data in this way?**

Users are informed about how data are collected, stored, processed, analysed and disseminated. These pieces of information will be provided in the consent form documentation. Data will not be used in any other way than the one denoted therein.

4. **Do they include children or other vulnerable groups?**

Children will not be recruited but older individuals will be included.

5. **Are there prior concerns over this type of processing or security flaws?**

There are no concerns or security flaws that need further consideration during CIRCUIT project.

6. **Is it novel in any way?**

The data collection process followed in the CIRCUIT project is not novel. It is systematic and clear, aiming to accommodate the project needs across all its activities.

7. **What is the current state of technology in this area?**

The SoA related to CIRCUIT is described in D7.1: Project inception report.

8. **Are there any current issues of public concern that you should factor in?**

No public concern related issues exist or are anticipated.

9. **Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?**

Describe the context of the processing:

Data processors are experienced data scientists and engineers. Partners taking up these roles are all trained and hold postgraduate degrees.

4.5 STEP 3: CONSULTATION PROCESS

Consider how to consult with relevant stakeholders:

1. **Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.**

Data from users will be collected during:

- *On-line/Physical Surveys (questionnaire completion - anonymous during data collection)*
- *Workshops and focus groups (anonymously).*

2. **Who else do you need to involve within your organisation?**

The Project Executive Group (PEG), which comprises of the project coordinator, the WP leaders, the Scientific-Technical Manger and the Ethics Manager will be involved. 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.

3. **Do you need to ask your processors to assist?**

No, as of now, but might change through the advancement of the project at later stages.

4. **Do you plan to consult information security experts, or any other experts?**

No.

4.6 STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

Describe compliance and proportionality measures, in particular:

1. **What is your lawful basis for processing?**

- *Data processing will be used for CIRCUIT digital platform which is an explicit goal of the Contract signed with the EC.*
- *A GDPR compliant informed consent procedure to be followed for all participants is provided in and D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan.*

2. **Does the processing actually achieve your purpose?**

Yes.

3. **Is there another way to achieve the same outcome?**

There is no other way to reach the same outcome. We ensure the data of the data subjects is only used for the purposes defined in the project GA and will remain safe and secure. We also aim (as far as possible) to be transparent with how we use data and data subjects always retain the option to withdraw consent.

4. **How will you prevent function creep?**

The technologies developed within the project are solely used for mobility and transportation. There will no widening or change of use till the end of the project.

5. **How will you ensure data quality and data minimisation?**

We are thoroughly considering and outlining the necessary data that we need to achieve our purpose but as we are still very early in the project cycle, not all the exact data are yet well defined and available to the partners of the Consortium. One of the goals of D7.4, and its three coming revisions is exactly this; to identify which are the data that need to be collected in all ends to be able to fulfil the KPI's defined. Overall, our data minimisation policy ensures that the only data collected is adequate, relevant and limited to the project's purpose.

Describe compliance and proportionality measures, in particular:
6. What information will you give individuals? ***User testing:*** *Users are informed about data treatment, storage, types, deletion, etc. as well as about their rights and the whole process in the informed sheet of the consent form. In addition, before any testing takes place, users are informed about the project, its objectives and the pilots (minimum information about the pilots' objectives is provided, to avoid users becoming biased).* **7. How will you help to support their rights? What measures do you take to ensure processors comply?** *The roles of data collectors and processors and their derived obligations are discussed in D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan.*

4.7 STEP 5: IDENTIFY AND ASSESS RISKS

Although at this early stage of the project a formal risk assessment procedure has not happened yet by all the partners regarding privacy and/or breach of safety, a list of potential risks is provided here that needs to be evaluated, complemented and defined in regard to the severity and likelihood of the potential risks.

Table 1 – List of potential data related risks

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk
1	Risk that the security of the data is compromised (i.e. data breach).	Risk that sensitive personal data is lost or stolen or destroyed causing distress or damaga to the data.	Risks of breach of data protection legislation.	*Risk of reputational damage to entity/entities involved and of enforcement action being brought. Risk to delivery of research objectives both current and in the future. Risk of complaints or litigation from affected individuals.*
2	*Risk that due to a data breach, the true identity of a user will be identified.*	*Risk that the real identity of a user will be identified. This means that, for example, the stored locations will be matched with a user and thus the locations of the places s/he most frequently*	*Risk of breach of data privacy legislation.*	*As above.*

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk
		visits (i.e. home, work, etc.) will be identified.		
3	*Risk that personal data is retained for longer than is necessary.*	*Risk that individual's data is held for longer than is required and that security and other organisational methods applied to the personal data lapse.*	*Risk of breach of data protection legislation.*	*As above.*

4.8 STEP 6: IDENTIFY MEASURES TO REDUCE RISK

As already mentioned in the above table, the aforementioned risks, as well as additional risks related to the data produced in the project, will be subject of risk assessment analysis that will take place in the risk assessment activity (WP7). The foreseen analysis will include, in addition to the risk impact assessment, a list of countermeasures to mitigate and/or reduce the identified risks.

4.9 STEP 7: SIGN OFF AND RECORD OUTCOMES

According to the obligations defined in D7.2, whenever and for whichever data controllers and basically processors applicable, the following table will be completed for the above listed measures (of Step 6).

1. **Who has approved the privacy risks involved in the project? What solutions need to be implemented?**

Risk	*Approved solution*	*Approved by*
E.g. Risk 1	*Data will be deleted when it is no longer necessary to retain such data.*	*E.g. Data Protection Officer. Note, if there is no DPO or National Agency responsible for that, the data manager will be responsible for looking into the privacy risks.*

2. **Integrate the PIA outcomes back into the project plan. Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that**

have been approved? Who is the contact for any privacy concerns which may arise in the future?

Overall: For integrating back into the plan, responsible is the Data Manager. For implementing the solutions, depends on who has developed the corresponding part. For contact in the future for the project, should again be the Data Manager.

Action to be taken	*Date for completion of actions*	*Responsibility for action*
Data to be deleted.	*Insert date/description of when.*	*E.g. Data Protection Officer.*

4.10 LOCAL DPIA

The leaders of all the test sites participating in CIRCUIT will be asked to explore along with their local DPOs if there is a necessity for a local DPIA to be performed at their sites and provide a justification as to why there is or there isn't a need for local DPIAs.

5 PRIVACY POLICY

5.1 INTRODUCTION – PRIVACY POLICY TEMPLATE FOR CIRCUIT WEBSITE

This privacy policy for the CIRCUIT PROJECT ("we," "us," or "our"), describes how and why we might collect, store, use, and/or share ("process") your information when you use our services ("Services"), such as when you:

- Visit our website, or any website of ours, including our social media, that links to this privacy policy
- Engage with us in other related ways, including any events organized by the Consortium, subscription in our newsletters or other types of communities to be endorsed by the Consortium during the project.

5.2 WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us. We collect personal information that you voluntarily provide to us when you register on the services, express an interest in obtaining information about us or our products and services, when you participate in activities on the Services, or otherwise when you contact us.

Personal Information provided by you. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal data we collect may include the following: names, email addresses, job titles, usernames, passwords, contact preferences, mailing addresses.

Sensitive Information. We do not process special categories of personal data, and specifically those revealing racial or ethnic origin, political opinions, religious or

philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

When visiting the CIRCUIT website
The IT systems and applications designated for the operation of this website detect, during their ordinary operation, certain data – the transmission of which is implicit in the use of Internet communication protocols – not associated with directly identifiable users. The data collected may include cookies, IP addresses of computers used by users connecting to the site, the URI – Uniform Resource Identifier – addresses of the resources requested, the time of the request, the method used to send the request to the server, the size of the file obtained in response, the numerical code indicating the status of the response from the server (completed successfully, error, etc.) and other parameters relating to the operating system and the user's IT environment.

When filing a question/request via our contact form
Other personal data collected are those provided by the user/visitor when corresponding with the e-mail addresses indicated on our site or when filling out our online contact form.
The sending of personal, non-mandatory data also by email on an optional, explicit, and voluntary basis to the addresses indicated on this website means that the address of the sender is then acquired, this being necessary to respond to the request, together with any other personal data included in the message.

When you register to receive Newsletters
We use the website as a service to create and distribute the project newsletter as well as manage subscriptions. The personal data that are collected are the following: email address; first name; last name, entity, position in entity.

Social Media Login Data. We may provide you with the option to register with us using your existing social media account details, like your Facebook, Twitter, or other social media account. If you choose to register in this way, we will collect the information described in the section about social logins below.

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

5.3 HOW DO WE PROCESS YOUR INFORMATION?

We process your personal information for a variety of reasons, depending on how you interact with our services, including:

- To facilitate account creation and authentication and otherwise manage user accounts. We may process your information so you can create and log in to your account, as well as keep your account in working order.
- To communicate CIRCUIT achievements, informing about project events and sending invitations for participation or diffusing project outcomes.

5.4 WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

The General Data Protection Regulation (GDPR) requires us to explain the valid legal basis we rely on to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- Consent. We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time.

- Legitimate interests. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

- Legal Obligations. We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.

We will only send you direct newsletters, emails, or text if we have your consent. You have the right to withdraw that consent at any time by contacting us.

5.5 WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

We may share your personal data with data recipients for:

- Elements that the Consortium is obligated or entitled to by law, contract, judgement, and regulatory decision to notify may be public and independent administrative authorities, judicial authorities and public officials.

- All the elements necessary for the achievement of each specific purpose: the administration and the relevant services of the Consortium.

The Consortium shall not disclose, assign, exchange, grant or otherwise dispose, without the consent of the user/visitor, to third parties, natural or legal persons, personal data other than the cases mentioned above within the scope of national laws provisions.

5.6 DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our cookies policy.

5.7 HOW YOUR PERSONAL DATA IS COLLECTED

We collect and further process personal data in compliance with all applicable legislation and/or regulations, including but not limited to the (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
We will comply at all times with data protection law and principles, which means that your personal data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you herein and/or from time to time, and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have informed you.
- Kept securely.

5.8 HOW DO WE HANDLE YOUR SOCIAL LOGINS?

Our Services offer you the ability to register and log in using your third-party social media account details (like your Facebook or Twitter logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile information we receive may vary depending on the social media provider concerned, but will often include your name, email address, friends list, and profile picture, as well as other information you choose to make public on such a social media platform.
We will use the information we receive only for the purposes that are described in this privacy notice or that are otherwise made clear to you on the relevant Services. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We recommend that you review their privacy notice to understand how they collect, use, and share your personal information, and how you can set your privacy preferences on their sites and apps.

5.9 HOW LONG DO WE KEEP YOUR INFORMATION?

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements), but no longer than 5 years after the conclusion of the project. No purpose in this notice will require us keeping your personal information for longer than the period of time in which users have an account with us.
When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

5.10 HOW DO WE KEEP YOUR INFORMATION SAFE?

Your personal data are processed by electronic means in compliance with the provisions of art. 32 of GDPR 2016/679, national law and in compliance with the principles of data's confidentiality, integrity, and availability. Your personal data are transferred in an encoded manner using the widely used and secure TLS (Transport Layer Security) encryption standard. You will recognise a secure TLS connection by the additional "s" after "http" (i.e., https://..) in the address bar of your browser or from the lock icon. Moreover, we use suitable technical and organizational measures, which are being continuously enhanced, to protect your data against accidental or intentional manipulation, partial or complete loss, destruction, or unauthorized access by third parties.
However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

5.11 DO WE COLLECT INFORMATION FROM MINORS?

We do not knowingly solicit data from children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records.

5.12 WHAT ARE YOUR RIGHTS?

You have the right to:

- Request information about whether we hold personal information about you, and, if so, what that information is and why we are holding it.
- Request access to your personal information. This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request rectification of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you.

- Request transfer of your personal information in an electronic and structured form to you or to another party (right to "data portability"). This enables you to take your data from us in an electronically useable format and to be able to transfer your data to another party in an electronically useable format.

- Withdraw your consent at any time. Please note that the withdrawal does not affect the processing of your data which is based on the consent you have given before the withdrawal. Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose/purposes you originally agreed to. However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

You can exercise any of these rights at any time by contacting us at the contact details provided on the website.

Account Information
If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies
Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services.

If you have questions or comments about your data protection rights, you may email us at ADD EMAIL HERE

5.13 DO WE MAKE UPDATES TO THIS NOTICE?

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a

notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

5.14 HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may contact our DPO by emailing us at ADD EMAIL HERE or by post to:

CIRCUIT PROJECT

ADDRESS

ZIP CODE

TOWN

COUNTRY

6 CONCLUSIONS

The first version of the Data Management Plan reports the procedures, ecosystems and key plans to be implemented in CIRCUIT in order to efficiently and safely manage the generated, collected and processed data throughout the project's lifecycle, in compliance with FAIR principles.
The first summary of the key project data is presented as they are defined at this early stage. Moreover, the first cross-cutting to the project DPIA is performed and presented. Finally, updates to the CIRCUIT Ethics and the Data Privacy Policy are included in this document with regards to their original definition in D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan [1].

The next version of the Data Management Plan, D7.4, which is scheduled to be released on M18 and will be the first of the three in total revisions of the DMP, will include a much more detailed summary of the CIRCUIT datasets as the activities related to them and defining them will be much more advanced. The clear strategies that will be followed on how those datasets will be handled, classified and stored will also be described in greater detail in order to comply with the data protection policies established. In addition to that, an updated DPIA will potentially be included as this assessment will be continuously on-going, following the corresponding developments in the project. Along the cross-cutting to the project DPIA, the probable local DPIAs performed will be also presented. Finally, the data governance models and dashboards will be revisited and enhanced and any further updates to the Ethics manual and data privacy policy will be provided.

REFERENCES

1. Deliverable D7.1 - Project inception report. CIRCUIT Project (GA 101104283)
2. Deliverable D7.2 - Project Quality Assurance, Ethics Manual and Risk Assessment Plan. CIRCUIT Project (GA 101104283)
3. https://gdpr.eu/data-protection-impact-assessment-template/

ANNEX 1 – DPIA TEMPLATE

Step 1 – Identify the need for a DPIA

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents. Summarize why you identified the need for a DPIA.

Step 2 – Describe the processing

Describe the nature of the processing:
1. How are you collecting, using, storing and deleting data? 2. What is the source of the data? 3. Will you be sharing data with anyone? 4. What types of processing identified as likely high risk are involved?

Describe the scope of the processing:
1. What is the nature of the data, and does it include special category or criminal offence data? 2. How much data will you be collecting and using? 3. How long will you keep it?

Describe the context of the processing:
1. What is the nature of your relationship with the individuals? 2. How much control will they have? 3. Would they expect you to use their data in this way? 4. Do they include children or other vulnerable groups? 5. Are there prior concerns over this type of processing or security flaws? 6. Is it novel in any way? 7. What is the current state of technology in this area? 8. Are there any current issues of public concern that you should factor in? 9. Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing:
1. What do you want to achieve? 2. What is the intended effect on individuals? 3. What are the benefits of the processing – for you, and more broadly?

Step 3 – Consulation process

Consider how to consult with relevant stakeholders:
1. **Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.** 2. **Who else do you need to involve within your organisation?** 3. **Do you need to ask your processors to assist?** 4. **Do you plan to consult information security experts, or any other experts?**

Step 4 – Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:
1. **What is your lawful basis for processing?** 2. **Does the processing actually achieve your purpose?** 3. **Is there another way to achieve the same outcome?** 4. **How will you prevent function creep?** 5. **How will you ensure data quality and data minimisation?** 6. **What information will you give individuals?** 7. **How will you help to support their rights? What measures do you take to ensure processors comply?**

Step 5 – Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.
State Likelihood of harm (Remote, possible or probable), Severity of harm (Minimal, significant or severe) and Overall risk (Low, medium or high).

Step 6 – Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Step 7 – Sign off and record outcomes

1. **Who has approved the privacy risks involved in the project? What solutions need to be implemented?**
2. **Integrate the PIA outcomes back into the project plan. Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?**