DIDYMOS XR
δίδυμος

DIGITAL, DYNAMIC AND RESPONSIBLE TWINS FOR XR

D1.2 – Data Management Plan

[WP1 – Project Management]

Funded by the European Union

Funded by the European Union under grant number 101092875.
UK based consortium partner Trilateral Research Limited, UK is funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [grant number 10069394].

Lead Contributor	Ben Howkins, Trilateral Research (TRI UK)
Other Contributors	Imad Elhajj, American University of Beirut (AUB)
	Konstantinos Moustakas, University of Patras (UPAT)
	Ulrich Ahle, FIWARE Foundation
	Tanja Kojic, Technische Universität Berlin (TUB)
	Agata Baizan D'Agostino, FICOSA (FICO)
	Boulos El Asmar, idealworks GmbH (IW)
	Georg Thallinger, Joanneum Research (JRS)
	Jan-Niklas Voigt-Antons, Hoschschule Hamm-Lippstadt (HSHL)
	Francesco Vona (HSHL)
	Panos K Papadopoulos, Centre for Research & Technology Hellas (CERTH)
	Dimitrios Zarpalas (CERTH)
	Joan Manel Martin Almansa, Fundació Internet I Innovacio a Catalunya (i2CAT)
	Jordi Romero, Neapolis (VNG)
	Steve Tate, Unity Softwarte (Unity)
	Adejoke Osuntogun, Unity Softwarte (Unity)
	Rahul Tomar, DigitalTwin Technology (DTT)
	Vangjel Gjorgjiev (TRI IE)
	Elsa Prieto (FIWARE)

Due Date	30/06/2023
Delivery date	
Type	Data Management Plan (DMP)
Dissemination level	PU = Public
Status	Living

Keywords	Research data, non-personal data, personal data, data protection, FAIR requirements.

Document History

Version	Date	Description	Reason for Change	Distribution
V0.2	15.06.2023	Original draft	Internal review (TRI)	15.06.2023
V0.4	16.06.2023	Review version	Quality assurance (JRS)	16.06.2023
V0.6	19.06.2023	Update	Updated to include DTT's response to the questionnaire	19.06.2023
V0.8	23.06.2023	Update	Feedback from QA process	23.06.2023
V1.0	29.06.2023	Final Version for submission	Feedback actioned from QA process	29.06.2023
V1.01			Updated FIWARE information,	08.07.2024
V1.02			added CAP in relevant tables, added new datasets	29.07.2024
V2.0	23.08.2024	Interim update	Updated for all partners ahead of interim review	30.08.2024

About the project

The digital transformation and the availability of more diverse and cost-effective methods for 3D capture has led to the creation of digitised representations of parts of our public spaces, machinery and processes, so-called Digital Twins. These Digital Twins are an important basis for building advanced extended reality (XR) applications for cityscapes and the industrial environments. These XR applications need high-fidelity models for accurate localisation, which are kept in-sync with the real world. The vision of DIDYMOS-XR is to enable advanced, more realistic and more dynamic XR applications, powered through artificial intelligence. The project thus focuses on advancing technologies for creating large-scale digital twins, synchronised with the real world. DIDYMOS-XR will research and develop methods for reconstruction and mapping from heterogeneous inputs, including static and mobile sensors, AI-based data fusion, scene understanding and rendering. Digital twin based XR applications also require means of accurately positioning in the environment, aware of the dynamics of the scene, also addressed by the project. The capture of scenes at scale, as well as using cameras and other sensor data for synchronising the digital representation, bears the risk of capturing personal and sensitive data. Hence, the technologies resulting from DIDYMOS-XR will be ethical and privacy-aware by design. In order to demonstrate and validate the enabling technologies researched and developed in DIDYMOS-XR, the project will address use cases of XR applications in two domains that differ in their scale and characteristics. One is urban planning and smart mobility, the other is the collaboration with autonomous mobile robots at an industrial production facility.

List of tables

List of figures

List of acronyms/abbreviations

Abbreviation	Explanation
CA	Consortium Agreement
DIDYMOS-XR	Digital, Dynamic and Responsible Twins for Extended Reality
DMP	Data Management Plan
DOI	Digital Object Identifier
DPO	Data Protection Officer
EAB	Ethics Advisory Board
EC	European Commission
FAIR	Findable, Accessible, Interoperable, and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
GPS	Global Positioning System

Abbreviation	Explanation
IMU	Inertial measurement unit
IPR	Intellectual property rights
LIA	Legitimate Interest Assessment
LIDAR	Light Detection and Ranging
NDA	Non-disclosure agreement
PM	Person Months
SB	Stakeholder Board
WP	Work Package

Table 1: List of acronyms/abbreviations

Abbreviation	Partner Organisation
AUB	American University of Beirut
CAP	Capgemini
CERTH	Centre for Research & Technology Hellas
DTT	DigitalTwin Technology GmbH
FICOSA	Ficosa
FIWARE	FIWARE Foundation e.V.
HSHL	Hoschschule Hamm-Lippstadt
i2CAT	Internet i Innovacio a Catalunya
IW	Idealworks
JRS	Joanneum Research
TRI	Trilateral Research Ltd.
TUB	Technische Universität Berlin
UNITY	Unity
UPAT	University of Patras
VNG	Neàpolis ~~Villanova~~

Table 2: Partner organisations and associated abbreviation

Glossary of terms

Term	Explanation
Data collection	The process of gathering information or data
Data Management Plan	A document describing the data management lifecycle for data to be collected, processed and/or generated, which includes information on the following: the handling of research data during

Term	Explanation
	and after the end of the project; what data will be collected, processed and/or generated; which methodology and standards will be applied; whether data will be shared or made open access; and how data will be curated and preserved (including after the end of the project).[1]
Data processing	'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[2]
Digital Object Identifiers	Digital identifiers for objects (whether digital, physical or abstract).[3]
Digital twin	A digital representation of an intended or actual real-world physical product, system, or process.
End-user	A person, group or organisation who has the potential to use or exploit the project's results and findings. Each stakeholder is thus also an end-user, but not vice-versa.
FAIR	The European Commission has recommended that beneficiaries make their research data FAIR, namely 'findable, accessible, interoperable and reusable, to ensure it is soundly managed'[4]
Metadata	Data about data.

[1] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereafter GDPR), Article 4(2).

[3] Digital Preservation Coalition, 'Digital Preservation Handbook' https://www.dpconline.org/handbook/technical-solutions-and-tools/persistent-identifiers

[4] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

Term	Explanation
Open access	Online access to research outputs provided free of charge to the end-user.
Open science	An approach to the scientific process based on open cooperative work, tools and diffusing knowledge.
Persistent identifiers	Globally unique and long-lasting references to digital objects (such as data, publications and other research outputs) or non-digital objects such as researchers, research institutions, grants, etc.[5]
Personal data	'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'.[6]
Research data	'Refers to information, in particular facts or numbers, collected to be examined and considered as a basis for reasoning, discussion, or calculation.'[7]
Research data management	The process within the research lifecycle that includes the data collection or acquisition, organisation, curation, storage (long-term), preservation, security, quality assurance, allocation of persistent identifiers (PIDs), provision of metadata in line with disciplinary requirements, licencing, and rules and procedures for sharing of data.[8]
Stakeholder	A relevant actor (persons, groups, or organisations) who: (1) is affected by the project's results and findings; (2) have the

[5] EU Grants: HE Programme Guide: V2.0 – 11.04.2022, p.43. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf
[6] Art.4(1) GDPR.
[7] H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020. European Commission. Version 3.2 (21 March 2017), p4. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf
[8] EU Grants: HE Programme Guide: V2.0 – 11.04.2022, p.42. <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf>

Term	Explanation
	potential to use or exploit the project's results and findings; or (3) have a stated interest or stake in the project results and findings.

Table 3: Glossary of terms

Executive summary

This deliverable reports the work carried out in the context of Task 1.3 'Data management', pursuant to the description of this task in the DIDYMOS-XR Grant Agreement (GA). As outlined here, the Data Management Plan (DMP) defines how the various types of data collected generated, and processed in the project will be handled and stored. The DMP will be maintained as a living document throughout the entire lifecycle of the project. This is the second version of the document, prepared for the project interim review, and will continue to be updated as the research progresses and project partners learn more about their data needs, and how they will use the data which they generate or acquire. Each project partner is responsible for the data they collect, process, store and use within the project, and for compliance with the strategy outlined in this document.

This deliverable will not only serve as guidance for the whole consortium in terms of data management within the project, but will also more immediately inform the 'Ethics and data protection' work in T2.2, for which the GA provides that project partner Trilateral Research Ltd. (TRI) is required to meet with task leaders to identify, discuss and resolve potential ethical, data protection and legal issues arising in their tasks. For this reason, the document includes a preliminary analysis of the ethical aspects of data management, as well as a section on the protection of personal data and the project's compliance with the General Data Protection Regulation (GDPR) and other relevant national data protection laws.

Table of Contents

1 Introduction

1.1 Background

This deliverable (D1.2) corresponds to Task 1.3 of the DIDYMOS-XR project. As described in the project Grant Agreement (GA)

> "*The Data Management Plan (DMP) will define how the various kinds of data collected and generated in the project will be handled and stored. It sets the requirements for the data store in terms of data security and privacy protection. It will be maintained as a living document*."

In order to gather information to be used in the project, Trilateral Research (TRI) developed a questionnaire for all partners to complete. This questionnaire is based on the template DMP questionnaire found in the '*Guidelines on FAIR Data Management in Horizon 2020*',[9] which was then expanded to meet the specific needs of the project. For the purposes of developing an initial DMP by M6, copies of this questionnaire were circulated in March 2023 to all partners, who were encouraged to consult with their Data Protection Officers (DPO) or other person responsible for data protection in their organisation when providing a response. The answers provided by the project partners on the data they will collect, process and produce over the course of the DIDYMOS-XR project form the basis of the information contained in this document. Completed questionnaire responses are kept on file by TRI. A copy of the questionnaire is included in Annex I, whilst an overview of partners' responses to questions on research data and personal data can be found in Annexes II and III, respectively.

The European Commission (EC) suggests that a DMP should include information on the following:

- The handling of research data during and after the end of the project;
- What data will be collected, processed and/or generated;
- Which methodology and standards will be applied;
- Whether data will be shared/made open access; and

[9] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- How data will be curated and preserved (including after the end of the project).[10]

This document includes information covering all of these aspects, and more. Regarding open access, the EC provides the principle of "as open as possible, as closed as necessary."[11] The consortium interprets this to mean that all data generated by the project should be made open access, unless there is a pressing reason not to. Accordingly, DIDYMOS-XR project partners will endeavour to make as much data as possible available to the public and other researchers for future research activities.

1.2 Purpose and scope

The purpose of this deliverable is to display what data the project will generate and use, and how. It also explains how the use of this data will comply, as far as possible, with the FAIR principles (Findable, openly Accessible, Interoperable, Re-usable). Further, it explains how data, particularly personal data, that is generated in the project will be protected and kept secure.

The scope of this deliverable is to explain the institutional policies and practices of each member of the consortium in their work on the project to provide an overview of data practices of the consortium as a whole. This deliverable does not cover the work of partners unassociated with the project. The entire 6-stage 'lifecycle' of data is considered in this document. The data lifecycle involves:

- **Planning research**: designing research; planning data management; planning consent for data sharing; planning data collection and processing protocols and templates; exploring existing data sources.
- **Collecting data**: data collection; capturing data and metadata; acquiring existing third-party data.
- **Processing and analysing data**: entering, digitising, transcribing, and translating data; checking, validating, cleaning and anonymising data; creating

[10] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[11] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

derivative data; describing and documenting data; managing and storing data; analysing and interpreting data; producing research outputs; citing data sources.

- **Publishing and sharing data**: establishing copyright; creating user documentation; creating discovery metadata; electing appropriate access to data; publishing and sharing data; promoting data.
- **Preserving data**: migrating data to the best formats/media; storing and backing-up data; creating preservation documents; preserving and curating data.
- **Re-using data**: conducting secondary analysis; undertaking follow-up research; conducting research reviews; scrutinising findings; using data for learning.[12]

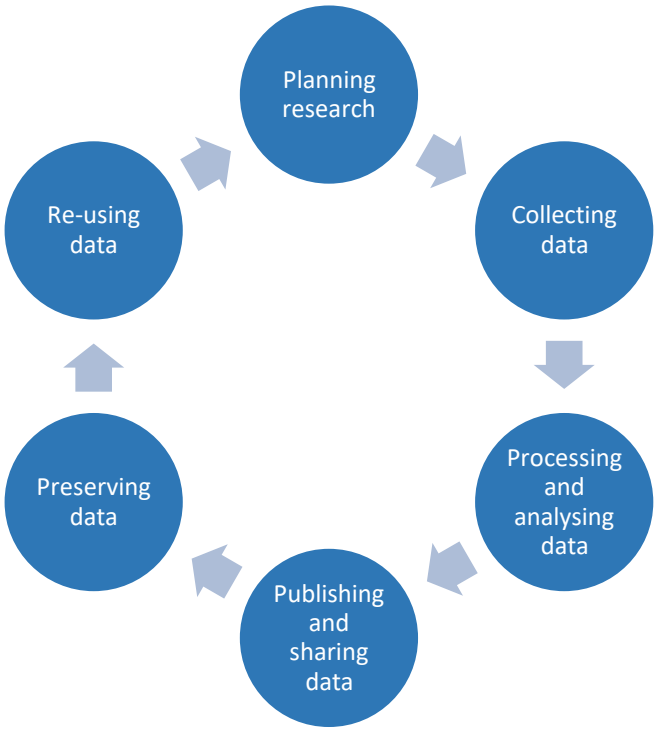

Figure 1: Steps in the research data lifecycle

The project engages with each stage of the data lifecycle. However, explaining the lifecycle here does not mean that every partner is bound to perform every aspect of each stage in the lifecycle, as not all partners are in a position to perform each activity.

[12] UK Data Service. (n.d.). *Data Lifecyle*. Retrieved 15 June 2023 from https://ukdataservice.ac.uk/learning-hub/research-data-management/

1.3 Deliverable structure

As noted above, this document follows the structure recommend in the European Commission's (EC) Horizon 2020 Data Management Plan Guidelines of 26 July 2016. Accordingly, this deliverable is structured as follows. Following this introduction, Section 2 provides an overview of the data that partners intend to use in the DIDYMOS-XR project and refers to the relevant annexes in which partners' more detailed responses to questions in the DMP questionnaire on research data and personal data can be found. Section 3 details applicable standards, guidelines and principles, focusing on partners' institutional policies on research data management and the processing of personal data. Sections 4 and 5 outline how the DIDYMOS-XR project will ensure that its data and other research outputs are findable, accessible, interoperable and re-useable (FAIR). Section 5 covers the protection of personal data in the project and compliance with Regulation 2016/679 General Data Protection Regulation (GDPR)[13] and other relevant national data protection laws. Section 7 elaborates on data security within the project, while Section 8 covers ethical aspects. Section 9 provides an overview of the responsibilities of different partners and allocation of resources for data management within the project. Finally, Section 10 concludes the document and notes planned future updates to the provisions therein.

2 Data summary

This section aims to give an overview of the data being processed in the DIDYMOS-XR project. It covers use of data by individual partners, as well as collectively where partners use shared datasets. In order to streamline the process of eliciting relevant information relating to the latter, the initial DMP questionnaire, as included in Annex I, referred partners at Question 6 to a separate document on 'Shared Research Datasets Questions'. Information provided by project partners in response to these questions, as well as those on data usage per partner organisation, has been aggregated and included in Annex II.

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

2.1 Overview of data in DIDYMOS-XR

Following the responses of the DIDYMOS-XR project partners to the initial DMP questionnaire issued in March 2023, the types of data (including personal data) that are preliminarily expected to be collected, processed and/or generated during the project include:

- Multi-view image and video data received from sensors including cameras;
- Point cloud data captured through LIDAR sensors;
- Oblique aerial photographs captured by drones;
- Inertial Measurement Unit (IMU) data;
- Global Positioning System (GPS) data;
- Volumetric data;
- Synthetic data used to set-up specific configurations, scenes or environments upon which machine learning algorithms can be trained;
- Demographic, behavioural and attitudinal data collected during interviews, surveys, usability questionnaires and through human subject evaluation forms;
- Video data in recordings of interviews, from which speech data will be analysed;
- Contact details, such as name, contact country, job title, company name and email address, of project partners, Stakeholder Board and Ethics Advisory Board members, subscribers to the project newsletter, and users of the 'contact us' function on the project website.

Depending on the purpose of the data and whether there are any data protection and/or ethical concerns, these data may be made public, shared only within the project consortium, or kept in institutional repositories. More information on the sharing of data within or outside the project can be found in the overview of partners' responses to questions on research data and personal data, as outlined in Annexes II and III.

An aggregated overview of the research data that will be collected, generated and processed in the DIDYMOS-XR project is presented in Annex II. It consists of a table with headings corresponding to the questions posed to project partners in the DMP questionnaire, which is included in Annex I. The answers provided by partners cover the following topics: data type; Work Package (WP)/Task in which these data are used; origin; format; size; URL; methods, software and tools used to process these data;

data users; data access at the partner organisation; data storage and the time period for retention; whether these data may be useful for other researchers; and whether these data will be shared with others within the project and/or the wider public.

An aggregated overview of the personal data that will be processed in DIDYMOS-XR is provided in Annex III. It consists of a table with headings corresponding to the questions posed to project partners in the DMP questionnaire, which is included in Annex I. The answers provided by partners cover the following topics: data type; data origin; necessity; legal basis; whether these data are sensitive pursuant to Article 9 GDPR and, if so, whether a relevant exemption applies, such as explicit consent; whether there are any ethical concerns with these data; whether these data will be anonymised, pseudonymised and/or encrypted; data format; data storage; data access; and whether these data will be shared with others within the project.

3 Applicable standards, guidelines and principles

The questionnaire circulated to project partners asked about institutional policies dealing with research data in general, and use of personal data specifically. This section presents an overview of partners' organisational policies and procedures relating to research data management and the processing of personal data. As a minimum, all project partners adhere to all applicable national and international (e.g., GDPR) laws and regulations on data privacy and the protection of personal data.

3.1 Overview of organisational policies and procedures for research data management

The following information is taken from the responses of each partner organisation to the questionnaire in Annex II.

Partner	Policy on data management
AUB	AUB policy on data with human subject information can be found here: https://www.aub.edu.lb/irb/Pages/default.aspx. This document details the responsibility of the Human Research Protection Program (HRPP) for safeguarding the rights and welfare of human

Partner	Policy on data management
	subjects participating in Biomedical and Social and Behavioural Sciences research activities conducted under the auspices of AUB/AUBMC. A core component of HRPP, the Institutional Review Board (IRB) is formally designated to review and approve the conduct of research involving human subjects who are recruited to participate in research activities conducted at AUB/AUBMC and/or by AUB/AUBMC faculty, students and staff, regardless of the funding source or the location of the research.
CAP	Capgemini is committed to protecting the privacy of its clients, employees and partners. In order to do so, Capgemini has adopted Binding Corporate Rules (BCR) as its global data protection policy. The policy details can be found here: Data Protection Policy | Management And Governance | Capgemini The EU Binding Corporate Rules (EU BCR) for Controller & Processor activities – initially approved by the European Data Protection Authorities in March 2016 and subsequently updated in January 2019 to comply with the General Data Protection Regulation (GDPR).
CERTH	CERTH has a policy on Scientific Research in accordance with the General Data Protection Regulation. This policy, written in Greek, is a confidential document, and its disclosure is strictly prohibited.
DTT	DTT complies the best practices of the General Data Protection Regulation (GDPR) on research data management applied within and across the organisation.
FICOSA	We have a non- written policy on research data management, but we work under the following guidelines, principles and best practices and FAIR Principles, based on the *Code of Practice on the management of intellectual assets for knowledge valorisation in the European Research Area:* - Promote open science and use, when possible, of open repositories - Follow "as open as possible and as closed as necessary" principle: focused on protecting our intellectual assets (understood as any

Partner	Policy on data management
	result or products generated by any R&I activities (such as intellectual property rights, data, know-how, prototypes, processes, practices, technologies, software) to boost inventions and innovation. - Follow strategic intellectual assets management practices: • Have a due diligence process for intellectual assets generated within our organisation: establish no infringement clauses, freedom to operate, analysing the terms and conditions of each intellectual asset used (datasets, software, databases, etc.) • Have an open-source software policy and specific internal governance bodies to manage open-source software. • Agree with partners on ownership issues early on including access and use rights. • Prepare a list identifying all background results, including IP, and relevant side ground information belonging to each of the partners and expected to be used during the project. • Check all applicable funding, institutional and legal requirements enabling open access to research results. • Raise awareness among all personnel in our organization on open data principles and protection of intellectual assets.
FIWARE	FIWARE does not have a specific policy on research data management a
HSHL	HSHL has a central plan for research data management. Additional Information on Data Protection applies to the central part of HSHL's webpages.https://www.hshl.de/en/hamm-lippstadt-university-of-applied-sciences/data-protection/ The controller within the meaning of the EU General Data Protection Regulation (GDPR) and other national data protection laws of the members dates as well as other data protection regulations is Hamm-Lippstadt University of Applied Sciences (HSHL) The President Marker Allee 76-78 59063 Hamm Germany Phone: +49 (0)2381 8789-0

Partner	Policy on data management
	E-mail: info@hshl.de Website: www.hshl.de
i2CAT	In i2CAT, we are working on an internal policy document on Research Data Management, which is expected to be approved in September 2023. Currently, in our internal intranet there is a document with comprehensive guidelines so that researchers have all information about this issue centralised and easy to consult. The main aspects covered in the document are: - Data management. - FAIR principles. - Data management planification. - Publishing, sharing and preservation research data. - Recommendations and templates for data management.
IW	IW follows best practices of ISO27001 and the GDPR.
JRS	JRS does not have an overall policy, but applies policies according to the project funding body's principles. As general guidelines, we are following the FAIR principles. In regard to keeping data secure and private we follow EU (i.e., GDPR) and national law. A process is in place to check for potential applicability of data protection measures already in the offering phase, which is then to be followed throughout the DIDYMOS-XR project.
TRI	TRI's institutional policies and procedures are specified in its internal Policies and Procedures document and its Data Protection Policy. TRI follows established guidelines in relation to any project work undertaken, which involves data collection, storage and transfer. Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR") and the British and Irish Data Protection Acts of 2018 ("the Acts") govern the processing of personal data. Any personal data collected is stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server filed is granted by invitation only; there is a log register and related licences for each person on the cloud. TRI encrypts access to the network via state-of-the-art network management tools, ensuring that only authorised TRI staff may access the shared network

Partner	Policy on data management
	environment and assets on the network. TRI project members store their laptops (and any other device used for DIDYOS-XR) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software. Any transfer of sensitive data only takes place over encrypted connections, using password protections and access controls in the case of uploads and downloads to and from repositories. TRI is accredited under the UK government Cyber Essentials Scheme.
TUB	In TUB's Handling Personal Data policy document, it is stated that the scientific community has to comply with data protection rules when working with research data, in accordance with both the EU Charter of Fundamental Rights and Germany's Basic Law (Grundgesetz). Key processes outlined here include determining the legal basis and controllership of the data in preparation for working with personal data, as well as immediately anonymising data, or at least pseudonymising, at the point of collection. Finally, after completion of the project, the research data on which the results are based will be retained for at least 10 years and, if possible, made publicly available.
Unity	Unity's Legal Information document contains its privacy policy, terms of service, data processing agreement and other relevant documentation.
UPAT	UPAT's policy on data management, which is only available in Greek, can be found here: https://alumni.upatras.gr/privacy/.
VNG	It does not have a policy on research data management.

Table 4: Overview of organisational policies and procedures for research data management

3.2 Overview of organisational policies for processing personal data

The following information is taken from the responses of each partner organisation to the questionnaire in Annex II.

Partner	Policy on processing of personal data
AUB	AUB's policy on the processing of personal data can be found in its Privacy Statement. This statement sets out how AUB, as the Data Controller, uses

Partner	Policy on processing of personal data
	personal information received from individuals, for what purpose(s) this information is used, and how it is processed, including the relevant legal basis. It is stated here that AUB takes data privacy seriously and adheres to all data privacy laws and regulation applicable to the institution. *AUB has a DPO under the remit of the Office of Compliance. See further here: https://www.aub.edu.lb/President/compliance/Pages/about.aspx.*
CAP	Capgemini is committed to protecting the privacy of its clients, employees and partners. In order to do so, Capgemini has adopted Binding Corporate Rules (BCR) as its global data protection policy. The policy details can be found here: Data Protection Policy | Management And Governance | Capgemini The EU Binding Corporate Rules (EU BCR) for Controller & Processor activities – initially approved by the European Data Protection Authorities in March 2016 and subsequently updated in January 2019 to comply with the General Data Protection Regulation (GDPR).
CERTH	CERTH has a Data Protection Policy. This policy, written in Greek, is a confidential document and its disclosure is strictly prohibited. In general, CERTH endeavours to minimise the collection of personal data as much as possible. When developing our algorithms, we strive to use anonymised data whenever feasible. In cases where personal data must be stored or processed, we only collect the minimum amount of data necessary and limit the number of individuals with access to that data to a minimum. *CERTH is required to have a DPO under Article 37 GDPR. Stella Papastergiou is CERTH's designated DPO.*
DTT	DTT makes sure not to store any personal data unless necessary and if so, to follow the specific regulation to protect it. For processing of any data that includes personal information as per the GDPR definition, we ensure to anonymise it completely.
FICOSA	In our corporate website you may find the link to our privacy policy: https://www.ficosa.com/privacy-policy/. Ficosa is committed to processing data in accordance with its responsibilities under the GDPR. We have put appropriate technical and organisational

Partner	Policy on processing of personal data
	security policies and procedures in place to protect personal data. Any personal data collected is stored on a secure, private, cloud-based server that is maintained on a regular basis. All access to cloud-based server files is granted by invitation only and under the signature of specific access request agreements (FSANS); there is a creation of internal user for each person on the cloud. In addition, in the framework of DIDYMOS project, we are working with an external consultant in a Data Protection Impact Assessment (DPIA) for the assessment of the activities and tasks we will carry out (acquisition of data). Ficosa encrypts access to the network via state-of-the-art network management tools, ensuring that only authorised Ficosa staff under a need-to-know basis may access the shared network environment. Ficosa has implemented limitations on both physical and digital access to internal information. Those individuals who have access to the data are required to maintain the confidentiality of such information being subject to non-disclosure agreements (NDAs). Ficosa personnel store their laptops (and any other devices used for DIDYMOS-XR) securely when unattended (office, home, travelling). Additional measures include: - Daily back-ups of fileservers stored data; - password protection (at least 14 characters with capital and numbers); - regularly changing users password (monthly); - using two-factor authentication (2FA) systems (password + one time password (OTP)); - encryption of home office network access / limit VPN; - installation and regularly updating of security and anti-virus software on all systems; - prohibition on documenting passwords in any way; - Encrypted backup copies. Ficosa has an outsourcing for services of privacy and personal data protection. Helas is the entity who assist us regarding all matters related to personal data protection, such as by reviewing personal data sections in

Partner	Policy on processing of personal data
	contractual agreements and the creation of internal policies, etc. In addition, Ficosa has created a Mixed Commission formed by a Human Resources Manager and Corporate Information Security Director, which observes and receives, prima facie, the exercise of rights of interested subjects and other requirements in the field of protection of personal data. *FICOSA is assessing whether the entity requires the designation of a DPO. In 2018, FICOSA subcontracted a data protection consultancy to analyse this question and the results were that, under automotive branch, and for general FICOSA activities, the designation of DPO was not necessary. However, for the DIDYMOS-XR project, FICOSA will take measures not foreseen in this analysis, so a new necessity analysis is underway.*
FIWARE	FIWARE's Personal Data Protection Policy details the types of information collected by the organisation, the principles it follows, whether and under what circumstances these data is shared with others, and the rights of individuals as data subjects under the GDPR. *FIWARE has a DPO, as is required under Article 37 of the GDPR.*
HSHL	The Guidelines for Information Security at Hamm-Lippstadt University of Applied Sciences details how information security at HSHL is to be implemented in accordance with current technical and data protection requirements. It cites the creation of a dedicated Data Protection and Data Security team, whose members include a data protection officer, to whom any observed vulnerabilities or incorrect handling of university data in terms of information security, data protection or information technology can be reported. Additional Information on Data Protection applies to the central part of HSHL's webpages. The data protection officer of the controller is Hamm-Lippstadt University of Applied Sciences Data Protection Officer: Ellen Kortenbach |ppc Data GmbH Marker Allee76-78 59063 Hamm E-mail: dsb@hshl.de
i2CAT	i2CAT has an internal Data Protection Policy, but is currently in the process of upgrading and updating it. Our General Policy Document of Personal Data

Partner	Policy on processing of personal data
	(GPDPD) is of obligatory compliance for all the staff with access to personal data and to the information systems in accordance with: - The REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data (GDPR) - The Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights and development regulations. This document determines its scope, obligations and responsibilities of staff members, security measures, rules procedures, regulations and standards in force on personal data processing. *i2CAT's designated DPO is Begonya Domene Amat*.
IW	IDEALworks is committed to compliance with all national and international laws and legislation maintaining appropriate procedures and work instructions. Personal data is classified as per the classification levels in Information Security Classification policy. The policy applies to all personal data held by the company, including paper and paperless formats. All employees will be provided with training to ensure that they understand IDEALworks' policy and the procedures it has put into place to implement that policy. The disciplinary process will be invoked in circumstances where this policy may have been transgressed. In addition to following best practices, including ISO27001 and the GDPR, personal data is only accessible to restricted personnel on a need-to-know basis. *IW is not required to have a DPO under Article 37 of the GDPR*.
JRS	JRS' Data Protection Information notice is available here: https://www.joanneum.at/en/joanneum/imprint/dataprotection/. In general, as far as possible JRS seeks to avoid collecting any personal data. If possible, in view of the algorithms we are developing within the project, data are anonymised. If personal data have to be stored or processed, the amount of data is kept to the minimum needed and the number of people who are handling that data again is restricted to the minimum.

Partner	Policy on processing of personal data
	As regards data protection in research projects, it is provided that Joanneum Research carries out the processing of research data on the basis of the Austrian and European data protection laws and also on the legal basis of Section 1 of the Austrian Research Organisation Act (Forschungsorganisationsgesetz, FOG) in conjunction with Art.89(1) GDPR. *JRS has a DPO, who is reachable via dataprotection@joanneum.at*.
TRI	Trilateral Research's Privacy Policy (last updated December 2018) aims at informing website visitors, our business and research partners, and other stakeholders about how we process personal data. We are committed to processing personal data responsibly, securely, and proportionally throughout our business. Particularly relevant are Sections 6 and 7, which detail what we do with personal data and how we secure it when processing. As regards the latter, we have put appropriate technical and organisational security policies and procedures in place to protect personal data (including sensitive personal data) from loss, misuse or destruction. We aim to ensure that access to personal data is password protected. We encrypt all data stored at our central location and data are restricted only to those who need to access it. Those individuals who have access to the data are required to maintain the confidentiality of such information. We install and regularly update all security and anti-virus software in use on all of our systems. Please be aware that the transmission of data via the internet is not completely secure. Whilst we do our best to try to protect the security of personal data, we cannot ensure or guarantee the security of data transmitted to our site. *Although not required by Article 37 GDPR, TRI has a DPO and offers professional DPO services to clients*.
TUB	TUB's policy for Handling Personal Data details the data protection legislation with which the handling of personal data by TUB is required to comply, including the Berlin Data Protection Act and the GDPR. Also found here is a series of resources, including practical guides to anonymisation and pseudonymisation and information for research subjects on joint data controllership.

Partner	Policy on processing of personal data
	Since TUB is governed by the State of Berlin, the University and its employees are subject to the Berlin Data Protection Act as well as the GDPR.
Unity	Unity's Legal Information document contains its privacy policy, terms of service, data processing agreement, and other relevant documentation. The Privacy Policy Hub sets forth Unity's policies and procedures regarding the collection, use and disclosure of information received by Unity, including its compliance with the GDPR and associated practices. *Unity is required to and has a DPO under Article 37 GDPR*.
UPAT	UPAT's policy on the processing of personal data is only available in Greek. The Privacy Policy for the institution's website states that the management and protection of personal data of visitors/users of the website is subject to the provisions of Law 2472/1997 "Protection of the individual from the processing of personal data" as applicable. The University of Patras takes all appropriate technological and organisational measures to protect personal data from breaches in order to prevent the unintentional loss, alteration, disclosure and use or access of personal data in an unauthorised manner. *While not required to, UPAT has a DPO.*
VNG	Legal advice about personal data on the website of the Vilanova City Council and La Geltrú is available in Spanish, Catalonian and English at the following link: https://www.seu-e.cat/es/web/vilanovailageltru/avis-legal *The City of Vilanova, as a public authority, is required to have a DPO under Article 37 GDPR*. Link contract with: UNIVE ABOGADOS, UNION TEMPORAL DE EMPRESAS, LEY 18/1982, DE 26 DE MAYO.

Table 5: Overview of data management policies and procedures related to the processing of personal data.

4 The FAIR principles

As noted in the *Guidelines for Horizon 2020*, to which reference is made in the absence of updated guidelines for data management in Horizon Europe projects, data that is made findable, accessible, interoperable and reusable (FAIR) can be managed more effectively, and this can ultimately foster better science through enabling others

to reproduce results and reuse data for future experiments.[14] In accordance with this guidance, this section outlines how DIDYMOS-XR will fulfil the FAIR principles.

4.1 The FAIR requirements

In order to make data **FAIR**, they must be:

- **Findable,** meaning that there are logical and easy to follow rules in place to enable data to be found, and that they can be easily searchable by members of the public who are interested in the project.
- **Accessible**, meaning that as many people as possible can access and use the data.
- **Interoperable**, meaning that data can be easily exchanged and used by different entities.
- **Reusable**, meaning that data is licensed in such a way that future researchers can use it for subsequent research.

4.2 Making data findable

Making data easily findable is advantageous for the DIDYMOS-XR consortium itself, as partners will be able to conduct their project work in a more efficient manner, and is also beneficial for future researchers and the wider public, who will be more likely to understand the project and make use of its outputs if they can easily find and locate different project documents. Where data cannot be accessed by other partners due to its sensitivity, the relevant data owner(s) will follow the principles outlined below to ensure this data is findable by researchers and other staff within their organisation.

4.2.1 Within the project

The internal project documents and administrative data of DIDYMOS-XR are stored in the centralised *NextCloud* files online repository. This shared cloud space was set-up and is hosted by the coordinating partner JRS and is accessible to all partners working on the project. JRS manages access rights and monitors folders and file names to ensure consistency throughout the data repository. In order to make data within the DIDYMOS-XR project findable, the following measures are also taken:

[14] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- **Location:** All project documents are stored in well-organised folders on internal drives and/or the shared project drive. Folders within the *NextCloud* files drive are divided into specific WPs, most of which are then subcategorised into the tasks within them (the WP1 folder, for example, includes 'T1.3' and 'D1.2' subfolders). All DIDYMOS-XR partners are responsible for storing project documents in the correct location within the shared drive. In some instances, depending upon different ethical, legal and/or security considerations, certain files with sensitive content might only be stored on a project partner's server (e.g., interview recordings from user requirements interviews in WP2).
- **Naming of files**: As part of its project management work in WP1, JRS has prepared a 'Project Handbook' (Deliverable 1.1), which includes clear guidance on the naming of project files. As outlined here, all files stored in the common cloud space hosted on NextCloud following a designated naming convention, namely: DIDYMOS-XR-Title-vnn(PPP). The letter 'v' and the sequential numbering (2 digits) denotes the version of the document, whilst '(ppp)' denotes an optional marker for a version modified by a partner requiring integration by the document editor.
- **Documenting contributors**: All deliverables have a common frontmatter containing information on authors and other contributors, dissemination level and other relevant metadata, as well as a table of key words. Also included here is a 'Document History' table, in which contributors can indicate what updates they have made and when these took place.
- **Overview**: The *NextCloud* files drive includes an 'Activity' tab where partners can track the timeline for documents created, changed and renamed. Also included here is a sharing function through which partners can share documents using an internal link, which only works for users with access to the file(s).

4.2.2 Beyond the project

The following measures will ensure that outputs from the DIDYMOS-XR project are findable externally:

- Once approved by the EC, all project deliverables marked 'PU – Public' will be made publicly available on the DIDYMOS-XR project website,[15] and in agreed

[15] https://didymos-xr.eu/

institutional and/or other open access repositories, such as Zenodo, along with informative material such as a factsheet;

- Any datasets which are publicly shareable will be made available on common data repositories, such as IEEE DataPort,[16] Open Research Europe,[17] GitHub,[18] and/or Zenodo;[19]
- A digital object identifier (DOI) will be assigned to datasets for a unique and persistent citation when uploaded to a designated repository, which can be used in any relevant publication to direct readers to the underlying dataset.
    - Datasets published under a DOI on Zenodo, for instance, will include metadata indexed to DataCite servers during DOI registration, which will be further linked to the dataset's DOI by employing the OpenRefine extension;
- A list of keywords will be provided in the frontmatter of every deliverable and report produced by the project;
- All partners will be advised of the availability of data and their location to facilitate access and wider sharing as appropriate.

4.3 Making data accessible

4.3.1 Open Access to Scientific Publications

Research outputs from the DIDYMOS-XR project in the form of publications will be made open access (OA) using the gold OA mode when possible, and green OA as an alternative. This entails making such scientific publications available in trusted OA and/or pre-archiving repositories, such as Zenodo, arXiv, and Open Research Europe, in addition to the final versions available at the publishers. The basis for this is Article 17 of the DIDYMOS-XR GA which, read in conjunction with the special rules outlined in Annex 5, requires that '[t]he beneficiaries must ensure open access to peer-reviewed scientific publications relating to their results.' In particular, partners are required to ensure that:

[16] https://ieee-dataport.org/
[17] https://open-research-europe.ec.europa.eu/
[18] https://github.com/
[19] https://zenodo.org/

- At the latest at the time of publication, a machine-readable electronic copy of the published version or the final peer-reviewed manuscript accepted for publication, is deposited in a trusted repository for scientific publications;
- Immediate open access is provided to the deposited publication via the repository, under the latest available version of the Creative Commons Attribution International Public Licence (CC BY)[20] or a licence with equivalent rights; for monographs and other long-text formats, the licence may exclude commercial uses and derivative works (e.g., CC BY-NC,[21] CC BY-ND)[22]; and
- Information is given via the repository about any research output, or any other tools and instruments needed to validate the conclusions of the scientific publication.[23]

In terms of the metadata of the deposited publications, DIDYMOS-XR partners will ensure to make these open under a Creative Common Public Domain Dedication (CC 0)[24] or equivalent, in line with the FAIR principles. This metadata must include information at least about the following: publication (author(s), title, date of publication, publication venue); Horizon Europe funding disclaimer; grant project name, acronym and number; licencing terms; persistent identifiers for the publication, the authors involved in the action; and, if possible, for their organisations and the grant.[25] Additionally, the metadata must include, where applicable, persistent identifiers for any research output or any other tools and instruments needed to validate the conclusions of the publication.[26]

The management of scientific dissemination and communication within DIDYMOS-XR will be handled by project partners involved in T6.1.

4.3.2 Open Access to Research Data

In accordance with Article 17 of Annex 5 of the DIDYMOS-XR GA pertaining to dissemination of results, the project will ensure open access to research data via a trusted repository. These data are to be deposited under the latest available version

[20] https://creativecommons.org/licenses/by/4.0/
[21] https://creativecommons.org/licenses/by-nc/2.0/
[22] https://creativecommons.org/licenses/by-nd/2.0/
[23] Annex 5, Article 17, DIDYMOS-XR Grant Agreement.
[24] https://creativecommons.org/publicdomain/zero/1.0/
[25] Annex 5, Article 17, DIDYMOS-XR Grant Agreement.
[26] Annex 5, Article 17, DIDYMOS-XR Grant Agreement.

of the Creative Commons Attribution International Public Licence (CC BY) or Creative Commons Public Domain Dedication (CC 0) or a licence with equivalent rights.[27]

Research data (and public deliverables, including technical reports) will be made accessible by deposit in an EC-funded repository system, namely Zenodo,[28] which will be linked to on the DIDYMOS-XR website. As the project progresses, the Consortium will also explore other repository options for making research data accessible. Based on partners' responses to the initial DMP questionnaire circulated in March 2023, these other options include, but are not limited to, GitHub, IEEE DataPort and arXiv. For any such repository used by the DIDYMOS-XR project, partners will also provide information via the repository about any other tools and instruments needed to re-use or validate the data, potentially including a description of and dictionary for these data.

However, in line with the guiding principle of "as open as possible as closed as necessary",[29] research data will not be made open access if one of the following factors are applicable:

- (i) It would be against the beneficiary's legitimate interests, including regarding commercial exploitation; or
- (ii) It would be contrary to any other constraints, in particular the EU competitive interests or the beneficiary's obligations under the GA.

Whilst the DIDYMOS-XR project will make datasets captured or created in the project available open access whenever possible, there are two main factors which may in certain instances override this. Firstly, as with the software generated by the project, some of the data generated may pertain to components, software and/or figures considered commercially confidential by one or more of the partners. Synthetic data generated by FICOSA, for instance, will not be made available to the public in order to protect intellectual property rights (IPR) of third parties, whilst IW will not make data from the industry use case openly available due to its inclusion of structural details of industrial facilities for which there is a commercial interest in keeping protected. A

[27] Annex 5, Article 17, DIDYMOS-XR Grant Agreement.
[28] https://zenodo.org/
[29] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

second constraining factor is that research data may also give rise to privacy concerns. Access to video data captured for the purposes of the cityscape use case, for instance, will be limited since personal data may be contained therein. In both instances, these factors necessitate limiting the amount of data that can be made openly accessible.

4.4 Making data interoperable

The DIDYMOS-XR partners exchange information using a variety of means as appropriate for the intended purpose, including by upload to the shared project NextCloud drive and via email. The DIDYMOS-XR project will use common file formats (e.g., .docx, .xls and .pdf) as much as possible to facilitate data exchange and re-use between partners, and ensure interoperability. With regards to datasets, technical partners are mostly planning to use openly available software and commonly used file formats for data including images, video and point clouds. However, some partners will use internally developed proprietary software in order to carry out their tasks in the DIDYMOS-XR project, which will not be interoperable unless the file format is made accessible with open-source software.

4.5 Making data re-usable and increasing re-use

4.5.1 Re-use of existing data

Some of the outputs created by the DIDYMOS-XR project will re-use existing data that is relevant to its tasks. For example, JRS will re-use two publicly available datasets (MS COCO and ADE20K) in WP3. Where pre-existing data is used, it will be referenced and acknowledged accordingly. Should any permissions for re-use be required, the DIDYMOS-XR partners will take the necessary steps to obtain these.

4.5.2 Increasing re-use of DIDYMOS-XR results

DIDYMOS-XR project partners will ensure that any deliverables which are classified as ‘PU – Public’ will be made publicly available on the project website once accepted by the EC and, where appropriate, in open access repositories, such as Zenodo. Files that are made publicly available will be created in a common file format to ensure interoperability. With regards to datasets, these will be made openly available where possible through open source data storage and sharing platforms such as IEEE DataPort, Open Research Europe, and GitHub.

5 Other research outputs

DIDYMOS-XR intends to make a large part of its core technology developments, including parts of its methods, available as open source code or software on GitHub and/or other similar repositories, which will aid in making project results as reproducible as possible and allow the project to reach out to the community via the integrated issue tracking. The open access availability of these research outputs will, however, be subject to a proper licence scheme to protect the background and generated intellectual property rights, which will be identified in the exploitation strategy to be developed as part of T6.3 on 'Exploitation and innovation management'.

6 Protection of personal data

The DIDYMOS-XR project collects and processes personal data only if, and insofar as, it is necessary for its research and engagement activities, including desk-based research, consultations, interviews and events, and to share its findings and results with stakeholders and other interested persons via mailings, the project website, and newsletters. In conjunction with the responses supplied by partners to questions on personal data processing in the DMP questionnaire (see Annex III), the purpose of this section is to outline how personal data that is collected and processed by the partners for their work in the project will be protected in accordance with the General Data Protection Regulation (GDPR) and other national data protection law as applicable. The section proceeds by first providing an overview of the types of personal data, including sensitive data, before outlining the different principles of the GDPR and elaborating on how the DIDYMOS-XR partners will abide by and adhere to them. Following this, the section provides a summary of the rights of data subjects under the GDPR, as well as the requirements applicable to international data transfers between partners within the project, highlighting here the relevant sections of the project's Research Privacy Policy included in Annex IV. Finally, a list of persons responsible for data management within project partner organisations is included at the end. Issues relating to data security and ethical aspects of data are then covered in Sections 7 and 8, respectively.

6.1 Types of personal data

Where personal data is processed under the GDPR, a legal basis is required. In the DIDYMOS-XR project, all partners have provided an appropriate legal basis for processing such data (see Annex III). The primary legal bases relied upon by partners within the DIDYMOS-XR project are consent (Article 6(1)(a) GDPR) and legitimate interest (Article 6(1)(f) GDPR). However, in order that partners reduce the risks of processing personal data as far as practicable, DIDYMOS-XR partners prefer to process pseudonymised or, ideally, anonymised data.

Personal data is defined under Article 4(1) GDPR as:

> '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.'[30]

With respect to how identifiable a data subject is, 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.'[31] Where it is not 'reasonably likely' that a data subject can be identified, then such data can be treated as anonymous data. However, anonymisation can be a high threshold to meet, and all objective factors should be considered when making such an assessment, particularly in terms of data subjects being singled-out, linkability between the supposedly anonymous data and other personal data, and the potential to infer personal data from a supposedly anonymous data subject.[32]

Where steps have been taken to de-identify a data subject, but it is still possible to identify them using additional information (e.g., the original names of data subjects have been replaced with alpha-numeric tokens), then the data are pseudonymised.

[30] Art.4(1), GDPR.
[31] Recital 26, GDPR.
[32] See, e.g., Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, Adopted on 10 April 2014, pp.11-12. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

As stated in the GDPR:

> 'pseudonymisation means the 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.'[33]

As it would be possible to identify a data subject using additional information, pseudonymous data is still personal data. All partners should, therefore, treat pseudonymous data as personal data and provide a legal basis for the processing of such data. In general, partners will take all steps practically possible to minimise personal data and allow the research purposes to be reached.

6.2 Sensitive personal data

Personal data that reveals very personal or private details can be seen as sensitive. Under the GDPR, there are two types of sensitive data:[34] special category data,[35] and criminal conviction/offence data.[36] Only the former is relevant to the DIDYMOS-XR project, the processing of which is subject to a conditional prohibition.[37] It follows that in order to process such special category personal data, a relevant exemption under Article 9(2) must apply in addition to an applicable legal basis under Article 6 GDPR.[38]

Special category personal data is defined under Article 9(1) GDPR as:

> 'personal data 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,

[33] Art.4(5), GDPR.
[34] Recital 51, GDPR.
[35] Art.9, GDPR.
[36] Art.10, GDPR.
[37] Art.9(1) GDPR.
[38] Art.9(2)(a)-(j), GDPR.

data concerning health or data concerning a natural person's sex life or sexual orientation.'[39]

The exemptions most likely to apply to the project are consent, scientific research, and where processing relates to personal data which are manifestly made public by the data subject.[40] Regarding consent, this should be explicitly given by the data subject for the processing of those personal data for one or more specified purposes that are described to them.[41] The scientific research exemption requires that processing for scientific purposes must include safeguards for the data subject, as required under Article 89(1) GDPR and national law, such as pseudonymisation, where possible.[42] Partners relying on these exemptions are acting in compliance with these legal requirements.

6.3 Lawfulness, fairness and transparency

The project will only process personal data relating to data subjects in a lawful, fair and transparent manner.[43] Personal data is processed in the project only insofar as it is necessary for the purposes of research, dissemination, and exploitation of the project results.

6.3.1 Lawfulness

Our primary legal bases for processing personal data within the DIDYMOS-XR project are consent (Article 6(1)(a) GDPR) and legitimate interest (Article 6(1)(f) GDPR). Where relying on the former, such as in surveys and/or interviews to validate chosen use cases in WP2, informed consent procedures shall be followed, with information sheets including all necessary information in compliance with Article 13 GDPR (see Section 6.3.3 below) to be provided to data subjects. In accordance with Article 7(1)(3), data subjects have the right to withdraw their consent at any time without any negative consequences. Accordingly, where individuals subscribe themselves to receive the DIDYMOS-XR project newsletter or use the 'Contact Us' function on the project website, they will have the option to opt-out of future communications. In addition to

[39] Art.9(1) GDPR.
[40] Art.9(2)(e) GDPR.
[41] Art.9(1)(a) GDPR.
[42] Art.9(1)(j) GDPR.
[43] Art.5(1) GDPR.

consent, an additional legal basis relied upon by the DIDYMOS-XR project for communication and dissemination activities in WP6 is legitimate interest. This is applicable in circumstances where the legitimate interests of the project partners are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of their personal data.[44] An example of our reliance on legitimate interests within the project is for the creation of contact lists for stakeholder engagement and dissemination of information. A legitimate interest assessment (LIA) has been conducted, and a copy of it is attached to this deliverable in Annex V. Like those whose personal data is processed on the basis of consent, data subjects contacted on the basis of the legitimate interests of the DIDYMOS-XR partners are free to opt-out of all project communications, including the newsletter managed by TRI through the platform Zoho,[45] at any time by clicking on the 'unsubscribe' option.

6.3.2 Fairness

The fairness principle requires that personal data are processed in a way that is fair, and also requires consideration of whether the personal data is processed in a way that is unfair, such as data collected by deception, data processed in an unreasonable way, or having an unjustified impact on data subjects.[46] No data collected, or re-purposed, by the project is, or was, collected by deception. The collection of some data, such as image and/or video data of pedestrians and vehicle number registrations, might be unexpected by data subjects, but is supported by an applicable legal basis for this processing (see Annex III).

6.3.3 Transparency

The principle of transparency requires that information addressed to the public or to a data subject is concise, easily accessible and easy to understand, with clear and plain language and, where appropriate, visualisation is used.[47] Transparency requirements are provided under Article 13 GDPR where data is collected directly from the data subject, and Article 14 where data is not collected from the data subject. All partners act in accordance with these requirements at all times. When any personal data is collected, partners provide information required under Article 13 on information sheets and/or informed consent forms provided to data subjects. Where personal data is

[44] Art.6(1)(f) GDPR.
[45] The privacy policy for which is available here: https://www.zoho.com/privacy.html
[46] Kuner, C., Bygrave, L., and Docksey, C. 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, OUP, Oxford, p.314; ICO, *Guide to the GDPR*, ICO, p.22.
[47] Recital 58 GDPR.

processed in the project that was not collected as part of the project, such as with the re-use of research datasets, all partners do their best to provide the information required under Article 14 to data subjects directly. However, noting that the majority of personal data used in research is pseudonymised and/or anonymised, it is difficult to determine the identity of the data subject in order to provide them with relevant information under Article 14. As such, where it is impossible, or would require disproportionate efforts, to notify a data subject under Article 14, partners provide information about their processing publicly available, as required under Article 14(5)(b), through the project Research Privacy Policy (see Annex IV). To ensure the project has made its best efforts to notify data subjects of the processing of their personal data, this privacy policy is shared on project communication channels, including the website, and will be updated as necessary during the project lifecycle.

6.4 Purpose limitation

The principle of purpose limitation requires data to be collected for a specific, explicit, and legitimate purpose. Or, if data are re-used, that the purpose of secondary processing is compatible with the original purpose. Recalling that scientific research in and of itself is a legitimate purpose,[48] the research activities conducted within the DIDYMOS-XR project are for the specific and explicit purposes detailed in the project GA. Further, the processing of personal data for communication activities are for the specific and explicit purposes of disseminating information on the DIDYMOS-XR project to interested stakeholders as required under the GA, which does not create disproportionate effects on data subjects and are therefore legitimate.

The repurposing of datasets in the DIDYMOS-XR project only occurs where this is compatible with the original purpose for collection. For communication and dissemination activities in WP6, the re-purposing of contact details to share information about the project with people who we have identified as being interested in it is, therefore, compatible with the original purpose, recalling as well that the re-purposing of personal data for scientific research purposes is, in accordance with Article 89(1) GDPR, not considered to be incompatible with the initial purposes.[49]

[48] Recitals 156-162 GDPR.
[49] Art.5(1)(b) GDPR.

6.5 Data minimisation

The principle of data minimisation requires that personal data are adequate, relevant, and limited to what is necessary for specified purposes.[50] Partners follow good data governance practices and collect no more personal data than is necessary. DIDYMOS-XR partners ensure that only data which is adequate, relevant and what is needed for their tasks is collected and/or processed. For example, contact details collected for the purpose of forming and coordinating the activities of the Ethics Advisory Board (EAB) will solely be used for this specific purpose. As such, partners do not collect extraneous information from data subjects where such personal data is not required to complete the task for which it was initially collected and/or processed.

As described in Section 6.1 above, the DIDYMOS-XR partners aim to minimise the amount of personal data they process, whilst still enabling specified research purposes to be met. This involves the use of pseudonymisation and anonymisation techniques where practicable. Such techniques used by partners within the project include the removal of identifiers within the data at the time of collection and the random numbering of datasets, the assignment of a unique identification number to data subjects and an aggregation of the data within particular datasets, and heavy pixelation of datasets, such as after processing by a human shape detection algorithm.

6.6 Accuracy

The principle of accuracy requires that personal data are kept up-to-date, and that any errors or inaccuracies are rectified, or, if necessary, destroyed. Should DIDYMOS-XR partners be made aware that any personal data they are processing is inaccurate, then they will rectify such data. If it is not possible, then they will seek to erase the data. However, in view of the possibility that these data may be essential to fulfilling research purposes, then the DIDYMOS-XR partners will need to assess how this principle can be fulfilled whilst also meeting the stated research purpose(s).

[50] Art.5(1)(c) GDPR.

6.7 Storage limitation

In addition to minimising the amount of data collected and processed within the project, partners will also limit the length of time it retains these data. The principle of storage limitation requires that personal data is not kept, or kept in an identifiable form, for longer than is necessary to achieve the purposes for which these data are processed.[51] This requires in particular that the period for which the personal data are stored by partners is limited to a strict minimum.[52] In line with this, where identifying information is no longer needed, it will be destroyed. Partners will review the personal data they hold for DIDYMOS-XR on a regular basis. When partners find that they are holding personal data that they do not need for their future work within the project, these data will be destroyed.

However, Article 20 of the DIDYMOS-XR GA, in conjunction with point 6 of the Data Sheet, requires project partners to retain records and documentation of their work within the project for five years following receipt of final payment from the EC. As such, personal data may be retained for this period of time where it is necessary to do so for purposes such as confidentiality, record-keeping and impact evaluation. Additionally, some partners have indicated in their responses to the DMP questionnaire that they will retain research data, potentially including personal data, for a longer period of time (e.g., up to 7 years) for legal and/or auditing reasons.

6.8 Integrity and confidentiality

The principle of integrity and confidentiality requires that appropriate security measures are put in place to protect personal data against unlawful or unauthorised processing, accidental loss, destruction or damage. DIDYMOS-XR partners will take appropriate technical and organisational measures to protect personal data, including anonymisation, pseudonymisation and/or encryption. Each partner has detailed the measures they will take to protect personal data in their response to the DMP questionnaire (see Annex III).

[51] Art.5(1)(e) GDPR.
[52] Recital 39; Art.5(1) GDPR.

6.9 Accountability

The principle of accountability requires that data controllers are responsible for complying with the above mentioned principles, and are able to demonstrate their compliance with them. Partners are able to demonstrate compliance through providing necessary information either in this DMP and/or their organisational policies on research data management and the protection of personal data, which are outlined in Tables 3 and 4 in Section 3 above. Further, a specified individual who is responsible for data management per partner organisation is provided in Section 6.12 below.

6.10 Rights of individuals

As outlined in Section 10 of the Research Privacy Policy (see Annex IV), individuals whose personal data is processed by DIDYMOS-XR partners within the project have the following rights as data subjects under the GDPR:

- The **right to withdraw consent at any time**, following which DIDYMOS-XR will cease further processing activities involving their personal data. However, this will not affect the lawfulness of any processing already performed before consent has been withdrawn (Article 7(3) GDPR);
- The **right to access** to the personal data processed in the DIDYMOS-XR project that pertains to them (Article 15 GDPR);
- The **right to be provided with a copy** of the personal data pertaining to them that is collected and/or processed by the DIDYMOS-XR partners (“the right to data portability”) (Article 20 GDPR);
- The **right to request the rectification** of any inaccurate personal data concerning them that is held by the DIDYMOS-XR partners (Articles 16 and 18 GDPR);
- The **right to request erasure** of their personal data (“the right to be forgotten”) (Article 17 GDPR);
- The **right to object** to the processing of their personal data by partners in the DIDYMOS-XR project (Article 21 GDPR);
- The **right to object to automated decision-making** (Article 22). However, the DIDYMOS-XR project does not engage in any automated decision-making;
- The **right to lodge a complaint** with a supervisory authority if they believe that their rights have been infringed (Article 77 GDPR).

As noted above, please refer to Section 10 of the Research Privacy Policy in Annex IV for more information.

6.11 International data transfers

As outlined in Section 8 of the project Research Privacy Policy (see Annex IV), two of the partner organisations within the DIDYMOS-XR consortium are located outside the European Union (EU). In case personal data is transferred, the requirements applicable to such data transfers between these and EU-based project partners are as follows:

- **AUB** are based in Lebanon. Law No.81 of 10 October 2018 on Electronic Transaction and Personal Data ("the Law") governs the processing of personal data in the Republic of Lebanon. Whilst the Law does not explicitly make provision for data transfers, the AUB Privacy Statement stipulates that third party providers must meet and adhere to strict data protection standards that are EU GDPR-compliant or of equivalent standard.
- **TRI** are based in the UK. The UK has implemented the GDPR in its national law under the Data Protection Act 2018. Since exiting the EU, the UK has implemented the GDPR into domestic law as the 'UK GDPR'. The EC implementation act of 28th June 2021 provides that the UK, for the purposes of Article 45 GDPR, ensures an adequate level of protection for personal data transfers from the EU to the UK. This adequacy decision is effective for four years following entry into force.

6.12 Persons responsible for data management in DIDYMOS-XR

The DIDYMOS-XR consortium is a collection of partners, each of which is a distinct legal entity. Therefore, each partner is either solely or jointly responsible (as in the case of joint controllership or controller-processor relationships) for the data they use. Listed below are the persons responsible for data management within the project.

Partner	Person responsible for data management within the project
AUB	Imad Elhajj
CAP	Hari Prasath Thirupathy

Partner	Person responsible for data management within the project
CERTH	Stella Papastergiou (DPO)
DTT	Kurt Sprengel
FICOSA	Romain Guesdon
FIWARE	Stefano de Panfilis and Udo Wenzel
HSHL	Jan-Niklas Voigt-Antons
i2CAT	Ivan Huerta
IW	Boulos El Asmar
JRS	Georg Thallinger
TRI	Irma Poder
TUB	Tanja Kojic
UNITY	Jamie Crabtree (DPO)
UPAT	Konstantinos Moustakas
VNG	Àlex Ginés

Table 6: Persons responsible for data management

7 Data security

Any personal data which partners do not retain is securely stored on the password-protected project NextCloud drive, or on other password-protected devices located on the premises of each partner organisation. In addition to the NextCloud drive, partners may store local copies of research data on their own machines, servers, or cloud-storage systems. See Tables 3 and 4 above for more information on the technical and organisational policies of each partner within the DIDYMOS-XR project consortium.

All partners as a minimum will:

- Ensure DIDYMOS-XR research data stored on their institutional servers is regularly backed-up with recovery ability;
- Ensure DIDYMOS-XR research data are safely and securely stored, with clearly defined access controls at the user level (e.g., via encryption, password protection, and restriction of access);
- Adopt good cybersecurity practices by protecting their own devices and servers through installing and updating anti-malware software and anti-virus software, and enabling firewalls;

- Ensure appropriate security and confidentiality of personal data, including preventing unauthorised access to, or use of, personal data and the equipment used for processing;
- Evaluate, where necessary, the risks of processing personal data and implement measures to mitigate them (e.g., pseudonymisation, anonymisation and/or encryption) in order to safeguard personal data;
- Ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation and considered against the risks and the nature of the personal/sensitive data to be protected.

Once the DIDYMOS-XR project has ended, responsibility for data security will default to those managing the DIDYMOS-XR project website (JRS/TRI), and those who manage the repositories where DIDYMOS-XR data will be available in the future.

8 Ethical aspects

Recognising that the research being carried out within the project could have ethical implications, the DIDYMOS-XR consortium is aware of the need to respect the ethical standards and rules of Horizon Europe. Article 14.1 of the GA requires that all partners carry out their work "in line with the highest ethical standards and the applicable EU, international and national law on ethical principles." Read in conjunction with Annex 5, which sets out specific ethics rules as a function of contact award, this means project partners are required to adhere to and comply with the following:

- Core ethical principles outlined in The European Code of Conduct on Research Integrity, including the highest standards of research integrity, reliability, honesty, respect, and accountability.[53]
- EU, international and national law, including the EU Charter of Fundamental Rights[54] and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.[55]
- The principle of proportionality, the right to protection of personal data, the right to the physical and mental integrity of persons, the right to non-discrimination,

[53] ALLEA (All European Academies). (2017). *The European Code of Conduct for Research Integrity* (Revised Edition). Berlin, Germany: The Berlin-Brandenburg Academy of Sciences and Humanities.
[54] Charter of Fundamental Rights of the European Union (2016/C 202/02).
[55] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos.11 and 14 (3 September 1953).

and the need to ensure protection of the environment and high levels of human health protection.

Ethics will be an ongoing consideration throughout the project's lifecycle. DIDYMOS-XR will follow a structured approach to identifying, assessing, working on and overcoming ethical issues, in line with its adoption of a privacy and ethics-by-design approach to the design, development and use of the tools being developed. This will primarily be achieved through the work of T2.2 'Ethics and data protection', for which TRI will conduct an impact assessment of issues raised by XR in different domains and provide advice to partners on how the consortium should address ethical issues in line with commonly accepted ethical principles. As part of this task, in April 2023, the DIDYMOS-XR project established an independent Ethics Advisory Board (EAB) comprising three external ethicists, who will be invited to review deliverables of interest to them and to offer their views on and possible solutions to ethical and social issues arising within the project. TRI will present the project's privacy and ethics-by-design solutions to the EAB, which will meet three times a year. Corresponding to this, Deliverables 2.2 and 2.4 summarise ethical and data protection issues identified in the project, describe the methodology for identifying these issues and how they are to be resolved, as well as the solutions presented to and discussed with the project's EAB. The first version of the 'Ethics, privacy and safety assessment report' was submitted in M18, with an updated version covering the second half of the project due in M36.

9 Responsibilities and allocation of resources

Task 1.3 of the DIDYMOS-XR project, as listed in the GA, is dedicated to data management. This task is led by TRI, which is responsible for the planning and overall coordination of this task, including information gathering and the writing of this deliverable. TRI have five person months (PMs) for this task, for which it is expected to develop and finalise this deliverable by not later than M6, and then to maintain it as a living document thereafter, with updates recorded as a minimum in M18 and M36 ahead of mid-term and final review, respectively. Project partners, each of whom has at least one PM for this task as listed in the GA, are responsible for providing relevant information, including by responding to the initial questionnaire circulated in March 2023 (see Annex I). Each project partner is also responsible for collecting, processing

and storing data within the project according to applicable ethical standards and legal requirements, as outlined in this document. Overall compliance will be overseen by TRI, as the task lead, along with JRS as Project Coordinator and WP1 lead. TRI will be available to partners for advice on data management throughout the project. However, each partner is responsible for ensuring their own compliance with the strategy and procedures outlined in this and other relevant documents.

Following submission of this initial DMP in M6, TRI will maintain and update the document as necessary throughout the entire lifecycle of the project. As outlined in the work plan for this task, data management issues are to be included as a standing item for discussion at one of the two bi-weekly project technical calls per month. Here, project partners are requested to inform TRI of any changes to their use of data within the project so that any corrective actions to the working version of the DMP can be recorded. Factors that may necessitate revisions to the DMP include: the availability of new data; the re-classification of existing datasets due to newly highlighted concerns; the availability of new or unanticipated datasets; changes in organisational data management, personal data or privacy policies, which have an impact on research data management within the project; changes in consortium composition; and external factors, such as changes to applicable data protection regulation.[56] DIDYMOS-XR partners are responsible for notifying TRI if any of these factors arise and of any other happenings which could have an impact on their use of data during the DIDYMOS-XR project. Partners are also advised to discuss any new data sources with their DPO and/or person responsible for data protection at their organisation..

Finally, TRI's role in coordinating data management within the project is closely related to its work in Task 2.2, for which it will meet with task leaders to identify, discuss and resolve potential ethical, data protection and legal issues arising in their tasks. So far, this has included discussions on the appropriate legal basis for processing of different datasets, data protection impact assessments; data processing relationships (e.g., joint controllership); and international data transfers between EU and non-EU states.

[56] European Commission. (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*. European Commission Directorate-General for Research & Innovation. Version 3.0. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

Where partners request further discussion about data processing in the DIDYMOS-XR project, or require assistance in dealing with data protection issues due to the particular nature of the project, TRI will hold such discussions and provide advice as necessary.

10 Conclusion

This deliverable has outlined the data management processes and procedures DIDYMOS-XR partners will follow to manage the production, collection and processing of data within the project. It provides an initial overview of the research and personal data that are expected to be processed within the project and how it meets the FAIR requirements. In addition, this deliverable has explained the measures that will be put in place to ensure that these data will be handled in a way that is compliant with legal requirements and ethical frameworks, as well as with due consideration for data security. As a living document, this deliverable will be continually updated as new information becomes available. Overall, each project partner is responsible for ensuring that their handling of data within the DIDYMOS-XR project complies with the procedures and strategies outlined in this document.

11 Annex I: Data Management Plan Questionnaire

1. Within your organisation, who is the person responsible for research data management and protection of personal data in the DIDYMOS-XR project?

2. Is your organisation required to have a Data Protection Officer (DPO) under Art.37 GDPR?[57]

3. Does your organisation have a policy on research data management?

If so, please provide a summary or link to it. If not, please provide a summary of applicable policies or legislation that inform your processes for keeping data secure and private (for example, your organisational policy on protecting personal data, applicable legislation, or industry standards that your organisation follows).

4. Does your organisation have a data protection/privacy policy? If so, please provide a summary or link to it here.

Dataset Questions

5. Please give an overview of the data you will process for the DIDYMOS-XR project.

6. Please provide details on the research data you will process.

You might want to create a table for each data set/type of data set. If so, copy the table as many times as you have data sets/types. Please note that ***personal data*** *are handled in* ***Question 8*** *below. For* ***shared datasets****, please refer to the supplementary doc available on NextCloud entitled* ***'Shared Research Dataset Questions'****.*

Question	Description
Name/type of data that you will collect. *If relevant, please name the dataset.*	
For what WP/task/deliverable is this data needed?	

[57] https://gdpr-info.eu/art-37-gdpr/

Please identify specific tasks/WPs/deliverables if you can.	
Data source. Collected or re-used? *Please explain where the data comes from, e.g., developed internally or re-used from previous project(s).* *If collecting, has this or will this need to be approved by an ethics review committee?* *If re-using, where did this data come from?*	
Data file format(s): *E.g., .doc, .docx, .xls, .pdf, .jpg, .mp3, .mp4, audio-visual*	
Data file size(s) *Please give an approximate size of the data. If unknown, give a likely range.*	
Dataset URL(s). *If available online, please provide the URL.*	
Describe the data and how you intend to process it.[58] *Please explain the purpose for the use of the data and how it contributes to the project's objectives.*	

[58] Pursuant to Art. 4(2) Regulation (EU) 2016/679 (General Data Protection Regulation, hereafter: GDPR), ''*processing' means any operation or set of operations which is performed* […], *whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*'.

What methods, software tools, or platforms will you use to process *(e.g., enter, create and analyse)* the data? *Please name relevant software, apps and hardware. Generic information (e.g., Windows PC) is not required.*	
Whom will this data be used by (data users)? *Please refer to specific research groups within the project/partner organisation*	
Who will be able to access these data at your organisation? *E.g., researchers working on the project, the organisation Data Protection Officer (DPO), all staff.*	
For what period do you intend to process this data? *Please note that the GA (Art.20 + Point 6) requires records and documentation to be kept for **5 years** after the final payment to prove implementation of the project.*	
How will you store the data?	
Could this data be useful for other researchers outside the project? If so, please specify.	

During the project, do you intend to share this dataset with the public?	

Data Protection and Security Questions

We strongly advise to contact your Data Protection Officer (DPO) or other person responsible for data protection in your organisation when providing this information. You can also ask TRI for advice.

7. Please specify your organisational policy on the protection of personal data.

8. Please provide details of the personal data you will process

If you plan to process[59] personal data,[60] please complete the following table:

Question	Description
What type of personal data will you process? *Please note 'personal data' means any information relating to an identified or identifiable natural person as per **Art.4(1) GDPR**.* *This may include names, opinions, in-text references to persons, email addresses, IP addresses, etc.*	
How will you collect this data?	

[59] See Art. 6 GDPR, or for re-purposing see Arts. 5(1)(b) and 6(4) GDPR.
[60] Pursuant to Art. 4(1) 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*'.

Please explain why it is necessary to process personal data or why non-personal data is insufficient.	
What is your legal basis for processing?[61] *Please see Art.6 GDPR, or national law if non-EU.*	
Are these personal data considered 'sensitive'? *Please note sensitive data are those listed as special category under **Art.9 GDPR**. This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health, sex life and sexual orientation.*[62]	
If you answered yes to the above, please provide the relevant exemption under Article 9(2) GDPR, and national law if required, for such data processing.[63]	
If your legal basis or special category personal data exemption is consent under Art.9(2)(a) GDPR, how is this collected, how can you demonstrate this, and can it be revoked?	

[61] Art. 6 GDPR provides six legal bases for processing: (a) consent; (b) performance of a contract; (c) legitimate interest; (d) vital interest; (e) legal requirement; and (f) public interest. Please note that your country may provide for additional legal bases for processing personal data.
[62] See further: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
[63] See further: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

Are there any ethical concerns about the data? *Please consider whether your processing of personal data could create any risks that could affect data subjects. This is particularly relevant for TRI's work in T2.2.*	
Will these data be subject to anonymisation, pseudonymisation, encryption, or another safeguarding measure? Please explain how. *For anonymisation, please explain how you will make it impossible for the data subject to be re-identified.*[64]	
File format(s): *E.g., .doc, .docx, .xls, .pdf, .jpg, .mp3, .mp4, audio-visual*	
How will you store the personal data?	
Who will be able to access these data? *Please also include the steps you will take to prevent unauthorised access to data.*	
Who will you share the personal data with?	

9. Are you engaged in any high-risk data processing and therefore required to complete a data protection impact assessment (DPIA) under Art.35 GDPR?

[64] For the definitions of pseudonymisation and anonymisation and their differences, see: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf (p. 8).

- Most applicably, if you are processing special category personal data, as defined in **Article 9(1) GDPR**, on a large scale and/or undertaking a systematic monitoring of a publicly accessible area on a large scale, you are legally obligated to conduct a DPIA.

10. Are you carrying out any international data transfers (i.e., bringing into the EU or transmitting out of the EU) of personal and/or sensitive data?

- a. If your organisation is transferring personal data to a country *outside of the EU*, you will need to explain why you are doing this, what data you are transferring, which country you are transferring to, and explain how the transfers are in accordance with **Chapter V of the GDPR** on international data transfers.[65]
- b. If your organisation is transferring data from a non-EU country *into the EU*, you need to explain why you are doing this, what data you are transferring, and explain how the data was collected lawfully in the country from which it is being transferred.

FAIR Requirements Questions

DIDYMOS-XR should comply with the **FAIR Principles**, according to which project data should be Findable, Accessible, Interoperable and Reusable.[66]

11. How will you make the data you are using findable and discoverable both during and following the project? E.g., use of metadata,[67] standardised file names, standard identification numbers, Digital Object Identifiers (DOIs), naming conventions, key words, version numbering.

12. How will data be made accessible both during and after the project? E.g., by deposit in a repository, if so, please specify which repository.

13. Which data produced and/or used will be made openly available by default? The key principle here is "as open as possible, as closed as necessary." If certain datasets cannot be shared, or are subject to restrictions, please explain why, clearly separating legal and contractual reasons from organisational policy or other reasoning. Please note that the Grant Agreement requires that all academic (peer-reviewed) publications are made open access.

14. What methods, software or platforms will you use to enter, create and analyse DIDYMOS-XR data? Please list any applicable data and metadata vocabularies, standards

[65] https://gdpr-info.eu/chapter-5/
[66] https://www.nature.com/articles/sdata201618
[67] Metadata is data that describes other data.

or methodologies you will follow to make your data **interoperable**.[68] If data is to be made publicly available, please specify how you will ensure the public can access it (e.g., publishing data in a commonly used file format, or providing open source software alongside the data).

15. Where will the data, associated metadata and documentation be deposited? (Preference should be given to certified repositories that support open access, such as Zenodo)

16. How will you exchange and re-use data with other members of the consortium?

17. If applicable, how will you exchange data with external stakeholders? Please note communication with the Ethics Advisory Board (EAB) and Stakeholder Board (SB) will primarily be channelled through Trilateral Research.

18. How will the data collected and generated in DIDYMOS-XR by your organisation be secured? Please include information on data recovery, safe storage, data transfer, etc.

19. What (if any) resources has your organisation allocated (i.e., costs, time, resources for long-term preservation) for DIDYMOS-XR research data management?

20. Please specify what (if any) regulations and standards your organisation subscribes to in relation to data management.

21. If you will create a research output other than data, what is your plan for making that findable, accessible, interoperable and re-usable? Please include any project result(s) that are not data and could be re-used, such as software, computer models, processes, toolkits, etc.

[68] The (meta)data use a formal, accessible, shared and broadly applicable language for knowledge representation.

12 Annex II: Overview of DIDYMOS-XR research data

Question/ Partner	AUB	TRI	UPAT	FIWARE	TUB	FICOSA	IW	CAP
Data type	(1) Images captured by visual sensor (2) Depth images, corresponding trajectory, ground truth mesh for training when needed.	(1) Academic and grey literature in relevant fields, such as journal articles, ethics guidelines, legal texts, industry reports, standards and other public deliverables and reports. (2) Work plans, internal notes, working documents, deliverables, articles and presentations.	We do not intend to collect our own data. We will use open access datasets, simulated data, and the data that are collected from other partners.	(1) Point cloud, oblique aerial photograph. (2) Footage from Community Hall in Etteln village.	Demographic, behavioural and attitudinal data.	(1) Raw data (2) Synthetic data	(1) 3D scan of industrial facility (2) 3D assets (3) Synthetic dataset (4) Change detection dataset (5)NeRF localization (6) Point cloud registration	NeRF, Point Cloud and 3D Mesh data.
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) MS COCO (2) ADE20K	Video recordings of user	Images and video files are expected to be used.	RGB and volumetric data of buildings,	PTZ-N24041-DE3 4MP – 4xIR Network PTZ Camera.	NeRF, Point Cloud and 3D Mesh data.	Odometry and GPS data; weather data provided by	

	(3) Kaiserfeldgasse (4) ADE20K (5) Cityscapes (6) Sim2Real (7) FICOSA Vilanova 500	interviews, workshops Demographic, behavioural and attitudinal data.		urban road and factory environments.			partners; image, video and point cloud data; spatial data	
WP/ Task/ Deliverable	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) WP4 (2) WP3 (T3.1; D3.1)	WP1 (T1.3); WP2 (T2.2 & T2.3); WP5 (T5.1 & T5.2) WP6 (T6.1 & T6.4)	WP3, WP4	WP5 – Etteln village use case.	WP2 – Validation of use cases	(1) WP1, WP3 & WP5; (2) WP3; T3.1	(1) & (2) & (3) & (4) & (5) & (6) WPs 4, 5 & 6	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) & (2) T3.2 (3) WPs 3 & 4 (4) WP3 (5) WP3 (6) T3.2 (7) WP3	WP2 (T2.1, T2.3) WP5 (T5.1, T5.3)	WP3 (T3.1, T3.3; D3.1) WP4 (T4.1, T4.2, T4.3; D4.1 & D4.2)	WP3 (T3.1, T3.2, T3.3) / WP4 (T4.3, T4.4)	WP5; D5.1	WP4 (T4.1, 4.2, 4.3 & 4.4) & WP5	T3.4, T4.1, T4.2; D3.1, D3.2; D4.1, D4.2.	
Data origin	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Collected live by the on-board visual sensor(s). (2) Mainly collected, developed internally.	(1) Collected from public sources and relevant repositories. (2) Developed internally	N/A	(1) Collected using a drone (2 over flights) (2) Footage manually taken with mobile phone.	Collected through user studies, to be approved by an ethics committee.	(1) Collected via recordings in the real world and public roads in Spanish territories (limited to Catalonia – Vilanova i a la Geltru)	(1) Collected via 3D capture of real-world facility. Approval from ethics review committee not required.	All data will come from that collected in the various work packages. CAP will not collect additional data.

						(2) Re-used data from previous research activities or other research projects. (3) Data will be created expressly for the project; some could be re-used from our repositories. FICO is creating these datasets together with a third-party who provides the software (rFpro).	(2) Proprietary 3D models of factory assets. (3) Manually generated simulation environment including the 3D assets. (4) 3D capture of IW R&D environment. Not including any personal or confidential information (5) Recorded dataset (ROS bags) from IW's iw.hub. Not including personal or confidential information (6) Multiple 3D captures of IW R&D environment. Not including any personal or confidential information	
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	

	(1) & (2) Re-used public dataset (3) Re-used dataset from previous project (4) Re-used public dataset (5) Re-used public dataset (6) Re-used public dataset (7) Annotations created for data recorded in DIDYMOS-XR.	Collected during user interviews. Collected during user studies	The primary source of data will be datasets provided by other partners, namely FICOSA and IW.	Re-use of common datasets: (1) CWI Point Cloud Social XR (2) COCO dataset (3) DTU (4) ZJU-Mocap (5) CMU (6) Tanks and temples (7) NuScenes (8) KITTI. Newly collected data No need for approval from an ethics review committee.	Re-using data collected from 4 cameras installed in the city of Vilanova I la Geltru.	All data will come from that collected in the various work packages. Unity will not collect additional data.	Primarily collected by DIDYMOS-XR partners, in particular FICOSA, FiWare, and IW. DTT also plans to use data from the open data repositories provided by third parties to train the AI algorithm.	
Format	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) .jpg, .webm, .mp4. (2) .png (or other) for depth images; .txt (or .log or	.docx .pdf .xls .ppt	N/A	(1) 3D tiles (2) .mp4	.xls	(1) psd, mp4, jpeg, plys, PCDs, Csv, ncom, docx, doc, xls, pdf (2) .mp4, .bmp,.csv.	(1) .e57 (2) .USD or .fbx (3) .png for RGB data + annotation files (.json, .png)	.fbx, .obj, .png, .nvol, .gltf, glb, .b3dm.

	other) for trajectory; .ply (or other) for point cloud scans/mesh.						(4) rosbags (.db3) + .png (5) rosbags (.rosbag) (6) rosbags (.db3) + .png	
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) & (2) JPEG images, JSOn metadata (3) Point cloud, .laz (4) & (5) JPEG, PNG, JSON (6) JPEG, PNG, OBJ (7) JPEG, PNG, JSON	.mp4, .csv , .xls	PNG, JPG, MPG & MP4.	Jpg, mp3.mp4,rgb,rgbd, rgbxyz (point cloud)	Audio-visual	.fbx, .obj, .png, .nvol, .gltf, glb, .b3dm.	IMU: CSV GPS: GPX or CSV Traffic: CSV, XML, JSON Weather: JSON, CSV Database of images: synchronised images (.jpg/.png)	
Size	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Depends on the duration of the SLAM application. (2) - A set of 3000 depth images takes about 2xx MB in size. - An additional >1GB if corresponding	Approx. 5GB by the end of the project	N/A	(1) 2.1 GB (2) Measured in seconds: 1 minute 36 seconds	Unknown	(1) 2GB approx. (2) 340 MB approx. per 1 dataset (4 sensors).	(1) ~50GB (2) ~5GB (3) ~10 GB compressed (4) ~17.7 MB (5) ~6.8 GB compressed (6) ~4.4 MB	Unknown

	images are stored too (could be used for generating depth images via MVS). - Trajectory takes < 1 MB - Ground truth point cloud of rooms potentially > 1GB (e.g., a normal size room takes around 1.7 GB).							
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) ~19 GB (2) ~10 GB (3) ~2 GB (4) ~1.5 GB (5) ~55 GB (6) ~1.6 GB (7) ~200 MB	Max 1GB	Approximate size of the data may vary, but is expected to range from several GBs to TBs.	10 – 50 GB	(i) Video bitrate 32 Kbps to 16384 Kbps (ii) Audio bitrate 64 Kbps (G.711)/16 Kbps (G. 722,1)/16 Kbps (G.726)/32 Kbps to 160 Kbps (MP2L2).	1-10GB	Depending on the data format type (e.g., .jpg, .xls, etc.), the approximate size may vary, although would likely be between several GBs and TBs.	
URL	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) & (2) N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	

	(1) https://cocodataset.org (2) https://groups.csail.mit.edu/vision/datasets/ADE20K/ (3) N/A	https://nxc.joanneum.at/index.php/s/eF9HBrKXyP7SWyP	No dataset URLs are currently available.	N/A	N/A	N/A	Currently no dataset URL is available.	
Description	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) The image data is the main input to the Hybrid SLAM application. (2) An indoor place is scanned using a highly accurate imaging laser scanner (Lecia BLK360) to generate a ground truth point cloud/ mesh. - Multi-sensors	(1) TRI will analyse these data and use them to inform project deliverables. (2) TRI will initially use these data internally and share with relevant partners with whom we collaborate on specific tasks.	N/A	(1) Scan Data are loaded into the viewer of virtual city systems to provide access to the 3D model of the village. (2) Footage has been recorded the purpose of developing Use Cases	User study data can be processed using statistical analysis, qualitative coding, or machine learning algorithms to extract insights that inform design decisions and improve the user experience. Processing the data helps designers and developers to	(1) Acquisition of the raw data with sensors implemented in the car for smart mobility use cases or others that come up during project implementation. Purpose: Multisensory sync, multisensory fusion, 2D data enhancement, 3D reconstruction, 3D data enhancement.	(1) Used as basis to generate a digital twin simulation (2) Used as basis to populate a digital twin simulation with factory assets. (3) synthetic images generated form simulation of industrial environment, including the factory assets	Data will represent objects that can be rendered within Unity. Objects may be streamed or downloaded into the Unity editor and runtime for the purpose of rendering these objects in XR.

	(asynchronous, collaborative) setup: at least two depth sensors capturing the space while tracked by an OptiTrack system. - The mesh + depth streams (from both sensors) + their trajectories will be used to train a learning-based 3D reconstruction system. This system learns sensor-dependent noise to predict which sensor performs better on which part of the scene.				better understand user needs and preferences, contributing to the project's objectives of creating more intuitive and effective products and services.	(2) These data sets will only be used in the initial phases of training the algorithms as support to real data.	(4) multiple 3D captures of same area, each time with a change or assets arrangement, to develop methods for change detection (5) ROS bags captured from iw.hub to test NeRF-based indoor localization approaches developed in the project (6) Multiple areas are scanned of the same environment while making sure that there is an overlapping area between the different scans. The	

							registration algorithm will find the overlap and patch the scans together.	
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) 330K images (>200K labelled), 1.5 million object instances, 80 object categories, 91 stuff categories, 5 captions per image and 250,000 people with key points. Will be used as training and validation data for object detection and segmentation methods. (2) 27,574 images (25,574 for training and 2,000 for	The dataset is composed of video recordings of the user interviews done for the elicitation of the use cases, system requirements and user needs.	Images or video streams depicting places in a city or manufacturing environments. The main aim of the methods we are developing is to perform 3D reconstruction and localisation with high accuracy on visual data.	Training and testing the multi-camera, multi-object detection and tracking, Nerf and super-resolution techniques used.	Data collected by 4 cameras 1/3" progressive scan CMOS up to 2560 x 1440@25fps resolution.	Data will represent objects that can be rendered within Unity. Objects may be streamed or downloaded into the Unity editor and runtime for the purpose of rendering these objects in XR.	For some of these data types (e.g., IMU, GPS), we intend to use them to transform and align other sensor data with respect to the scene, while other will be used to interpret the scene, or judge the reliability of information (e.g., surface reflection changes due to weather conditions).	

	testing) spanning 365 different scenes. 707,868 unique objects from 3,688 categories, along with their WordNet definition and hierarchy.193, 238 annotated object parts and parts of parts. Polygon annotations with attributes annotation time, depth ordering. Will be used as training and validation data for object detection and segmentation methods. (3) Point cloud of a static scene							

	with ~7 Mio points. (4) Indoor and outdoor scenes with semantic and instance segmentation annotations of objects and object parts. (5) Vehicle view scenes of different cities with semantic and instance segmentation s. (6) CAD models of 12 object classes, and real images with ground truth segmentation. (7) 500 images from Vilanova,							

	captured using FICO's car, with semantic segmentation annotations.							
Method/ Software/ Tools used to process	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Ubuntu, ROS, C++, Open CV. (2) Each industrial camera has an SDK - "Motive" is the software needed to process the data coming from OptiTrack - App and PC software specific to the Lecia BLK 360 - Matlab could possibly be used to synchronise the depth streams with	TRI will file, analyse and produce these data on our internal SharePoint drive, as well the shared DIDYMOS-XR NextCloud.	N/A	(1) Virtual city systems https://vc.systems/en/ (2) Mobile camera.	Collected through standardised questionnaires and SPSS. Data analysis methods will depend on the type of data collected and research questions.	(1) Data recording: Adasens Computer Vision (ACV) tool, media gateway device an internal software tool. (2) FICO will use the rFpro software environment, which allows us to set-up specific configurations, scenes or environments and obtain images and data from it.	(1) NaVvis IVION instance; Unity 3D game engine. (2) Unity 3D game engine (3) Unity 3D game engine (4) rosbags and LSLiDAR C32 LiDAR (5) idealworks' onboard 3D stereo camera Lips Edge AE400, rosbags (6) rosbags and LSLiDAR C32 LiDAR	Unity

	OptiTrack output.							
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-2), (4-5) & (7) DNNs (3) & (6) DNNs & renderers	Interviews were recorded on Webex. Answers have been converted in an Excel Sheets and stored in the shared project folder .	The data will be processed using methods and software tools for 3D reconstruction and localisation. This may include techniques like Neural Radiance Fields (NeRF) and relevant software and tools. Hardware requirements may involve powerful computing resources, GPUs, and high-capacity storage.	Internally developed and owned software tools	Yet to be determined.	Unity	The data will be used for training, testing and deploying machine learning algorithms and models being developed. Development tools/frameworks such as Python, Keras, UNity, etc., would be used to process and analyse the data.	
Data users	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) & (2) Possible users include the following: UPAT,	TRI as task leader/contributor, along with project partners	N/A	(1) (2) Future users of these data will be	Researchers working on the project.	(1) Partners of the project who need access for implementation of their tasks	(1) & (2) & (3) & (4) & (5) & (6) Members of WPs 3 & 4.	Members of the DIDYMOS-XR consortium and end users of the

	CERTH, i2CAT, Unity, JRS.	working on the above tasks.		citizens of Etteln		subject to access control requirements. (2) Accessible only for the implementation of the project, with the following specifications for each partner: (i) CERTH – Data enhancement and sensor data synchronisation and integration (ii) UPAT & AUB - data enhancement, semantic segmentation, object detection and tracking, 3D reconstruction and AI algorithmic training. (iii) i2CAT – data enhancement, 3D data compression, point cloud compression, object detection		project use cases.

						and tracking, 3D reconstruction and AI algorithmic training. (iv) JRS – semantic segmentation, object detection and tracking, AI algorithm training.		
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1) & (2) XRECO teams of the following partners: JRS, i2CAT, AUB, UPAT. (3-6) JRS (7) XRECO teams of the following partners: FICO, JRS, i2CAT, AUB, UPAT, DTT, CERTH	TUB & HSHL	WP3/WP4 partners such as i2CAT, UPAT, AUB and FICOSA.	Technical, academic research and industrial partners	Technical partner in WPs 3 and 4.	Members of the DIDYMOS-XR consortium and end users of the project use cases.	These data will be used by researchers and , project employees within the identified WPs.	
Access	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) & (2) Researchers working on the project.	All TRI staff with access to the password-protected	N/A	(1) (2) Researchers working on the project.	Researchers working on the project.	(1) Researchers working on the project; workers on a need-to-	(1) & (2) & (3) & (4) & (5) & (6) Researchers and members	Members of CAP Digital twin team, R&D and T&I team.

		internal SharePoint.				know basis and subject to access control requirements; consultants. (2) Researchers and interns working on the project; consultants involved in the project.	of the digital simulation team.	
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-7) All research group members.	Jan-Niklas Voigt-Antons & Francesco Vona	Access to the data will be granted to the authorised individuals and teams from the research group VCL involved in the project who require it for their specific tasks.	Researchers working on the project	Technician to be hired	Members of Unity's Digital Twin team, DPO, Unity Cloud Services.	Researchers and other project employees (e.g., developers) who are working on the identified WPs and tasks will be able to access these data.	
Time period	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) & (2) 8 years	These data will be produced, collected, and analysed throughout	N/A	(1) (2) For the duration of the project	For the duration of the project, plus the necessary retention of documents.	For the duration of the project, as stated in the consortium agreement.	(1) & (2) & (3) & (4) & (5) & (6) 7 years	During the length of the project

		the duration of the project (i.e., Jan 2023 – Dec 2025). In accordance with Art.20 GA, records and logs will be kept on file for 5 years after the end of the project.						
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-6) At least for the project duration (7) unlimited	The collected data will be stored, analysed till the project is finalised (i.e. April 2023-July 2026) or as long it is necessary for legal reasons	The duration of the project. As per the GA, records and documentation related to project implementation should be kept for at least 5 years after final payment. Therefore, we will ensure that all data processing activities and associated records are maintained and	3-5 years	Dec 2023 – Dec 2027	During the length of the project	These data will be processed during the whole lifecycle of the project. We will follow the GA requirements of record-keeping, which states that records and documentation related to the project should be kept for at least 5 years after the final payment.	

			persevered for the timeframe mandated by the GA.					
Storage	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Video format (.webm or .mp4) on researcher PC and personal drive on cloud. (2) Images (depth, RGB) in folders, per sensor - Two trajectory files (.txt, .log, etc) - A ply (or any other format) for the GT mesh Storage on local PC and personal cloud drive.	Data will be stored securely on TRI's internal SharePoint and the shared project NextCloud, both of which are password-protected.	N/A	(1) Cloud storage as part of the DiDoZ project (2) Internal partner storage	In excel and SPSS file.	Local servers located on the premises (Amazon Web Services); AWS GDPR Data Processing Addendum.	(1) & (2) & (3) & (4) & (5) & (6) SharePoint; local storage.	The intention is to store all data in a repository shared with the consortium. If any assets are stored outside the consortium will be stored in a secure repository.
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-2) & (4-6) Local storage of partners (3) Network attached storage	Next cloud	Stored on a network storage device without public access (I.e., accessible only	Internal organisation storage (Drive, GitLab)	Undecided at this stage	The intention is to store all data in a repository shared with the consortium. If any assets are	These data will be stored on internal network storage devices that can be	

	(provided to partners per SFTP). (7) Local storage and Zenodo		through VCL's local area network).			stored outside the consortium will be stored in a secure repository.	accessed via VPN.	
Useful for others?	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Yes, the data provides a benchmark/ reference for future researchers to build upon. (2) Yes, this data could be used for mulit-sensor 3D reconstruction algorithms (training/ evaluation).	Yes, these data could be useful for other researchers in related fields. However, all deliverables marked as sensitive will be limited under the conditions of the project GA.	N/A	(1) Yes, these data could be useful e.g., for the Waterverse project where a flood warning system is planned. (2) No further usage foreseen.	Yes, user study data can be useful for other researchers in related fields to inform their own research and design decisions, as well as for benchmarking and replicating findings. Sharing data can contribute to the larger scientific community, but it's important to ensure participant privacy is protected.	(1) Yes, these data may be useful for other internal projects that implement the same type of sensors and operational domain design (ODD). (2) According to limited uses of these data, it can only be useful for other internal research projects agreed with rFpro.	(1) & (2) & (3) & (4) & (5) & (6) No	Other researchers who work in the same/similar domains would potentially benefit from these data.
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-6) Yes, for the identified	Interviews are not meant to	Yes, the 3D reconstruction	Yes, for further AI-	Not at the moment.	Yes, large NeRF datasets and	Other researchers	

	project partners. (7) Made available to the public	be used by other partners. User studies data can be used for analysis	and localisation data could be useful for other researchers working in fields like urban planning, VR, AR, and related domains, Sharing the dataset with external researchers may lead to further advancements and collaborations.	based research		point clouds could be useful for other teams within Unity.	who work in the same/similar domains would potentially benefit from these data.	
Sharing with the public?	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**	**CAP**
	(1) Yes (2) Yes, at a later stage.	Final deliverables will be submitted to the EC and made publicly available (unless marked as sensitive) by upload to the Zenodo repository, as linked to on	N/A	(1) Yes (2) No (due to meaningless information for public)	No	(1) Sharing with other project partners (2) With project partners (above); any public repository is foreseen for that type of data.	(1) & (2) & (3) & (4) & (5) & (6) No	No

		the project website.						
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**	
	(1-7) Already publicly available.	Video interviews are not collected to be shared with the public. Data collected during user studies will be available upon request	Yes	Yes, in publication of papers.	Yes, maybe it will be possible.	No	Yes, on a case-by-case basis. We primarily plan to share the datasets used in related in related tasks/WPs at some point during the project.	

13 Annex III: Overview of DIDYMOS-XR personal data

Question/ Partner	AUB	TRI	UPAT	FIWARE	TUB	FICOSA	IW
Data type	Deidentified human subject survey such as the NASA-TLX. b	(1) Contact details (e.g., name, contact country, job title, company name & email address) of SB and EAB members, subscribers to the project newsletter and users of the 'contact us' function on the website. (2) In-text references to the names of authors of different publications.	We do not intend to process personal data.	No plans to process personal data. (1) Scanned images by drones don´t contain personal data. (2) Footage from Community Hall don´t contain personal data	Demographic data such as age, gender, education level, and occupation. Attitudinal data such as opinions, preferences, and emotions, to be collected through surveys or interviews.	Images/videos of pedestrians, plates	No personal data collected or processed within the project
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Images of city or manufacturing environments, which might also contain persons and vehicles.	Video recordings of user interviews. Demographic data such as age, gender, education level, and occupation. Attitudinal data such as opinions, preferences, and emotions, to be collected through surveys or interviews	Images or video streams depicting places in a city or manufacturing environment, which might contain persons & vehicles.	Images of natural persons	Not planned to process personal data at this stage	N/A	Images or video streams depicting manufacturing or cityscape environments (which might contain persons and vehicles).
Data origin	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**

	Collected using forms before, during and after testing of AR/VR and other interfacing applications	**Collected Directly** – E.g., agreeing to involvement with/registering for meetings of the EAB/SB; using 'contact us' function on the website; subscribing to the newsletter. **Collected Indirectly** – E.g., from research partners; public and open data sources; news articles and internet searches; social and professional networking sites e.g., LinkedIn.	N/A	N/A	Collected through user studies.	Collected using cameras, sensors, radars, etc.	Collected using robot's onboard 3D stereo camera, robot onboard 2D LiDARs, external 3D LiDARs
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Collected via moving (on vehicles) and static cameras operated by one of the use case partners.	Collected during user interviews, workshops Collected through user studies.	Collect using stationary or mobile cameras	Collected via video recordings	N/A	N/A	DTT will collect the data from partners involved in the project and responsible for the generation of data via cameras and LiDAR scanners. If, by any chance, DTT has to generate the data then we will be using the Matterport camera

							for the collection of it.
Necessity	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	To evaluate interfaces from human user perspective, we need to process opinions.	(1) To contact relevant persons regarding their role on the respective boards; (2) To cite authors' work according to referencing conventions.	N/A	N/A	To gain insights into participants' behaviours, preferences and attitudes. It can provide important context and help researchers understand how different demographics might use a product or service differently.	We need to provide raw data "as is" because one of the main characteristics of our datasets is to be useful for training algorithms to detect all objects found in a road, e.g., streets, pedestrians, traffic lights, sidewalks, etc.	To develop methods for digital twins generation and indoor localization in industrial environments
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Persons and vehicles will be part of the camera views.	User interviews: Answers extracted to elicit project use cases, needs and requirements User studies: To gain insights into participants' behaviours, preferences and attitudes. It can provide important context and help researchers understand how	Using cameras to capture data can result in the inclusion of individuals or vehicles within the camera's range.	Necessary to process these data to train algorithms to detect the objects found in real-world settings. These data are not the purpose of but rather incidental to the data collection.	N/A	N/A	Within this project we have a use case of city scanning, which means that while scanning, people, vehicles with their number plates and buildings with personal information might be scanned. People and vehicle number plates will definitely be removed before processing. Building information might be required for the localization

		different demographics might use a product or service differently.					or mapping requirements.
Legal basis	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	Consent (Art.6(1)(a) GDPR) Consent form completed prior to start of study.	For data collected **directly**: consent (Art.6(1)(a) GDPR & Art.6(1)(a) UK GDPR). For data collected **indirectly**: legitimate interest (Art.6(1)(f) GDPR & Art.6(1)(f) UK GDPR) – see Annex V	N/A	N/A	Legitimate interest (Art.6(1)(f) GDPR)	Under analysis. "Processing is necessary for compliance with a legal obligation to which the controller is subject" is being considered. (Art.6(1)(c) GDPR)	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Legitimate interest (Art.6(1)(f) GDPR)	Legitimate interest (Art.6(1)(f) GDPR)	Legitimate interest (Art.6(1)(f) GDPR)	Unknown at this stage. To be determined in consultation with FICO.	N/A	N/A	Legitimate interest (Art.6(1)(f) GDPR).
Sensitive (Art.9 GDPR)	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	No	Yes, contact country may reveal racial/ ethnic origin.	N/A	N/A	No	No	No
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	No	No	No	No	N/A	N/A	No
Exemption (Art.9(2) GDPR)	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	N/A	Consent (Art.6(1)(a) & Art.9(2)(a) UK GDPR; Art.6(1)(a) & Art.9(2)(a) UK GDPR. Legitimate interests (Art.6(1)(f) GDPR &	N/A	N/A	N/A	N/A	N/A

		Art.6(1)(f) UK GDPR) + data made public by the data subject (Art.9(2)(e) GDPR; Art.9(2)(e) UK GDPR).					
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Consent (Art.9(2)(a) GDPR))	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	N/A	Demonstrable and withdrawable at any time.	N/A	N/A	N/A	N/A	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Any ethical concerns	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	None specified at this stage	None that are identifiable at this stage. Any potential ethical concerns relating to these data will be identified, along with the steps taken to mitigate any risks in D2.2 & D2.4.	N/A	N/A	No, as these data are not the main aim of processing	No. We are managing the risks associated with the acquisition and recording of these personal data, but from a data protection not an ethical perspective.	No, as these data do not include personal information
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	No, as the personal data are not the main of processing.	No, as the personal data are not the main of processing.	No, since the primary objective of the data processing is not focused on personal data.	Data subjects are not directly identifiable within the raw data, which will then be anonymised where possible (see	N/A	N/A	No. We are not processing any personal data.

				below), so the overall risk of privacy harm is low.			
Anonymisation pseudonymisation and/or encryption	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	Anonymisation at time of collection. No identifiers are logged with the data. Data sets are randomly numbered	Most of the personal data collected by TRI will not be anonymised /pseudonymised as they are only for internal and restricted use within TRI/ the project.	N/A	N/A	Anonymisation via assigning a unique identification number to each participant and removing any identifying information, such as names, gender and/or occupation. These data will then be aggregated in a way that does not reveal the identity of individual participants.	No - raw data provided “as is”. Even though these data will not be pseudonymised, our entity does not associate the image with other data sources, so we will only manage disassociated data. E.g., We will have videos with pedestrians, but we will not know the identity of these pedestrians.	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Anonymisation through heavy pixelization might be applied, although this might influence the performance of the methods to be developed.	Anonymisation via assigning a unique identification number to each participant and removing any identifying information, such as names, gender and/or occupation. These data will then be aggregated in a way that does not reveal	To protect the privacy of individuals, anonymisation techniques such as heavy pixelation could be utilised.	When it is possible, these data will be anonymised. This will happen after processing by a human shape detection algorithm.	N/A	N/A	DTT will decouple the identity from image and video for the anonymisation of data.

		the identity of individual participants.					
Format	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	.docx and .xls	(1) .xls (2) .docx; .pdf; .ppt	N/A	N/A	.xls	.pcd, .mp4	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Jpeg, png, mpg, mp4.	.mp4, csv, .xls	PNG, JPG, MPG, MP4	Jpg, mp3, mp4 rgb, rgbxyz (point cloud).	N/A	N/A	PNG, JPG, MPG, MP4, etc., for the images and videos.
Storage	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	On local machine and OneDrive. Password protected.	On the project-designated repository, hosted on NextCloud, and TRI's internal SharePoint, both of which are secure, and password protected.	N/A	N/A	In Excel and SPSS file	Local servers on premises (Amazon Web Services); AWS GDPR Data Processing Addendum.	On the project-designated repository, hosted on NextCloud, and IW's internal SharePoint, both of which are secure, and password protected
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Stored on a network storage device	On the project-designated repository, hosted on NextCloud	Stored on a network storage device without public access (I.e., accessible only through VCL's local area network).	Internal organisation storage (Drive, gitlab)	N/A	N/A	DTT will be using the project repository for storing the data.
Access	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	Researchers collecting the data and PIs.	TRI staff with access to the internal SharePoint.	N/A	N/A	Researchers working on the project	Internal employees of FICO under a need-to-know basis. The access of these data will be restricted to those	Researchers working on the project

						employees who will need to treat such data.	
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Access will only be possible to the members of the research group Vision Applications of DIGITAL@JOANNEUMRESEARCH.	Researchers working on the project	Granted only to the member of the research group VCL	Researchers working on the project	N/A	N/A	Access has only been granted to the members of the research group.
Sharing	**AUB**	**TRI**	**UPAT**	**FIWARE**	**TUB**	**FICOSA**	**IW**
	None expected at this time. Future sharing contingent upon a data sharing agreement.	Data will be shared with project partners as necessary.	N/A	N/A	Other DIDYMOS-XR partners involved.	With partners of the consortium and identified stakeholders.	N/A
	JRS	**HSHL**	**CERTH**	**i2CAT**	**VNG**	**UNITY**	**DTT**
	Other partners involved in WP3/4	With partners on the project	Other partners in WPs 3 and 4	With partners on the project	N/A	N/A	Partners of WP3 & 4 within the project.

14 Annex IV: Research Privacy Policy

Research Privacy Policy (updated August 2024)

This privacy notice solely concerns the data processing taking place as part of research activities in the DIDYMOS-XR project. The Privacy Policy relating to the processing of personal data for the operation of the project website can be found here.

1. Overview

The purpose of processing:

We ("the DIDYMOS-XR consortium") process personal data to research extended reality (XR) applications and digital twin technology; to research the ethical, legal and data protection implications of these technologies; administer the project, including its events; and to communicate to stakeholders and other interested persons about project research. The vision of the project is to enable advanced and more dynamic XR applications, powered through artificial intelligence (AI). The project thus focuses on advancing technologies for creating large-scale digital twins synchronised with the real world, addressing uses cases in two domains that differ in scale and characteristics, namely cityscapes and industry environments.

Data controllers:

The DIDYMOS-XR consortium is made up of 14 partners from Europe and beyond. They are as follows:

- Joanneum Research (JRS) (AT)
- American University of Beirut (AUB) (LB)
- Centre for Research and Technology Hellas (CERTH) (GR)
- Internet i innovacio a Catalunya (i2CAT) (ES)
- Digital Twin Technology (DTT) (DE)
- University of Patras (UPAT) (GR)
- Ficosa (FICO) (ES)
- Technische Universität Berlin (TUB) (DE)
- Hamm-Lippstadt University of Applied Sciences (HSHL) (DE)
- FIWARE Foundation (DE)
- Neapolis (VNG) (ES)

- idealworks (IW) (DE)
- ~~Unity (DK)~~
- Capgemini Engineering Deutschland SAS & Co KG (DE)
- Trilateral Research Ltd. (TRI) (UK)

Your rights as a data subject:

If your personal data is processed by the DIDYMOS-XR partners within the project, you have the following rights as a data subject:

- You have the **right to withdraw consent at any time**, following which DIDYMOS-XR will cease further processing activities involving their personal data. However, this will not affect the lawfulness of any processing already performed before consent has been withdrawn.
- You have the **right to access** your personal data processed in the DIDYMOS-XR project.
- You have the **right to be provided with a copy** of your personal data that is processed by the DIDYMOS-XR partners.
- You have the **right to rectify** any inaccurate personal data concerning you that is held by the DIDYMOS-XR partners.
- You have the **right to request erasure** of your personal data ("the right to be forgotten")
- You have the **right to object** to the processing of your personal data by partners in the DIDYMOS-XR project.
- You have the **right to lodge a complaint** with a supervisory authority if you believe that your rights have been infringed.
- You have the **right to object to automated decision-making**. However, the DIDYMOS-XR project does not engage in any automated decision-making.

For more details, see Section 10.

Processing that could have an impact on data subjects:

The DIDYMOS-XR partners process several different sources of personal data within the project. One source is data collected during user interviews and surveys, for which data subjects will provide their consent. For the real-world mapping of the identified use cases, the data captured in cityscape environments, in particular, may contain personal data in the form of images and/or video streams of pedestrians and vehicle

registration numbers, of which the identifiable data subject(s) may not be aware. Such data will, however, be subject to pseudonymisation and, where possible, anonymisation techniques. Further, the contact details of people whom the DIDYMOS-XR partners believe would be interested in and a stakeholder for the project have been added to the project's contact list. Such persons can unsubscribe from any project communications they receive.

Responsible research:

The DIDYMOS-XR project seeks to comply with the fundamental tenets of Responsible Research and Innovation, and with national and European research ethics requirements, in a manner that has been developed in strict compliance with the relevant ethical and legal guidelines, provisions, procedures, and protocols that have been identified by the European Commission (EC) and project partners working on ethical and legal compliance. We put particular emphasis on privacy-awareness and legal compliance of the research and development within the project.

Regulatory model:

The DIDYMOS-XR consortium has followed a regulatory model with internal and external controls. Within the project, partners leading on ethical, legal and data protection issues analyse the project and work to implement recommendations to enhance the work of technical partners from ethics-and privacy-by-design perspectives. All partners work closely with their own Data Protection Officers (DPOs) or legal teams, and, where necessary, national Data Protection Authorities (DPAs) to comply with data protection requirements. Additionally, partners will, where applicable, seek approval from ethics committees. The DIDYMOS-XR project is overseen by an Ethics Advisory Board, comprised of three external ethicists, which provides advice to partners. Further, the EC sets requirements for the project to meet in order to evidence that it is complying with ethical and legal standards that are applicable to research.

General Data Protection Regulation (GDPR):

The DIDYMOS-XR project will only collect personal data insofar as it is necessary to collect these data for the completion of research, validation, dissemination, and exploitation of the project results. The DIDYMOS-XR project is a research project and, to this end, Regulation (EU) 2016/679 on the protection of natural persons with regard

to the processing of personal data and on the free movement of such data, known as the 'General Data Protection Regulation', hereafter 'GDPR', is the primary basis for the processing of personal data by partners within the project. The GDPR protects the rights of persons, known as data subjects, whose personal data is collected and/or processed. These various rights are set out in Section 10 below.

Contact details:

The contact details of the project coordinator and the project ethics, legal and data protection advisers are included below. For any questions about the processing of your personal data in the DIDYMOS-XR project, please feel free to contact them. If your personal data is being processed in the DIDYMOS-XR project, you can use these details to exercise your rights as data subjects.

Project coordinators:

Georg Thallinger and Werner Bailer < didymos-xr-office@joanneum.at >

Ethics and legal advisers:

Irma Poder < irma.poder@trilateralresearch.com >

2. Consortium and Controllership

The DIDYMOS-XR project consortium consists of 14 partners from 7 countries, as listed above. Organisations include technical, university, and small and medium-sized enterprises (SMEs) with expertise in technology, ethics, law and data protection. There is a broad spectrum of activities within the project. These activities include research about the technological ways to meet the requirements of users; research on the ethical, legal and data protection implications of the project itself; and communicating and disseminating information about the work of the project to stakeholders. In determining the purposes and means of processing personal data, the project was informed by all areas of partner expertise. In most cases, partners act as individual data controllers for the processing of personal data in their work in individual tasks. However, partners do also collaborate across tasks and where they jointly determine the means and purposes for processing, they are joint data controllers.

The specific tasks involved in the research are defined in the Grant Agreement ("GA") between the EC and the project partners. To achieve the technical or other objectives of tasks within the DIDYMOS-XR project, each task leader must further specify the remit and means of data processing. Typically, the data controller undertakes data processing activities. Each partner is responsible on an individual basis for adhering to data protection rules for the data processing activities carried out. This responsibility is exercised with an expectation of support from other project partners.

3. Purposes of Processing

The DIDYMOS-XR consortium processes personal data in order to effectively participate in a scientific research project which aims to develop more advanced, more realistic and more dynamic XR applications enabled by AI. The vision of the project is to advance the state of the art of enabling technologies that are ethical and privacy-aware by design, and which will allow for the creation of large-scale digital twins, synchronised in real-time with use cases in cityscape and industrial environments.

With this overarching vision in mind, the following purposes behind processing of personal data can be identified:

(a) Research, design and develop XR applications synchronised with digital twins.

(b) Research the ethical, legal and data protection implications of the project.

(c) Organise and administer the project, including its events; and

(d) Disseminate and communicate the outputs from the project.

The DIDYMOS-XR project is strictly a research project and processes personal data for the above purposes only. The DIDYMOS-XR consortium has no intention to monitor any person, or to take decisions against them.

4. Personal Data and Data Minimisation

Personal data is, as per Article 4(1) GDPR, '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'. Where actions in DIDYMOS-XR process personal data, the project engages in data minimisation. This will ensure that the processing of personal data is:

- **Adequate** – meaning sufficient to fulfil the stated purpose.
- **Relevant** – meaning the processing has a rational link to the stated purpose.
- **Limited** – meaning that only data necessary to fulfil the stated purpose is processed.

Partners will follow good governance ensuring that they only process personal data that is adequate, relevant, and limited to what is needed for their task(s). To this end, the DIDYMOS-XR project prefers to process anonymous (i.e., non-personal data). Pseudonymous data, if linked with additional information, has the potential to (re)identify individuals. However, re-identification of pseudonymised data provides no scientific benefit to the project, is not a project aim, and it is, therefore, a consortium policy to not re-attempt re-identification of pseudonymised data subjects. In addition, and above all else, only where necessary do project partners process personal data.

5. Categories of Personal Data Processed in the project

The DIDYMOS-XR project processes the following types of data for the following purposes:

- **Video and image data** to train algorithms in the detection of objects and other (more) static parts of real world city and manufacturing environments. The data captured may relate to an identifiable natural person, such as a pedestrian or registered vehicle owner, and therefore constitute personal data, although this is not the main aim of and is instead incidental to the collection of these data.
- **Recordings of opinions, needs and preferences** through surveys and interviews in order to understand how different demographic groups might use a product or service differently, and to validate the project's chosen use cases.
- **Text data** to train machine learning algorithms to extract insights from written responses to surveys and questionnaires that inform design decisions and improve user experience. An additional source of these data is in-text

references to the names of authors of different publications within project deliverables, the purpose of which is to properly cite these authors' work according to established academic referencing conventions.

- **Contact details** of persons in the project contact list to organise and administer the project and project meetings, including those of the external Stakeholder and Ethics Advisory boards, and to disseminate project outputs.

6. Transparency

This research privacy policy is intended to meet the requirements of Articles 13 and 14 GDPR concerning information on the purposes of and legal basis for the processing of personal data (Art.13(1)(c) and Art.14(1)(c)), which is to be provided to the data subject where personal data are collected from the data subject, and where personal data have not been obtained from the data subject, respectively. In relation to the latter, this obligation does not apply where provision of information would require disproportionate efforts, or otherwise render impossible or seriously impair the achievement of the scientific research purpose being pursued, in accordance with Article 14(5)(b) GDPR. However, appropriate measures will be established to protect the rights of data subjects, such as making the relevant information publicly available.

The legal basis for the processing of personal data required for research, validation, dissemination and exploitation activities in DIDYMOS-XR varies depending on the form of personal data and the nature of the data controller. This is the case across both the GDPR and relevant national law. The below provides an overview of the main legal bases and purposes for data processing relied upon in the DIDYMOS-XR project.

Personal data selected by partners for dissemination and communication purposes on the legal basis of legitimate interests:

- Entries in the DIDYMOS-XR contact list (contact details, not openly available).

Personal data collected by the project from data subjects on the legal basis of legitimate interests:

- Responses in user interviews (video data is contained in this dataset, but only speech data is processed from it; not openly available).

- Entries in the DIDYMOS-XR contact list (contact details, not openly available).

Personal data collected by the project from data subjects on the legal basis of consent:

- Responses in user interviews (video data is contained in this dataset, but only speech data is processed from it; not openly available).
- Responses to DIDYMOS-XR surveys (text data, not openly available).
- Entries in the DIDYMOS-XR contact list (contact details, not openly available).

Where the processing of personal data is based on the consent of the data subject, data subjects can withdraw their consent at any time by notifying the project partners using the contact details listed below (Section 11).

The following table presents the legal basis relied on by partners processing different categories of personal data. The information was gathered from project partners in their response to the DMP questionnaire. Please note that the partners located outside of the EU are obligated to act as if bound by EU law under the DIDYMOS-XR GA, and so, where applicable, an equivalent legal basis has been provided for them under EU law in addition to relevant national level. Please also note that datasets which do not contain personal data are not listed here.

Partner	Data type/datasets	Legal basis
AUB	Deidentified human subject survey, such as the NASA-TLX.	Anonymous data, so no legal basis required.
TRI	Contact details provided by data subjects	Art.6(1)(a) & Art.9(2)(a) GDPR; Art.6(1)(a) & Art.9(2)(a) UK GDPR.
	Contact details selected by project partners	Art.6(1)(f) GDPR & Art.9(2)(e) GDPR; Art. 6(1)(f) & Art.9(2)(e) UK GDPR (the legitimate interests pursued here are the effective dissemination of project content to people whom the project partners believe will be interested in it).

TUB	Demographic data, such as age, gender, education level and occupation, and attitudinal data such as opinions, preferences and needs of users	Art.6(1)(f) GDPR.
FICO	Image data of pedestrians and vehicle number plates	Art.6(1)(c) GDPR.
JRS	Image data of pedestrians and vehicle number plates	Art.6(1)(f) GDPR.
HSHL	Demographic data, such as age, gender, education level and occupation, and attitudinal data such as opinions, preferences and needs of users Video data collected during user interviews	Art.6(1)(a) GDPR.
CERTH	Images or video streams containing persons and vehicle number plates	Art.6(1)(f) GDPR
i2CAT	Images of natural persons collected via video recordings	Unconfirmed at this stage; to be determined.

Please note that only data relevant to the project's activities will be processed and analysed. The aim of processing the above data is to research XR applications and their synchronisation with real world environments through digital twin technology, and to organise events and disseminate information about these activities. Please also note that the DIDYMOS-XR project processes other datasets that do not contain personal data, the details of which are not included within this document and can instead be found within the project DMP (to which this Privacy Policy is attached).

7. Recipients of Personal Data

Personal data may be shared between research partners/institutions involved in the project strictly for the purposes of the project, provided appropriate agreements are in

place. Personal data processed for research purposes is not shared with third parties outside the project unless there is a legal obligation to do so.

8. International Data Transfers

A couple of partner organisations within the DIDYMOS-XR consortium are located outside the European Union (EU). The requirements applicable to data transfers between these and EU-based project partners are as follows:

- **AUB** are based in Lebanon. Law No.81 of 10 October 2018 on Electronic Transaction and Personal Data ("the Law") governs the processing of personal data in the Republic of Lebanon. Whilst the Law does not explicitly make provision for data transfers, the AUB Privacy Statement stipulates that third party providers must meet and adhere to strict data protection standards that are EU GDPR compliant or of equivalent standard.
- **TRI** are based in the UK. The UK has implemented the GDPR in its national law under the Data Protection Act 2018. Since exiting the EU, the UK has implemented the GDPR into domestic law as the 'UK GDPR'. The EC implementation act of 28th June 2021 provides that the UK, for the purposes of Article 45 GDPR, ensures an adequate level of protection for personal data transfers from the EU to the UK. This adequacy decision is effective for four years following entry into force.

9. Storage and Retention

Personal data will not be stored for longer than is necessary for research purposes pursued by the DIDYMOS-XR project. Over the course of the project, data will be reviewed periodically, and the necessity of ongoing storage assessed. Data which is no longer needed will be anonymised or deleted. The project is scheduled to end in December 2025, at which point each partner will individually re-assess whether further storage is necessary and lawful. The maximum duration will be five years following the completion of the project in order to fulfil reporting requirements to the EC stipulated in the project GA.

10. Data Subjects' Rights and Limitations

If your personal data is processed by DIDYMOS-XR consortium partners in the course of the DIDYMOS-XR project, you have the following rights, subject to the described restrictions.

Right to withdraw consent (Article 7(3) GDPR)

You can withdraw your consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent. It may mean that we are not able to provide certain services to you and we will advise you if this is the case.

Right of access (Article 15 GDPR)

You have the right to obtain confirmation as to whether or not DIDYMOS-XR consortium partners are processing personal data concerning you within the project and, where that is the case, to have access to these data. Upon request, and subject to Article 12 GDPR, we will provide you with a copy of your personal data undergoing processing free of charge and in a commonly used electronic form – see further "right to data portability" below.

Right to rectification (Articles 16 and 18 GDPR)

You have the right to obtain the rectification of any inaccurate personal data concerning you. If you have challenged the accuracy of your personal data and asked for rectification, you also have the right to request the restriction of processing (see below) while we are assessing your rectification request.

Right to erasure/to be forgotten (Article 17 GDPR)

You have the right to request that we erase your personal data on a number of grounds, including when we no longer need it for the purpose it was originally collected (Art.17(1)(a)) and after you withdraw your consent to processing (Art.17(b)).

Right to restriction of processing (Article 18 GDPR)

In certain circumstances, you have the right to request that we temporarily restrict our processing of your personal data if you contest the accuracy of your personal data,

prefer to restrict its use rather than have us erase these data, or require us to preserve it for you to establish, exercise, or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate ground to process these data. You can ask us to inform before we lift a temporary processing restriction.

Right to data portability (Article 20 GDPR)

You have the right to be provided with the personal data concerning you, which you have provided to the DIDYMOS-XR project on the basis of consent, or a contract, or where the processing is carried out by automated means, in a structured, commonly used and machine-readable format which can be used to transfer data.

Right to object (Article 21 GDPR)

You have the right to object to our use of your personal data in the DIDYMOS-XR project. In order to do so, you must provide us with specific reasons based upon your particular situation. Please note that the right to object is not an absolute right. The project will carefully consider your objection and provide an appropriate response. If the processing is carried out in the context of performing a task in the public interest (Art.6(1)(e) GDPR) or for a legitimate interest (Art.6(1)(f) GDPR), we can continue with the processing if we can demonstrate legitimate grounds for the processing which overrides your interests, rights, and freedoms. If the processing is carried out for scientific research purposes (Art.9(2)(j) GDPR), we can continue with the processing if the processing is necessary for the performance of a task in the public interest.

If any of the above are applicable in the circumstances pertaining to your objection, we will explain our decision to you, otherwise your data will be excluded from processing. You have the right to request the restriction of processing while we are considering your objection (see above). While considering your objection, we may need to keep some minimal information (e.g., email address) to deal with your request.

Right to lodge a complaint with supervisory authority (Article 77 GDPR)

Should you believe that your rights have been infringed, you have the right to lodge a complaint with the data protection supervisory authority where you reside, work, or where the alleged infringement took place. This is without prejudice to any other administrative or judicial remedy you have.

11. Limitations on Data Subjects' Rights

It is possible that national laws will exist that may in certain circumstances restrict the rights of the data subjects listed above. For example, national law may derogate from some of the rights set out above in circumstances where the data is processed for scientific research purposes, pursuant to Article 89(2) GDPR.

The project consortium is not obliged to maintain, acquire, or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR pursuant to Article 11(1). However, pursuant to Article 11(2) GDPR, in circumstances where data subjects provide additional information in order to exercise their rights, the DIDYMOS-XR consortium will handle the request in a manner compliant with technical and legal requirements. In this regard, the identity of the data subject, as well as their relation to the data referred to in the request has to be sufficiently verified.

Although data subjects' rights may be restricted under the conditions described above, all requests to the below mentioned points of contact will be carefully assessed on a case-by-case basis.

12. Contact Details

If you have any concerns relating to personal data processing within the project, please contact either the coordinating partner, namely JRS, or the partner leading work on data protection issues, namely TRI. The contact details for these partners can be found below.

Project coordinator:

Georg Thallinger and Werner Bailer < didymos-xr-office@joanneum.at >

Ethics and data protection lead:

Irma Poder < Irma.Poder@trilateralresearch.com >

15 Annex V: Legitimate Interest Assessment

Legitimate interest assessment (LIA)

of the creation of contact lists

for stakeholder engagement and dissemination of information

Last update: 27 January 2023

This document, prepared by Trilateral Research Ltd, provides the justification for the processing of personal data in the DIDYMOS-XR project and, more specifically, the creation of a contact list of stakeholders whom we will contact periodically to inform of project results by means of an e-mail, press release, newsletter or other means.

The DIDYMOS-XR contact list contains the names, titles, organisations and e-mail addresses of the individuals whom we identified in the course of a stakeholder analysis as being potentially interested in the results of our project, as well as stakeholders who have requested to be added to our contact list.

Data processing in the DIDYMOS-XR project includes collecting and sharing within the consortium contact details obtained from publicly available sources (such as on the website of stakeholder organisations) or provided by stakeholders themselves (such as through the project website), as well as sending information to contacts. Under the General Data Protection Regulation (GDPR), most bases for lawful processing of personal data require that such processing be 'necessary' for a specific purpose, such as the performance of a contract (Article 6(1)(b)). For the purposes of our project, the collection and sharing of contact data, and the sending of information to contacts about our project results are necessary for the project to achieve impact, to ensure that our target stakeholders are informed of the results of our project, and to engage with stakeholders to ensure that the technologies developed meet their needs and are accepted by the target user communities. Hence, our project results have a larger social purpose than simply benefiting the consortium partners ("the beneficiaries" in the terminology of the European Commission).

For EU-funded projects, such as ours, two legal documents are particularly relevant.

The first is the project Grant Agreement (GA), Article 17(1) of which states that beneficiaries of Horizon Europe projects have an obligation to "promote the action and its results by providing targeted information to multiple audiences (including the media and the public), in accordance with Annex I and in a strategic, coherent and effective manner." This clearly indicates that consortia are obliged to disseminate their results to multiple audiences, which implies the need to compile a contact list targeted at multiple audiences in a strategic and effective manner, i.e., not just a random list of people who visit the project's website and ask to be put on the contact list. It has to be a *targeted* and *strategic* contact list. Hence, we consider that the GA serves as a valuable justification for the DIDYMOS-XR consortium to process personal data for this purpose.

The second is the GDPR, which outlines several possible bases for the lawful processing of personal data under Article 6. For example, Article 6(1)(a) permits the processing of personal data with the **consent** of the individual concerned (the data subject). The various conditions for consent, as set out in Article 7, include that consent is informed, "freely given", and withdrawable at any time. An additional basis is Article 6(1)(f), which allows processing necessary for the **legitimate interests** pursued by the controller or by a third party. The DIDYMOS-XR project has a legitimate interest for processing personal data on the basis of Article 17.1 (Communication – Dissemination – Promoting the action) of its Grant Agreement, as referenced above. Through this we are obliged to inform stakeholders, including the public, about our project, disseminate and communicate its results.

Legitimate interest is the most flexible lawful basis for processing but must be carefully assessed in each specific case. The existence of a legitimate interest also depends on the **reasonable expectations** of the persons concerned, where we use people's data in ways they would reasonably expect and where such use would have a minimal privacy impact, and where there is a compelling justification for the processing. Most stakeholders on our contact list have their e-mail addresses on their organisation's website, that is, they have already made their contact details publicly available, hence, they must have a reasonable expectation that others will contact them. Others have specifically requested to be added to the contact list.

In addition, a balancing exercise must be conducted between the legitimate interests of the project and the interests of the data subjects concerned. For this balancing, DIDYMOS-XR consulted the website of the Information Commissioner's Office (ICO), the UK data protection authority, which offers detailed guidance on how to conduct the balancing exercise,[69] and on which the following is adapted.

The ICO says that there are three elements to the legitimate interest basis. We must

1. *identify a legitimate interest* – As stated above, we have a legitimate interest, under Article 17(1) of the GA, to process personal contact details in order to create impact for our EU-funded project.
2. *show that the processing is necessary to achieve it* – 'Necessary' means that the processing must be a targeted and proportionate way of achieving our purpose. We must collect the contact details of stakeholders across the EU in order to inform them of the progress of the project and its results, enable them to participate in ongoing consultations as part of the co-development of XR technologies and applications, and to enable them, as the expected future users of the technologies developed, to use the results of our project. The processing is necessary as we could not reasonably achieve the same result in another way.
3. *balance it against the individual's interests, rights and freedoms* – A balancing test is conducted below, which we are confident demonstrates that the consortium's legitimate interest does not infringe upon the individual's interests or fundamental rights.

As noted below, our processing of personal data will not cause harm any more than any other e-mail to our stakeholders. We are not using people's personal data in ways they would find intrusive, or which could cause them harm. We will always offer stakeholders an option to unsubscribe from our contact list.

69 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Safeguards

Even though we believe there are no significant risks to the data subjects of their being on our contact list and sending them relevant news, we have considered safeguards to further reduce any risks, as follows: Trilateral Research Ltd commits to keep its contact list in a secure, password-protected file to which only a limited number of individuals will have access on a need-to-know basis.

As we wish to rely on legitimate interests as the basis for processing data on our contact list, we have conducted this legitimate interest assessment (LIA) before we start the processing. According to the ICO, an LIA is a type of light-touch risk assessment based on the specific context and circumstances of processing. It helps ensure that processing is lawful. Recording our LIA also helps to demonstrate compliance in line with our accountability obligations under Articles 5(2) and 24 GDPR.

The Information Commissioners Office (ICO) posits the following questions as part of its LIA exercise. Opposite each question in the left-hand column, we give our response in the right-hand column.

First, identify the legitimate interest(s).

Why do you want to process the data – what are you trying to achieve?	We wish to inform stakeholders about the development in the DIDYMOS-XR project of technologies enabling more advanced, more realistic and more dynamic extended reality (XR) applications, powered through artificial intelligence (AI).
Who benefits from the processing? In what way?	The consortium partners benefit from the processing because they are able to inform our contacts about the results of our project. Stakeholders also benefit because they will have the possibility to contribute to the development of DIDYMOS technologies to ensure these fulfil their needs and they will eventually have access to advanced XR applications for cityscapes and the industrial environments.
Are there any wider public benefits to the processing?	Yes, the special attention given to including end-users and transdisciplinary research including social sciences and

	humanities will enable and enhance the uptake of suitable, ethical and safe XR applications.
How important are those benefits?	Very important, especially if they can help technology and application developers to prioritise ethics and privacy-awareness by design in the tools and technologies they develop. The project will give stakeholders from the target domains the tools they don't currently have. The project consortium already includes technical experts, research bodies, and academics, and they can evidence the potential benefits to other potential users.
What would the impact be if you couldn't go ahead?	It would affect our ability to fulfil our contractual obligation.
Would your use of the data be unethical or unlawful in any way?	No, we will follow good data protection practices and established ethical guidelines.

Second, apply the necessity test.

Does this processing actually help to further that interest?	Yes, this processing will help our legitimate interest to inform stakeholders about the development of tools aimed at helping them.
Is it a reasonable way to go about it?	Yes, it is the only way to enter into direct contact with the stakeholders – apart from telephoning them directly, which would be more intrusive than an e-mail.
Is there another less intrusive way to achieve the same result?	As above. Telephoning would be more intrusive.

Third, apply the balancing test.

By applying the balancing test (based on the questions below), we consider the impact of our processing and whether it overrides the interest we have identified.

What is the nature of your relationship with the individual?	The individuals in this instance are the various stakeholders across the EU. Stakeholders are our targets for the tools being developed and so this relationship is potentially significant.
Is any of the data particularly sensitive or private?	No. We are collecting only basic contact data that is already publicly available. In addition to the contact details we have compiled, some stakeholders visiting the

	DIDYMOS-XR website have asked to be put on our contact list. We keep a log of such requests.
Would people expect you to use their data in this way?	Yes, especially stakeholders who have put their contact details on their websites. Hence, they must have a reasonable expectation that people will contact them. In addition, the circulation of e-mails informing stakeholders about EU-funded project outcomes is a common practice in the field, and we assume that the carefully selected stakeholders will receive this communication positively.
Are you happy to explain it to them?	Yes. We will inform our contacts about the mission of our project and how its results could be of assistance to them. We will also inform them about the project's privacy policy. Our privacy policy will respond to the requirement under Article 14 GDPR to provide information to the data subjects.
Are some people likely to object or find it intrusive?	No, as mentioned above, they have an interest in knowing about the project's results.
What is the possible impact on the individual?	There is no negative impact on the individual. We expect only a positive impact, in the sense that Stakeholders will become aware of how our project's results could help them. Typically, we would expect to e-mail our stakeholder contacts no more than a few times a year.
How big an impact might it have on them?	As above.
Are you processing children's data?	No. We do not aim to do this.
Are any of the individuals vulnerable in any other way?	Not that we are aware of.
Can you adopt any safeguards to minimise the impact?	We want to maximise the (positive) impact of and for the project. However, as noted above, we are implementing safeguards to protect our contact list – notably, our contact list file is securely stored, password-protected, and only a few individuals have access to the file. For further details, see the project's privacy policy.

Can you offer an opt-out?	Yes, we include an “unsubscribe” option for all our communications with stakeholders, such as, newsletters, press releases, and project flyers.

The decision on legitimate interest

Based on the foregoing, we conclude that legitimate interest under Article 6(1)(f) is an appropriate basis for our processing of personal data, as described above. We are confident that our legitimate interests are not overridden by any risks to the data subject.

Next steps

We will inform our contacts that we are relying on legitimate interest for the processing of their contact details, and we will explain what this interest is, specifically by drawing to the attention of stakeholders the focus of DIDYMOS-XR on the research and development of ethical, privacy and safety-by-design technologies for creating large-scale digital twins, synchronised with the real world, specifically for use in cityscape and industrial environments.

We understand that if we want to process the personal data for a new purpose, we may be able to continue processing under the legitimate interest provision as long as our new purpose is compatible with our original purpose. If necessary or useful, we will conduct a new LIA to demonstrate compliance with this requirement.

We will keep this record of our LIA on file in order to demonstrate compliance with the GDPR, if required. We will also keep our LIA under ongoing review and repeat it if circumstances changes.