Onto-DESIDE GA number: 101058682

ONTO-DESIDE

DELIVERABLE

D8.1 OEI – Requirement no. 1

Deliverable number	D8.1
Deliverable name	OEI – Requirement no. 1
Work package	WP8
Lead partner	LIU
Contributing partners	Ethical Advisor
Deadline	2022-08-31
Dissemination level	SEN
Date	2022-08-31

Funded by
the European Union

Project information

Project summary

Circular economy aims at reducing value loss and avoiding waste, by circulating materials or product parts before they become waste. Today, lack of support for sharing data in a secure, quality assured, and automated way is one of the main obstacles that industry actors point to when creating new circular value networks. Together with using different terminologies and not having explicit definitions of the concepts that appear in data, this makes it very difficult to create new ecosystems of actors in Europe today. This project will address the core challenges of making decentralized data and information understandable and usable for humans as well as machines. The project will leverage open standards for semantic data interoperability in establishing a shared vocabulary (ontology network) for data documentation, as well as a decentralized digital platform that enables collaboration in a secure and privacy-preserving manner.

The project addresses a number of open research problems, including the development of ontologies that need to model a wide range of different materials and products, not only providing vertical interoperability but also horizontal interoperability, for cross-industry value networks. As well as transdisciplinary research on methods to find, analyse and assess new circular value chain configurations opened up by considering resource, information, value and energy flows as an integral part of the same complex system. Three industry use cases, from radically different industry domains, act as drivers for the research and development activities, as well as test beds and demonstrators for the cross-industry applicability of the results. The developed solutions will allow for automation of planning, management, and execution of circular value networks, at a European scale, and beyond. The project thereby supports acceleration of the digital and green transitions, automating the discovery and formation of new collaborations in the circular economy.

Project start date and duration

1st of June 2022, 36 months

Project consortium

No	Partner	Abbreviation	Country
1	Linköping University	LiU	Sweden
2	Interuniversitair Micro-Electronica Centrum	IMEC	Belgium
3	Concular Ug Haftungsbeschrankt	CON	Germany
4	+Impakt Luxembourg Sarl	POS	Luxembourg
5	Circularise Bv	CIRC	The Netherlands
6	Universitaet Hamburg	UHAM	Germany
7	Circular.Fashion Ug (Haftungsbeschrankt)	FAS	Germany
8	Lindner Group Kg	LIN	Germany
9	Ragn-Sells Recycling Ab	RS	Sweden
10	Texon Italia Srl	TEXON	Italy
11	Rare Earths Industry Association	REIA	Belgium

Document reference

Project acronym	Onto-DESIDE			
Programme	Horizon Europe			
Grant agreement number	101058682			
Project URL	https://ontodeside.eu/			
EU Project Officer	Giuseppina LAURITANO			
Project Coordinator	Name	Eva Blomqvist	Phone	+46 13 28 27 72
	E-mail	eva.blomqvist@liu.se	Phone	
Project Manager	Name	Svjetlana Stekovic	Phone	+46 13 28 69 55
	E-mail	svjetlana.stekovic@liu.se	Phone	+46 701 91 66 76
Deputy PC	Name	Olaf Hartig	Phone	+46 13 28 56 39
	E-mail	olaf.hartig@liu.se	Phone	
Deliverable name	OEI – Requirement no. 1			
Deliverable number	D8.1			
Deliverable version	1.0			
Deliverable nature	ETHICS			
Dissemination level	SEN			
Due data	2022-08-31			
Delivery date	2022-08-31			
Keywords	Ethics, ethical assessment, ethical risks			

Document change log

Version	Date	Description	Authors	Checked by
0.1	2022-08-10	First draft	Kai Kimppa	Eva Blomqvist
0.2	2022-08-28	Second draft	Eva Blomqvist	Kai Kimppa
0.3	2022-08-30	Draft edited based on review	Kai Kimppa	Eva Blomqvist, Reviewer: Fenna Blomsma
1.0	2022-08-31	Final version	Eva Blomqvist	Svjetlana Stekovic

Document approval

Version	Date	Name	Role in the project	Beneficiary
0.3	2022-08-30	Fenna Blomsma	Internal reviewer	UHAM
0.3	2022-08-30	Kai Kimppa	Ethical Advisor	
1.0	2022-08-31	Eva Blomqvist	PC	LIU

Table of Contents

1. Summary

The Onto-DESIDE project deals with data sharing, hence also ethical aspects of sharing data between organisations will be important to address. This has been pointed out by the EC during the proposal evaluation phase, and the grant negotiation. Based on that assessment, ethical requirements were stated, including (1) to appoint an external ethical advisor (EA), who will supervise the project on ethical aspects, and (2) who will each project year assess the project with respect to those aspects in a report submitted to the EC.

The General Assembly of the project has in July 2022 appointed an EA, adjunct prof. Kai Kimppa, University of Turku, with background and considerable experience acting as EA. The EA will follow the project work closely and participate in various meetings, including each General Assembly meeting, to report on his view on ethical aspects in the project, and to raise awareness of any ethical risks that should be considered in the project risk assessment. Further, after each project year, the EA will submit a yearly report on ethical aspects to the EC.

In this deliverable, the EA has identified the overall ethical aspects of security, privacy, confidentiality, and bias, as the main relevant aspects for the project. However, at this point, the EA does not foresee any major issues regarding any of these aspects, but they should still be monitored and considered throughout the project implementation.

2. Introduction

The project targets the main challenge of methods and tools for decentralised secure and confidentiality-preserving data sharing for supporting the circular economy. Since the project deals with data sharing, ethical aspects of sharing data between organisations will be relevant to address, as well as ensuring that a minimal amount of personal data is handled, in order not to run into any privacy issues. This has been pointed out by the EC during the proposal evaluation and grant negotiation phases, and detailed in an ethical assessment statement. In response to that assessment, ethical requirements were put on the project, including mainly (1) to appoint an external ethical advisor (EA), who would follow and supervise the project in ethical aspects, and (2) who would each project year assess the project with respect to those aspects and submit a report to the EC.

2.1 Objectives

The objectives of this deliverable is to present (1) the appointed external ethical advisor (EA), and (2) to give an overview of the potential ethical issues that can be identified in relation to the project objectives and work plan.

2.2. Introduction to deliverable

The deliverable gives an introduction to the ethical concepts relevant for the project, in section 3. Then presents the appointed EA in section 4, and an overview and discussion of the specific ethical issues that will become relevant for the project, in section 5, as viewed by the EA. The deliverable is concluded with a summary of the actions taken so far, and next steps, in section 6.

Since the project has just recently started, and the detailed description of use cases and technical requirements are not yet finalised, potential ethical issues can in this deliverable only be discussed at a general abstract level, while the EA will then get a more detailed understanding of the potential issues as soon as detailed use case descriptions are available (e.g. through D6.1, delivered in September 2022).

3. Ethical Concepts

The potential ethical issues discussed in this deliverable are related to the following general concepts:

Security (computer security, cybersecurity) is needed to protect the users' data from unauthorised access for viewing, misusing, or altering it. This applies both to data of individuals working for organisations as well as the data of the organisations themselves.

Privacy of the individuals using systems needs to be secured. Only relevant data for the use of a system should be saved in it to minimize potential misuse of individual persons' data. It is worth noting that data of various transactions falls within the scope of privacy protection as well as it can indirectly be used to garner information about the users that ought not fall into unauthorised hands.

Confidentiality of data within a system needs to be protected, as at least some data about organisations can fall under trade secrets or be used as strategic advantage for the organisation. Only authorised individuals ought to have access to data in any system and there needs to be safeguards in place to ensure this.

Bias which favours certain users or user groups, and disfavours others can occur in any system that is complex enough and handles large amounts of data. Especially, but not only systems which use machine learning

methods bias from the data used for learning can reflect in the decision-making processes of the system. However, any suitably complicated algorithm can suffer from bias due to carelessness of implementation.

For privacy and confidentiality security needs to be implemented carefully, but security protocols by themselves are not necessarily enough to guarantee privacy or confidentiality, there needs to also be consideration on how data related to privacy and confidentiality is handled within a system and who has access to it.

4. Project Ethical Advisor

The project general assembly has decided to appoint adjunct prof. Kai Kimppa as the ethical advisor of the project. Kai Kimppa is a university research fellow and an adjunct professor at University of Turku. He does research in variety of ethical issues of ICT of privacy, security, IPRs, accountability and access to information within fields such as organisational ICT development in both private and public sphere, AI, computer games, augmented reality and beyond. For more information on his research see his Google scholar profile[1] and the homepage of the Future Ethics research group within University of Turku, which he is the leader of[2]. He has participated in various EU FP6 and FP7 projects as an external ethics advisor, most recently in the VALCRI project (FP7).

During the project lifetime, the ethical advisor (EA) will be invited to participate in all General Assembly (GA) meetings, and all consortium meetings. In both these types of meetings a dedicated slot will be planned for the EA to provide feedback and guidance to the project. Specifically in the GA discussions on risks and risk mitigation, care will be taken to involve the EA in order to capture and sufficiently deal with ethical risks. The EA will receive all project deliverables as soon as they are produced, to spot any potential ethical issues in them. The EA will provide a report directly to the EC (through the PO) after each project year, as D1.3-5 (Ethics assessment report).

5. Ethical Issues Relevant for the Project

During the project implementation, ethical considerations should be addressed both when producing, sharing and using data internally *within the project*, as a part of the research process, as well as considering *ethical issues and implications of the research output* of the project, i.e. the delivered ontologies, data sharing platform software, methods, and research data etc. The potential ethical issues that could concern the project seem to fall under the following general categories, as defined previously:

- Security
- Privacy
- Confidentiality
- Bias

Implementing robust **security** in the produced data sharing platform is of course necessary, as for any data sharing system, but it ought not be overly difficult, and is already included in the Solid[3] platform, which will be

[1] https://scholar.google.com/citations?user=Bnh6cP4AAAAJ&hl=en&oi=ao
[2] https://future-ethics.utu.fi/personnel/kimppa/

[3] https://solidproject.org/

the foundation of the data sharing platform to be built. As the system often does not handle actual data of the organisations, but rather proof that the organisations can deliver what is requested, this also reduces the security requirements. However, in some cases the actual data will have to be transmitted and shared with another organisation, whereby normal web security measures have to be used. Still, there are well-established methods for access control that can be used (c.f. the access control and authentication parts of the Solid specification[4]), and this will be checked as a part of the project internal quality checks of source code deliverables. Main challenges rather lie in the confidentiality aspect described below.

It is highly unlikely that the decentralised digital platform proposed in the project would cause major **privacy** issues, as there usually is no need to save significant personal information on any users in the system – only a minimal amount of relevant information (e.g. user IDs and login data), and this can be handled by the current EU and member state legal systems and standard technologies (c.f. references to Solid above). It is worth noting that the data of the participating organisations stays with the organisations, instead of being moved into the platform. This limits exposure of potentially sensitive data to other participants. Also, the system delivers mainly *proof of data*, not the data itself, thus in many cases not directly handling sensitive data at all. Hence, privacy concerns shall be monitored, but are not envisioned to play a large role.

The only exception foreseen to the above discussion on privacy and security, would occur if considerable *usage data* would be needed for some use cases. Usage data could mean to record and monitor the usage of some product or part by its end users, in order for such data to then be used for facilitating further analysis for supporting reuse, refurbishment etc. of the product. Usage data can be sensitive even when anonymised, and risks of de-anonymisation often exist. At the moment, no such use case is foreseen within the project, and such usage data will therefore most likely not be collected within the project. However, to make the platform extensible and exploitable in other use case in the future, i.e. after the project, the possibility of such data being held within the platform should be at least considered when the technical requirements regarding security and privacy are specified in WP2.

Again, proof of data rather than the actual data being delivered guarantees **confidentiality** of data in the system to a necessary extent, if implemented correctly. However, as mentioned earlier, in some cases data do need to be shared, and in those cases technologies for limiting the use and access period of data needs to be put in place and enforced by the system. This needs to be followed through the project and is a key issue of the system to be implemented, mainly related to activities in WP4. This WP already has several tasks planned in order to deal with confidentiality aspects, and the main technology (i.e. Solid) has been developed with exactly these aspects in mind, hence, the project has a good starting point for addressing these requirements.

Potential for **bias** in the platform needs to be followed as well. It does not seem likely, however that this would be a problem, since the system is mainly based on manually curated knowledge models, i.e. ontologies, rather than data-driven machine learning models. None the less, it is a point of concern and specific care needs to be taken in WP3, where models are created, as well as in WP6, where data is collected and/or produced. Bias will also be relevant to consider in WP5, where the methodology for development, assessment and formation of circular value networks is studied. However, WP5 will include such aspects in their research plan and methodology, to make sure it is considered in the manner appropriate for qualitative research and method development.

[4] More about authentication for Solid is described in the specification here: https://solidproject.org/TR/oidc , about identities here: https://solid.github.io/webid-profile/ , and about access control here: https://solidproject.org/TR/acp

In all the previous potential issues the fact that the platform will be created as **open source software** helps as well; any of the participating organisations can either themselves or through hiring a third party verify that the system works in a secure, privacy preserving, confidential and non-biased way.

Still, implementation of all these aspects need to be followed through the project, so that it can be verified that they are implemented correctly. On top of these potential ethical issues, the EA will be following the project implementation and will point out any other potential arising issues, and offer their expertise for solving any that arise from the previously identified areas or any other issues, if any are found.

6. Conclusion

The project has appointed an EA with background and considerable experience in acting as EA for projects similar to this. The EA participated in the online kick-off of the project, and has been invited to the upcoming project meetings, in order to be able to follow the project work closely. The EA will also be part of each General Assembly meeting, to report on his view on ethical aspects in the project, and to raise any ethical risks that should be considered in the project risk assessment. Further, in M12 of the project, the EA will submit his first yearly report on ethical aspects in the first project year (D1.3).

Overall, the EA has identified the general aspects of security, privacy, confidentiality, and bias, as the main relevant aspects for the project. However, at this point, the EA does not foresee major issues regarding any of these aspects, and most of these concerns and counter measures already appear in the work plan of the project WPs as well, but they should still be monitored and considered throughout the project implementation.