NGI TRUST CHAIN

D3.8 TrustChain Support to third party innovators

Guide for Open Call implementation - 2

07/11/2024

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D3.8 TRUSTCHAIN SUPPORT TO THIRD PARTY INNOVATORS

GUIDE FOR OPEN CALL IMPLEMENTATION - 2

Work package	WP3
Task	3.8
Due date	16/01/24
Submission date	7/11/24
Deliverable lead	ALA
Version	1.2
Authors	Pablo Vela (ALA), Alexander Herranz (ALA)
Other contributors	Caroline Barelle (ED), Andrés del Álamo (CIB), Thanasis Papaioannou (NKUA), Ruben Roex (TLX), Akanksha Dixit (ICS), Vlado Stankovski (UL), Petar Kochovski (UL), Vasilios Siris (AUEB)
Reviewers	Andrés del Álamo (CIB), Vasilios Siris (AUEB)
Abstract	This document presents the coaching, monitoring, and evaluation activities in the context of the TRUSTCHAIN project OC2 and provide the information needed for the selected applicants to successfully conduct their subproject work.
Keywords	Coaching, monitoring, evaluation of open call activities

Document Revision History

Version	Date	Description of change	List of contributors(s)
v0.1	11/01/2024	First version of the deliverable	Alexander Herranz (ALA) Pablo Vela (ALA)
v0.2	12/01/2024	First revision	Andrés del Álamo (CIB)
v0.3	15/01/2024	Review comments	Thanasis Papaioannou (NKUA)
v.1.0	16/01/2024	Deliverable final version	Pablo Vela (ALA)
v1.1	23/01/2024	Corrected final dates	Pablo Vela (ALA)
V1.2	06/11/2024	Made corrections to address comments from midterm review.	Petar Kochovski (UL), Thanasis Papaioannou (NKUA)

DISCLAIMER

The TRUSTCHAIN project is funded by the European Union's Horizon Europe Research and Innovation programme under grant agreement no. 101093274.

COPYRIGHT NOTICE

The TRUSTCHAIN Consortium is the following:

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	F6S NETWORK IRELAND LIMITED	F6S	IE
3	UNIVERZA V LJUBLJANI	UL	SI
4	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	AUEB	EL
5	FUNDACION CIBERVOLUNTARIOS	CIB	ES
6	CONSORCIO RED ALASTRIA	ALA	ES
7	TIME.LEX	TLX	BE
8	ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON	NKUA	EL
9	CITY UNIVERSITY OF LONDON	ICS	UK

EXECUTIVE SUMMARY

This document presents the guidelines for the implementation of the OC2 projects of TRUSTCHAIN. The scrum methodology for coaching and monitoring of the OC2 projects is described, and the contents of their required deliverables are outlined. Also, the evaluation criteria and KPIs for each deliverables are identified and a calendar of TRUSTCHAIN events for community building, for the SCRUM meetings and for the deliverables' deadlines is presented. Moreover, this document contains contact details of OC2 projects and of the TRUSTCHAIN coaches along with all other information needed by the selected applicants to successfully conduct their project's work.

TRUSTCHAIN produces a dedicated and self-contained implementation guide for each open call. Each guide includes both standardized information that applies across all open calls and content tailored specifically to the unique requirements of the respective open call. While certain information is thus repeated from one guide to the next, this approach is necessary to ensure completeness and clarity for the intended audience—the innovators.

Repeating material in each open call implementation guide, rather than simply including references to previous guides, enables each implementation guide to serve as a comprehensive, standalone, and self-contained document. This ensures that innovators have all relevant information at hand, without the need to cross-reference multiple documents. This structure enhances the ease of use and minimizes the chances for misunderstandings or gaps in guidance.

This strategy has been adopted to provide consistent, accessible information across all open calls, supporting the innovators in fully understanding both the general framework and the specifics of each open call.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AI	Artificial Intelligence
BaaS	Blockchain-as-a-Service
CCR	Cross-Cutting Requirements
DAO	Decentralised Autonomous Organization
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
DT	Digital Twin
GDPR	General Data Protection Regulation
ID	Identity
IoT	Internet-of-Things
IP	Internet Protocol
KPI	Key Performance Indicator
KYC	Know Your Customer
OC	Open Call
OLA	Operational Level Agreement
SLA	Service Level Agreement
SSI	Self-Sovering Identity
TCP	Transmission Control Protocol
TR	Technical Requirement
TRL	Technology Readiness Level
VC	Verifiable Credential
WP	Working Package
W3C	World Wide Web Consortium
ZKP	Zero-Knowledge Proof

1 CONTEXT

In an ever-evolving digital landscape, the importance of user privacy and data governance has taken a central stage. The internet has transformed the way we live, connecting us through our digital identities and influencing various aspects of our lives, from health and well-being to education and information access. However, this digital transformation has brought forth a multitude of challenges related to identity, trust, and the safeguarding of personal data.

As we navigate the digital realm, concerns such as delusion and manipulation, privacy violations, personal data exploitation, misinformation, and security breaches have become prevalent. The initial spirit of the internet, rooted in individual freedom, progress, and community values, is facing a paradigm shift towards individualism, materialism, and moralism, often straying from essential ethical and democratic principles.

In response to these challenges, Trustchain, a groundbreaking blockchain project, emerges as a beacon of hope. It recognizes that the convergence of Internet of Things (IoT), Decentralized Oracles, Artificial Intelligence (AI), Cloud-to-Edge computing, Distributed Ledger Technology (DLT), and Digital Twin (DT) technologies demands the creation of democratic systems that eliminate central points of control. Trustchain seeks to bridge the gap between universally agreed objectives in the physical world and their digital representations, thereby fostering trusted relationships in the Next Generation Internet.

To achieve this, Trustchain leverages various consensus mechanisms, pairing proofs with digital representations to help individuals discern the objective truth. This empowers users to make well-informed decisions, whether manually or through automated processes, fostering a Next Generation Trusted Internet that supports humanity in all facets of life.

In an era marked by global challenges and the United Nations' call for achieving 17 Sustainable Development Goals, Trustchain's mission is clear: to embed principles of human rights, sustainability, ethics, and other enduring values into the fabric of the Next Generation Internet. The core concept of Trustchain revolves around co-creating this future by deploying decentralized digital identity architectures in conjunction with IoT, AI, Cloud-to-Edge, DLT, and DT.

Trustchain envisions an ecosystem of user-centric blockchain solutions, processes, and business models with a strong market potential, particularly in trusted blockchain-based data management, metadata, ontology, knowledge, and information exchange. These solutions hold the promise of fostering trustworthy content handling, information exchange, and service delivery within the Next Generation Internet and vital sectors of the European economy.

Funded by the European Union

As part of its commitment to further this vision, the Trustchain consortium is set to launch a series of five Open Calls aimed at funding third parties who will contribute to the development of the Trustchain blockchain ecosystem. This Implementation Guide, dedicated to Trustchain OC2 – User privacy and data governance, offers a detailed roadmap for potential applicants, outlining the key steps from preparation and publication to evaluation and analysis.

In the upcoming sections, we will delve into the intricacies of Trustchain's Open Call, providing guidance, insights, and expectations for applicants, ensuring that this endeavour advances the cause of user privacy, data governance, and the evolution of a more democratic, transparent, and resilient digital future. Trustchain stands at the forefront of technological innovation, driving progress while upholding the values that have shaped our society throughout centuries of human evolution.

To implement this, a series of key activities have been undertaken as part of Trustchain's overall project structure (WP2):

- **Open Call Preparation**: This phase involves the meticulous creation of all necessary open call documents, including the open call text, guidelines, materials, and contract templates for sub-grantees. These templates are designed based on the collective experience of past partners in third-party financing.
- **Open Call Publication and Promotion**: Trustchain actively disseminates open call proposals on platforms like F6S while coordinating closely with the Dissemination WP to ensure effective promotion to a wide audience.
- **Open Call Evaluation**: A rigorous and transparent evaluation process is employed, which includes the selection of an evaluation board to assess the submitted proposals.
- **OC Winners Contracting**: The Trustchain consortium is dedicated to preparing and signing sub-grantee agreements. This process is executed by the coordinator, representing the consortium. Every sub-grantee, in turn, brings a set of administrative tasks to ensure adherence to the principles outlined by Horizon Europe.
- **Results Analysis**: Continuous monitoring and statistical analysis of open call results are conducted to gauge performance and impact.

For the selected applicants participating in OC2 and future Open Calls, **Trustchain provides comprehensive support through key project work packages**, including WP3, T3.4, and WP4, T4.1, T4.2, T4.3, T4.4:

- **OC Winners Coaching**: Applicants receive valuable guidance and feedback, aligning their efforts with Trustchain's expectations.
- **OC Winners Monitoring**: Regular follow-up activities are carried out to oversee experiments, deliverables, and outcomes, ensuring that projects remain on track.
- **OC Winners Evaluation**: Trustchain defines Key Performance Indicators (KPIs) and evaluates the deliverables of selected applicants against these performance metrics.

This Implementation Guide serves as an indispensable resource to elucidate the coaching, monitoring, and evaluation activities within the context of the Trustchain project, with a specific focus on OC2 – User Privacy and Data Governance. It is designed to equip selected applicants with the necessary information to successfully navigate their subproject work in this critical domain of data privacy and governance.

Trustchain remains dedicated to driving innovation and ensuring data security, paving the way for a more secure and user-centric digital future.

2 THE TRUSTCHAIN OPEN CALL 2 – USER PRIVACY AND DATA GOVERNANCE

2.1 TRUSTCHAIN OC2 SPECIFIC OBJECTIVES

It has become increasingly important to minimize the amount of data needed for specific online services. As more and more organizations share business sensitive data, it is important to preserve privacy while maintaining data utility. Therefore, is is necessary to give the control of their online data sharing back to the user and ensure privacy preserving ways of data exchange in the future internet. Establishing privacy, security and consent in specific data management processes should be a pre-requisite condition of online data sharing. The objective of this Open Call is to develop tools, cryptographic mechanisms, and other algorithms for data handling and sharing as well as for the management of data lakes in compliance with GDPR and other regulations that implement techniques such as:

- Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the challenges stated below,
- Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning in both a vertical and horizontal framework,
- Privacy-preserving data processing, data storage, and data computation techniques such as differential privacy, data obfuscation/perturbation, and anonymization techniques,
- Encrypted data analytics based on homomorphic encryption and Trusted Execution Environments,
- Protocols to verify authenticity and accuracy of data using technologies like Zero Knowledge Proofs,
- Protocols to support the digital sovereignty-based data flow and data spaces initiatives,
- Data identification, data provenance, data tracking mechanisms or protocols should be built so that the data that is exchanged can be tracked, so that trustworthy data handling according to the user consent can be verified.

Applications should cover real needs of the end-users in one a specific sector such as for example banking, education, healthcare, or e-government.

2.2 TRUSTCHAIN OC2 CHALLENGES TO ADDRESS

In the current Internet, all user data is owned and managed by a handful organizations, which dictate the terms of data exchange with third parties. In most cases, user consent is either not explicitly specified or is masked in elaborate notices. Purpose limitation and data minimization is a key data management practice that the current Internet is missing. Today's digital systems are faced with a multitude of challenges due to the centralised nature of the Internet. The Internet was initially developed without the human in the loop. However, with the exponential growth of online usage, evolution of decentralised systems and the power of cloud and edge computing has made the centralised model obsolete for many future online applications. In order to develop effective user privacy preserving and state-of-the-art consent-based data management, the following challenges that exist today need to be addressed:

- The online data sharing model is flawed as it encourages data duplication, long term data retention and intensive data collection across service providers. There is also lack of data traceability and accountability in online data sharing.
- Privacy is important when user data is employed for training machine learning models. Information leakage in training models is a persistent problem. Local differential privacy with federated learning models can be explored to address this challenge.
- The data accuracy vs privacy trade-off in privacy-preserving techniques like differential privacy is an open challenge, and its solution can be key to solving many open-source data sharing issues.
- Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol.
- Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed.
- A trust layer is missing, and it is often difficult to ensure authenticity of data. Thus, trustworthy data access and data integrity mechanisms based on SSI technologies, including decentralized identifiers and Verifiable Credentials, need to be designed.
- In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users.
- Users have little to no control over access to their personal data shared online. Therefore, automated user consent/smart user consent for data sharing needs to be implemented.

- Data owners currently do not have ways to be compensated or to enable fair data value sharing with the big players in the market. When users want to participate in the data economy, they should be able to do so by means of data tokenization/trading capabilities.
- Users should be empowered to add the necessary levels of anonymity in order to share their data with a third party.

A **user centric design approach** should frame the developed solution carefully consider the following:

- The real needs of the target users, with evidence of the existence of such needs.
- Identification of the user target groups
- User/Citizens privacy protection, data retention and data deletion, right to be forgotten, data minimization,
- Digital sovereignty of the user and citizen over its data,
- Data minimization and user informed data deletion.
- Ease of use of the solution's interface
- A senseful integration of the solution in the life of users
- Proven co-creation and validation of the tool by users with established methodologies and reports

2.3 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

In the realm of privacy-enhancing technologies and privacy-aware data sharing, the future holds promising expectations. Anticipated outcomes include the development of open APIs, SDKs, and libraries tailored to this domain, designed to offer a spectrum of solutions. These solutions encompass privacy-preserving data oracles, advanced data processing techniques utilizing technologies like Homomorphic Encryption and Trusted Execution Environments, data anonymization methods, privacy-conscious microservice architectures, versatile DLT-based solutions for privacy and data governance, as well as smart contracts designed to safeguard user privacy and data governance.

These advancements unlock a wide array of potential applications, spanning records of data processing activities (ROPAs) with verification and certification to ensure GDPR compliance, data processing within Trusted Execution Environments, consent management systems, collaborative secure data sharing platforms, privacy-preserving social networks, and the development of privacy-preserving machine learning models. This dynamic landscape promises to redefine the way data is handled and protected in our increasingly digital and interconnected world.

Open APIs, SDK, and libraries related to privacy-enhancing technologies and privacy-aware. Data sharing is expected outcomes. These outcomes should provide:

- Privacy-preserving data oracles,
- Privacy-preserving data processing techniques using technologies such as:
    - Homomorphic Encryption and Trusted Execution Environments,
    - Data anonymization and perturbation techniques,
    - Privacy-by-design microservice architectures,
    - General-purpose DLT-based solutions for privacy and data governance,
    - Smart contracts for user privacy and data governance.
- Possible use-cases and application domains include the following:
    - Records of data processing activities (ROPAs) with verification and certification for
    - GDPR-policy compliance,
    - Data processing in Trusted Execution Environments,
    - Consent management systems,

- Collaborative secure data sharing platforms,
- Privacy-preserving social networks,
- Privacy preserving machine learning models.

2.4 TRUSTCHAIN OC2 SELECTED PROPOSALS

TRUSTCHAIN OC2 was welcoming applications that should clearly define, upgrade/extend the state-of-the-art, and develop the following types of solutions:

- Decentralised user-centric identity management framework for supporting an automated privacy preserving, legal and regulatory compliant infrastructure (e.g., GDPR) potentially in alignment with emerging European regulations and standards (i.e., eIDAS).
- Protocols for trustworthiness assessment of entities by means of verifiable credentials and decentralized reputation systems.
- Smart oracles assessing the trustworthiness of data associated with digital identities.
- Inclusive digital identity platforms focusing on marginalized communities (e.g., refugees, elderly, vulnerable).
- Social identity for delegation and recovery that drives community-based trust establishment (i.e., social guardians).
- Systems considering both public and private administration roles in issuing and managing decentralized identifiers.
- Decentralized identity systems supporting Decentralised Autonomous Organizations (DAOs),
- Use-case driven identity management system deployment (e.g., banking, publishing, healthcare, education etc).

As a result of the implementation of the evaluation process defined in the Guide for Applicants, 15 proposals were selected to join the TRUSTCHAIN project.

TABLE 1 PROPOSAL, THEIR OBJECTIVES, EXPECTED OUTCOMES AND THE CHALLENGES THEY WILL TACKLE

Proposals	Objectives & expected outcomes	Challenges expected to be tackled
DOOF **(Data Ownership Orchestration Framework)**	DOOF aims to revolutionize data visibility control by leveraging Ecosteer's patented encryption scheme and smart contracts. It intends to develop open SDKs, libraries, and smart contracts that enable data owners to exercise their data ownership rights, such as granting, revoking, and monetizing data visibility. The framework seeks to integrate with various data sources and IT systems, ensuring privacy compliance. A key outcome includes deploying user-friendly, GDPR-compliant data exchanges.	The project plans to address challenges related to centralization in data visibility control, ensuring GDPR compliance, and enhancing trust in data sharing. It seeks to tackle issues in the current European data market, where data owners lack involvement, and aims to improve data sharing incentives through a transparent and ethical approach.
UtiP-DAM (Utility-Preserving, Decentralized Anonymity of Mobility data)	UtiP-DAM focuses on enhancing privacy in mobility data handling. It seeks to develop a decentralized method for mobility data anonymization that prevents re-identification by any party, including the data controller. Additionally, the project aims to produce an auditing tool for risk assessment in datasets and a verification tool for individuals and companies to check for similar data trajectories in public datasets.	The project confronts the complexities of anonymizing detailed spatiotemporal data and the limitations of centralized anonymization approaches. It addresses the risk of individual re-identification through mobility data and the challenge of securing data against cross-referencing with other datasets.
MorphMetro	MorphMetro aims to create an open-source solution for secure data exchange and analysis in quality assurance across various industries. The project focuses on developing a system for the secure, privacy-preserving transfer and analysis of measured data, utilizing emerging technologies and standards.	The project addresses the lack of a universally accepted protocol for structuring and disseminating measurement data. It seeks to ensure data security and privacy, especially when measured data contains Personally Identifiable Information (PII), and to comply with metrology regulations and standards.
SURE **(Synthetic Data, Utility, Regulatory compliance, and Ethical privacy)**	SURE is focused on generating synthetic data for AI and analytics, particularly in sensitive fields like banking and healthcare. The project aims to develop an open-source library that balances user privacy with data utility for AI training. It emphasizes regulatory compliance,	The project addresses privacy risks in AI, particularly the identification risks in anonymized data. It seeks to promote responsible data practices using Privacy-enhancing Technologies (PETs), specifically in the financial

	including GDPR adherence, and provides fine-grained privacy controls, enabling the evaluation of privacy and utility in anonymized and synthetic datasets.	sector, ensuring privacy without compromising the data's utility for AI applications.
dGUARD	dGUARD aims to create a privacy-preserving data-sharing platform leveraging blockchain and advanced cryptographic technologies. The project's primary focus is to enhance user trust by ensuring data sovereignty and secure data exchange. Key components include a consent management system based on self-sovereign digital identity, privacy-preserving authentication mechanisms, a proxy re-encryption scheme for end-to-end data privacy, and a blockchain-notarized audit trail for data traceability and accountability.	The project addresses the challenge of lack of trust in data sharing platforms due to privacy and control concerns. It seeks to overcome users' helplessness regarding data usage and sharing, aiming to provide a secure, transparent, and user-empowering platform for data exchange.
NG-SC **(Next Generation Smart Cities)**	NG-SC focuses on transforming data storage and management within the Next Generation Internet (NGI), emphasizing user-centric data governance. The project proposes a decentralized model where users and IoT devices control and manage all core infrastructure layers. Key innovations include a novel Multi-Party Computation (MPC) protocol and open-source software, aiming to empower users in data economy and transform data ownership in the NGI era.	The project aims to overcome the challenges of centralized data control by corporations and entities, transitioning to a user and IoT device-driven infrastructure. It addresses the high financial barrier in setting up smart city infrastructures and aims to ensure data privacy and ownership while utilizing IoT devices' computational resources.
DUME **(Decentralised User-Centric Media Extension)**	DUME aims to decentralize digital platforms like Tidy City, enhancing user control over submitted data. The project intends to extend the Solid Protocol for managing large-scale media datasets on decentralized web platforms. It focuses on validating the decentralized, user-centric features by implementing and testing in Tidy City, aiming to establish a pathway for decentralized digital sovereignty.	The project confronts the complexities of handling large volumes of high-resolution images with metadata, crucial for AI model training. Challenges include efficient data retrieval, rich metadata annotations, specific AI access control, and robust versioning mechanisms for dynamic data. This aims to ensure quick search, filtering, and data accessibility while maintaining privacy and user control.
AURORA MINDS	AURORA MINDS is dedicated to enhancing early and accurate ADHD diagnosis in children, with a strong focus	The project addresses the need for privacy and security in ADHD diagnosis technologies. It aims to

	on data privacy and security. The project integrates advanced privacy measures into ADHD assistive technologies, employing Identity Management (IdM) and Privacy-Enhancing Technologies (PETs). It leverages machine learning for secure data collection and analysis, ensuring GDPR compliance.	protect sensitive user data through federated learning and local differential privacy, and manages access rights using Privacy-Attribute-Based Credentials. This approach benefits children, parents, educators, and clinicians by offering secure, tailored ADHD risk assessments and diagnosis tools.
OIDC PRINCE **(OpenID Connect with PRIvacy-eNhanced ConsEnts)**	OIDC PRINCE aims to improve privacy in OpenID Connect consent processes. The project focuses on integrating proof of privacy regulation compliance, like GDPR, using data privacy vocabulary (DPV). It proposes secure storage of these proofs on a blockchain and enhances privacy analysis through Fuzzy Logic models to assess risks in services accessing private user information.	The project addresses privacy concerns in user consents for accessing personal information within the OpenID Connect framework. It seeks to provide informed consents, minimize data sharing with untrusted entities, and ensure entities managing user data demonstrate trustworthiness in privacy management.
PECS **(Privacy Enrooted Car Systems)**	PECS focuses on enhancing privacy control for drivers in modern car ecosystems, addressing the issue of personal data harvesting by car brands. The project aims to develop an interface for drivers to control their data sharing preferences and to implement privacy measures like Federated Analytics, Secure Multi-Party Computation, and Pseudonymisation. It's expected to significantly impact technical, societal, and industrial sectors by introducing privacy-focused car services and software support technologies.	The main challenge is the weak privacy control over personal data generated in modern cars. PECS seeks to ensure full compliance with data protection regulations like GDPR and to revolutionize data privacy in the automotive domain.
EIDCMP **(eIDAS compliant membership platform)**	EIDCMP, developed by WalliD and APBC, aims to create an advanced membership platform for Professional and Governmental Associations. The platform will enable seamless verification of member IDs and issuance of dynamic, verified credentials, ensuring compliance with eIDAS regulations and W3C standards. It focuses on safeguarding user data and providing a secure environment for credential management.	The project addresses challenges in verifying member identities and issuing credentials in compliance with eIDAS regulations. It seeks to enhance the security and privacy of the verification and credentialing process in membership management.

DID-IMP **(Decentralized Public Key Infrastructure for Defended IoT Data Management and Procurement)**	DID-IMP focuses on creating a decentralized public key infrastructure for secure and traceable data delivery in IoT. By leveraging blockchain technologies and eliminating traditional structures like CA and RA, it aims to facilitate secure, automatic data sharing (SADS) in various sectors including connected cars, remote healthcare, cognitive cities, energy management, and more.	The project addresses the need for secured and traceable data in IoT, replacing traditional administrative roles with blockchain smart contracts. It aims to enhance data traceability, security, and management across various IoT applications, ensuring compliance with evolving regulations and reducing administrative overhead.
GUEDHS **(Data Governance and User Privacy Envisioning an EHDS Pilot Deployment)**	GUEDHS is designed to pilot the European Health Data Space (EHDS) at an interregional scale, focusing on efficient health data use and data-sharing initiatives. It aims to improve patient outcomes and accelerate the development of new health services while ensuring data privacy, control, and transparency.	The project addresses challenges in securely sharing and reusing health data across borders, particularly in the context of epidemic risks and crisis preparedness. It seeks to establish a federated learning framework and adapt cybersecurity tools for a Federated Network, demonstrating a solution for respiratory infections data management.
ProvenAI **(Provenance in AI)**	ProvenAI aims to create a Decentralized Provenance Platform for unstructured data, emphasizing traceable lineage and unique identifiers for each data segment. The project focuses on enabling knowledge creators to track and receive fair compensation for the use of their content. It stands out by segmenting unstructured datasets into semantically relevant sections, addressing data minimization and protection against data exposure.	ProvenAI seeks to revolutionize the way AI models assimilate data, ensuring ethical AI development and robust data governance. It aims to redefine the dynamics of knowledge acquisition and compensation in AI, focusing on user privacy and rights of content creators.
LED-UP	LED-UP is focused on enhancing data governance and user privacy in decentralized systems, with a particular emphasis on the needs of individuals in refugee camps. The project, utilizing tools like Decentralized Digital Identity and Homomorphic Encryption, aims to establish a framework where data privacy is central.	The project addresses the challenge of maintaining user privacy and data governance in decentralized systems. It prioritizes user consent, traceability, and security in every data interaction, especially catering to the unique requirements of vulnerable populations like refugees.

2.5 TRUSTCHAIN OC2 REQUIREMENTS

2.5.1 Technical Requirements

When implementing their projects, all the selected projects will have to consider whenever relevant and applicable the following aspects in a technical manner according to the solution they envisioned:

- TR1 - Privacy and Data Protection
- TR2 - Data Transparency and Accountability
- TR3 - Cross-Border Data Flow Compliance
- TR4 - Data Management and Consent Control
- TR5 - Ethical Data Use and Fairness
- TR6 - Privacy-preserving Technologies Integration
- TR7 - Secure Data Provenance and Tracking
- TR8 - Usability and User Experience
- TR9 - Interoperability and Standardization

TR1, TR2, TR3 and TR8 have been described in more detail regarding the challenges they raise, the requirement to be addressed and their expected outcomes in Section 2.5.1 of the deliverable D3.7. The rest of the technical requirements at the level of the envisioned solution are described in more detail in the tables below.

2.5.1.1 TR4 – Data Management and Consent Control

TR3 - Data Management and Consent Control	
Definition	Addressing data management and consent control concerns to ensure user data is handled appropriately.
Challenges to be tackled	• Data retention and deletion: Ensuring that data is not retained beyond its necessary lifespan and retained and deleted as per user preferences. • Data erasure effectiveness: Guaranteeing that data erasure processes are thorough and irreversible. • Consent tracking and compliance: Managing and tracking user consent for data processing activities. • User data retrieval: Developing mechanisms for users to request and confirm data deletion.
Requirements to be addressed	• Data retention policies: Establishing clear policies for data retention and deletion as per user preferences. • Consent tracking and compliance: Managing and tracking user consent for data processing activities. Providing users with the ability to revoke consent at any time. • User data retrieval: Developing mechanisms for users to request and confirm data actions. • Data deletion: Creating a user-friendly process for users to request data deletion. Implementing automated user-friendly processes for data erasure which provides confirmation. Maintaining records of data deletion activities. Ensuring that deleted data cannot be recovered.
Expected outcomes at the level of your solution	• Effective data management: Efficient collection, retention, and deletion of user data. • Consent compliance: Alignment of data processing with obtained consents. • User empowerment: Empowering users to control their data and consent preferences. • Transparent data history: Providing a clear and transparent history of data actions and consent changes.

2.5.1.2 TR5 - Ethical Data Use and Fairness

TR4 - Ethical Data Use and Fairness	
Definition	Ensuring that user data is used in an ethical and responsible manner, aligning with ethical principles and guidelines.
Challenges to be tackled	• Ethical data use gaps: Identifying and addressing areas where data usage may not align with ethical principles. • Bias and fairness: Ensuring that data-driven decisions are fair and unbiased. • Informed consent: Obtaining informed consent from users regarding data usage in ethically sensitive contexts.
Requirements to be addressed	• Ethical data use guidelines: Establishing clear guidelines for ethical data usage. • Bias detection and mitigation: Implementing mechanisms to detect and mitigate biases in data and algorithms. • Algorithmic transparency: Providing transparency in how algorithms make decisions. • Ethical impact assessments: Conducting assessments to identify and address ethical risks in data usage. • Ethical AI governance: Implementing governance structures to ensure ethical AI and data use.
Expected outcomes at the level of your solution	• Ethical data use: Alignment of data usage practices with ethical principles. • Fair and unbiased algorithms: Mitigation of biases in data-driven decision-making. • Informed user consent: Users provided with information about ethical considerations related to data usage. • Ethical data culture: Fostering a culture of ethical data use within the organization.

2.5.1.3 TR5 – Cross-Border Data Flow Compliance

TR5 - Cross-Border Data Flow Compliance	
Definition	Ensuring compliance with international regulations and standards related to cross-border data transfers.
Challenges to be tackled	• Data sovereignty and jurisdiction: Navigating complex legal and jurisdictional requirements for cross-border data flows. • Data localization: Adhering to regulations that require data to be stored or processed within specific geographical boundaries. • Data transfer mechanisms: Identifying and implementing secure mechanisms for cross-border data transfers.
Requirements to be addressed	• Legal compliance framework: Establishing a framework to ensure legal compliance in cross-border data flows. • Data localization solutions: Implementing solutions to address data localization requirements. • Secure data transfer protocols: Using secure protocols and encryption for data transfers. • Jurisdiction mapping: Mapping data flows to relevant jurisdictions and regulations.
Expected outcomes at the level of your solution	• Legal compliance: Ensuring compliance with cross-border data transfer regulations. • Efficient data flows: Facilitating secure and efficient cross-border data transfers. • Data localization solutions: Implementing effective solutions to address data localization requirements.

2.5.1.4 TR6 - Privacy-preserving Technologies Integration

TR6 - Privacy-preserving Technologies Integration	
Definition	Integrating privacy-enhancing technologies such as differential privacy, secure enclaves, and homomorphic encryption into data processing workflows.
Challenges to be tackled	• Technology integration complexity: Integrating privacy-preserving technologies into existing data processing systems. • Performance trade-offs: Balancing privacy protection with system performance and efficiency. • User impact: Ensuring that privacy-enhancing technologies do not negatively impact user experience.
Requirements to be addressed	• Privacy technology integration plan: Developing a clear plan for integrating privacy-preserving technologies. • Performance optimization: Optimizing the performance of systems using privacy-enhancing technologies. • User-friendly privacy: Ensuring that users are not inconvenienced by privacy measures. • Privacy impact assessments: Evaluating the impact of privacy technologies on data processing.
Expected outcomes at the level of your solution	• Effective privacy protection: Integration of privacy-preserving technologies to protect user data. • Efficient data processing: Achieving a balance between privacy and system performance. • Positive user experience: Providing privacy protection without compromising user experience.

2.5.1.5 TR7 – Secure Data Provenance and Tracking

TR7 - Secure Data Provenance and Tracking	
Definition	Establishing mechanisms to track the origin and history of data, ensuring data authenticity and integrity.
Challenges to be tackled	• Data provenance ambiguity: Ensuring that data origin and history can be reliably traced. • Data tampering prevention: Preventing unauthorized tampering or alteration of data. • Data integrity assurance: Ensuring that data remains intact and unchanged during its lifecycle.
Requirements to be addressed	• Data provenance tracking: Implementing systems to track and record data origin and changes. • Data integrity checks: Employing mechanisms to verify data integrity and authenticity. • Immutable data records: Ensuring that data records cannot be altered or deleted. • Data tampering alerts: Implementing alerts for detecting and responding to data tampering attempts. • User access logs: Recording user access to data and changes made.
Expected outcomes at the level of your solution	• Transparent data history: Providing a clear and transparent history of data changes. • Data integrity: Assurance that data remains intact and unaltered. • Detection and prevention: Detecting and preventing unauthorized data tampering.

2.5.1.6 TR9 - Interoperability and Standardization

TR8 - Interoperability and Standardization	
Definition	Ensuring that solutions are interoperable with other systems and promoting standardization in the field of privacy and data governance.
Challenges to be tackled	• System compatibility: Ensuring that solutions can seamlessly integrate with existing systems and platforms. • Data format and protocol mismatches: Overcoming issues related to data format and communication protocols. • Lack of industry standards: Addressing the absence of standardized practices in the privacy and data governance domain.
Requirements to be addressed	• Interoperability frameworks: Implementing interoperability frameworks and APIs. • Data format standardization: Adopting standardized data formats and communication protocols. • Integration guidelines: Providing guidelines and documentation for system integration. • Industry collaboration: Engaging in industry collaboration efforts to promote standardization. • Testing and validation: Conducting interoperability testing to ensure compatibility.
Expected outcomes at the level of your solution	• Seamless integration: Easy integration with other systems and platforms. • Data exchange compatibility: Compatibility with various data formats and protocols. • Alignment with standards: Adherence to industry-standard practices.

2.5.2 Cross-Cutting Requirements

When implementing their projects, all the 15 selected projects in OC2 will have to address the cross-cutting requirements according to the solution they envisioned, specifically:

- **CCR1 - User Centred Approach:** Implementation of a User Centred Approach
- **CCR2 - Legal, Regulatory and Ethical framework:** Adherence and compliance to the current legal, regulatory and ethical framework
- **CCR3 - Business Plan:** Design and evaluation of a business plan based on a detailed market and cost-benefit analysis in the TRUSTCHAIN context (see Annex 1 of the deliverable D3.7)
- **CCR4 - Standardisation activities:** Leverage existing standards and/or contribute to standardisation activities in the TRUSTCHAIN context
- **CCR5 - Environmental sustainability:** Commitment to EU sustainable goal and six environmental objectives of the EU Taxonomy Regulation presented hereafter

The cross-cutting requirements have been described in detail in Section 2.5.2 of the deliverable D3.7.

2.5.3 Key Performance Indicators

The following KPIs, described in detail in Section 2.5.3 of the deliverable D3.7, should be assessed on a regular basis by the selected innovators, when relevant/applicable to each specific solution:

- KPIs towards a more trustworthy and privacy-aware evolution of the internet
- KPIs towards a more decentralized NGI
- KPIs towards sustainable business
- KPIs towards new forms of user-centered interaction and immersive environments for NGI users
- KPIs related to the pilot studies
- KPIs related to interoperability and standardization
- KPIs towards legal and ethical compliance
- KPIs towards a greener NGI
- KPIs towards innovation
- KPIs related to the implementation

3 SUPPORT FOR THE OPEN CALL #2 WINNERS

To ensure an adequate integration of the technologies/solutions proposed by the selected applicant teams into the TRUSTCHAIN ecosystem, different layers of support have been defined:

- Coaching support
- Technical support with Alastria infrastructure
- Communication support

3.1 COACHING SUPPORT

3.1.1 Head coach role

A TRUSTCHAIN head coach is assigned to each OC2 winner (see section 3.1.2). The coach is the main TRUSTCHAIN contact point for the assigned applicant team, and will have the responsibility to support, guide, provide feedback, motivate, understand, and challenge the applicant team. More specifically, the head coach:

- Schedule weekly monitoring calls with their assigned selected innovator(s) (as described in detail in Section 5).
- Update the monitoring tool (described in Section 6.3).
- Connect their assigned selected innovator(s) with relevant other innovators to establish TRUSTCHAIN platform interoperability.
- Ensure that deliverables and milestones are submitted by their assigned selected innovator(s) at the end of each sprint (timekeeper).
- Engage their assigned selected innovator(s) on TRUSTCHAIN events.
- Liaise with the relevant TRUSTCHAIN partners based on their assigned selected innovator(s) needs.
- Attend the biweekly meeting for coaches to share experience and foster the support between coaches.
- Connect the winner teams with the members of TRUSTCHAIN expert in specific areas (such as User Centric Approach, Legal or Standardization) periodically and/or when estimated necessary

3.1.2 Head coach distribution per projects

The assignment of the selected projects per head coach and coaching team (TRUSTCHAIN consortium partner) is depicted in the table hereafter.

TABLE 2: SELECTED PROPOSALS AND ASSIGNED HEAD COACH

Proposals	Head Coach
DOOF	AUEB/NKUA
UtiP-DAM	AUEB/NKUA
MorphMetro	ALA
SURE	ICS
dGUARD	ICS
NG-SC	UL
DUME	ALA
AURORA MINDS	ICS
OIDC PRINCE	ALA
PECS	AUEB/NKUA
EIDCMP- eIDAS	UL
DID-IMP	ICS
GUEDHS	UL
ProvenAI	ALA
LED-UP	AUEB/NKUA

3.1.3 Coaching and collaboration organigram - Communication flow

One of the key points for the success of all the TRUSTCHAIN initiatives in the OC2 Frame as well as for coaching and different collaboration activities is good communication between the different parties. To assure this, a workflow of communication between the different stakeholders is proposed in the following figure.

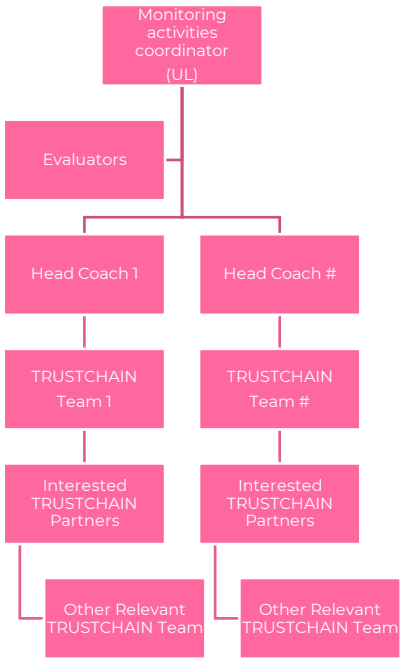

FIGURE 1: ORGANOGRAM OF THE COACHING/COLLABORATION ACTIVITIES IN TRUSTCHAIN.

3.2 TECHNICAL SUPPORT WITH ALASTRIA INFRASTRUCTURE

The available infrastructure, described in the Alastria's blockchain infrastructure for TrustChain document, will be live since the start of the first OC until the end of the last OC, with great system performance and uptime, improving every day with work of their employees and most active members. During this time any TrustChain participant will have access to this infrastructure in a Blockchain-as-a-Service (BaaS) manner, described in the Alastria Quick Reference for TrustChain document.

The TrustChain consortium's Service Level Agreement (SLA) and Operational Level Agreement (OLA) from Alastria towards OC2 subprojects regarding documentation,

guidance and support, as well as the procedures for Alastria networks infrastructure monitoring and maintenance have been described in Section 3.2 of the deliverable D3.7.

3.3 COMMUNICATION SUPPORT

Each OC2 team will receive a communication toolkit from the F6S team, reference for all their communication/dissemination activities.

This kit is composed of the following:

- Press release template
- Social media content
- Co-branding suggestions
- NGI, TRUSTCHAIN and EU logos
- NGI textual recognition
- Official credits of the EU support
- Social media engagement information

For all other matters related to communication activities and community building, OC2 winners can refer to F6S.

4 MONITORING, FOLLOW-UP AND EVALUATION

The monitoring, follow-up and evaluation procedures that will be followed for OC2 projects have been described in detail in Section 4 of the deliverable D3.7. Specifically, there have been described the day-to-day communication channels, the scrum methodology for subproject monitoring and support, the TRUSTCHAIN community building activities and the procedures for the evaluation of the four deliverables of OC2 projects.

5 TIMELINE

Bi-weekly SCRUM meetings are omitted from the table below for clarity. The meeting dates must be treated in a tentative manner, while the deliverable deadlines are hard.

TABLE 3: MEETINGS AND DEADLINES TIMETABLE

Sprint #	Activity	Description	When	Who is involved
1	Projects kick-off meeting	Presentation of TRUSTCHAIN project, TRUSTCHAIN Architecture, services and functionalities, OC2 project pitches, OC2 guidelines for implementation	**17/01/2024**	OC2 Beneficiaries, TRUSTCHAIN Coaches, TRUSTCHAIN Projects Coordinator
1	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**22/01/2024**	OC2 Coaches
1	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**24/01/2024**	OC2 Beneficiaries, Coaches
1	Sprint Planning Meeting	Online meeting to plan the subproject activities	**29/01/2024 - 05/05/2024**	One OC2 Team and their Coaches

1	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**05/02/2024**	OC2 Coaches
1	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**07/02/2024**	OC2 Beneficiaries, Coaches
1	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**19/02/2024**	OC2 Coaches
1	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**21/02/2024**	OC2 Beneficiaries, Coaches
2	Sprint Planning Meeting	Online meeting to assess the subproject progress	**26/02/2024 - 01/03/2024**	One OC2 Team and their Coaches
2	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**04/03/2024**	All Coaches
2	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and	**06/03/2024**	OC2 Beneficiaries, Coaches

		common orientation for the development of the TRUSTCHAIN ecosystem/network		
2	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**18/03/2024**	All Coaches
2	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**20/03/2024**	OC2 Beneficiaries, Coaches
2	Delivery of the D1		**22/03/2024**	OC2 teams
3	Sprint Planning Meeting	Online meeting to plan the subproject progress	**25/03/2024 - 29/03/2024**	One OC2 team and their Coaches
3	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**01/04/2024**	All Coaches
3	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**03/04/2024**	OC2 Beneficiaries, Coaches

3	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**15/04/2024**	All Coaches
3	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**17/04/2024**	OC2 Beneficiaries, Coaches
4	Sprint Planning Meeting	Online meeting to assess the subproject progress	**22/04/2024 - 25/04/2024**	One OC2 Team and their Coaches
4	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**29/04/2024**	All Coaches
4	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**01/05/2024**	OC2 Beneficiaries, Coaches
4	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**06/05/2024**	All Coaches
4	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and	**08/05/2024**	OC2 Beneficiaries, Coaches

		common orientation for the development of the TRUSTCHAIN ecosystem/network		
4	Delivery of the D2		**10/05/2024**	OC2 teams
5	Sprint Planning Meeting	Online meeting to assess the subproject progress	**06/05/2024 - 10/05/2024**	One OC2 Team and their Coaches
5	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**13/05/2024**	All Coaches
5	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**15/05/2024**	OC2 Beneficiaries, Coaches
5	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**27/05/2024**	All Coaches
5	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**29/05/2024**	OC2 Beneficiaries, Coaches

6	Sprint Planning Meeting	Online meeting to assess the subproject progress	**03/06/2024 - 07/06/2024**	One OC2 Team and their Coaches
6	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**10/06/2024**	All Coaches
6	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**12/06/2024**	OC2 Beneficiaries, Coaches
6	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**24/06/2024**	All Coaches
6	Biweekly Plenary Meetings	*Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network*	**26/06/2024**	OC2 Beneficiaries, Coaches *Beneficiaries, Coaches*
7	Sprint Planning Meeting	Online meeting to assess the subproject progress	**01/07/2024 - 05/07/2024**	One OC2 Team and their Coaches
7	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**08/07/2024**	All Coaches

7	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**10/07/2024**	OC2 Beneficiaries, Coaches
7	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**22/07/2024**	All Coaches
7	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**24/07/2024**	OC2 Beneficiaries, Coaches
7	Delivery of the D3		**26/07/2024**	OC2 teams
8	Sprint Planning Meeting	Online meeting to assess the subproject progress	**29/07/2024 - 02/08/2024**	One OC2 Team and their Coaches
8	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**05/08/2024**	All Coaches
8	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the	**07/08/2024**	OC2 Beneficiaries, Coaches

		TRUSTCHAIN ecosystem/network		
8	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**19/08/2024**	All Coaches
8	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**21/08/2024**	OC2 Beneficiaries, Coaches
9	Sprint Planning Meeting	Online meeting to assess the subproject progress	**26/08/2024 - 30/08/2024**	One OC2 Team and their Coaches
9	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**02/09/2024**	All Coaches
9	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**04/09/2024**	OC2 Beneficiaries, Coaches
9	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**16/09/2024**	All Coaches

9	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**18/09/2024**	OC2 Beneficiaries, Coaches
10	Sprint Planning Meeting	Online meeting to assess the subproject progress	**23/09/2024 - 27/09/2024**	One OC2 Team and their Coaches
10	Biweekly meeting for coaches	Online meeting to collectively assess the monitoring activities	**30/09/2024**	All Coaches
10	Biweekly Plenary Meetings	Follow up the integration activities and elicit challenges and common orientation for the development of the TRUSTCHAIN ecosystem/network	**02/10/2024**	OC2 Beneficiaries, Coaches
10	Delivery of the D4		**11/10/2024**	OC2 teams
10	Final Review Meeting (Community meeting)	Online meeting to collectively assess the monitoring activities	**14/10/2024 - 18/10/2024**	All OC2 Projects Beneficiaries, Coaches

6 Repositories

6.1 PROJECT REPOSITORY

A specific OC2 repository has been created in SharePoint. In this repository, there is:

- **OC2-General:** Where all documents and material to be shared between TRUSTCHAIN consortium and OC2 projects can be stored (e.g., the contact list of OC2 Innovators, the OC2 guide for implementation and the OC2 Kick off meeting presentations are part of this repository.)

- **OC2-[Project]:** Each project has its own dedicated folders only accessible by the project itself and TRUSTCHAIN core members. The folder name is composed by the OC topic number and the project acronym as depicted in the previous figure. It is decomposed in six subfolders:

1. **Proposal:** Where the proposal submitted by the respective OC2 selected innovators is saved, and which contains the project details.
2. **Contract:** After the signature of the sub-grant agreement a copy of it will be saved in this folder.
3. **Deliverables:** The place to save the OC2 4 deliverables requested according to the agreement.
4. **Communication:** The folder to save all relevant material related to the OC2 innovators communication activities.
5. **Monitoring:** The folder to save any kind of material related to the follow-up and progress monitoring of the project.
6. **Evaluation reports:** The folder to save the different evaluations reports done by the evaluators in reference to the different deliverables.

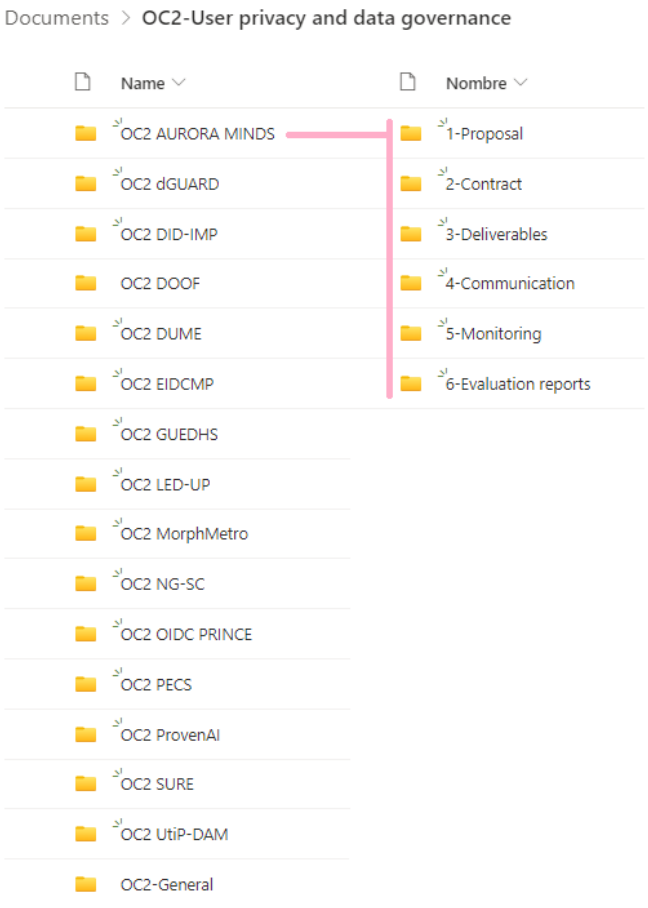

FIGURE 2: TEAM OC2 REPOSITORY

6.2 SOFTWARE REPOSITORY – GITHUB

TRUSTCHAIN has created its official GitHub organization: https://github.com/NGI-TRUSTCHAIN.

A private software repository for each applicant project has been created in TRUSTCHAIN GitHub organization, namely: https://github.com/NGI-TRUSTCHAIN/PROJECT-ACRONYM

An **Issue Tracker** per project for Feedback and Support can be found at: https://github.com/NGI-TRUSTCHAIN/PROJECT-ACRONYM/issues

Each individual project's repository must take into account the followings:

- **README.md:** A detailed and well-written README file for providing an overview of the project that includes information about the purpose, goals, and key features. Additionally, it should contain instructions on how to set up and run the project, any dependencies, and relevant documentation links.
- **Project structure:** Organising the codebase in a well-structured manner and that makes possible navigating it in an intuitive and/or easy way.
- **Documentation:** Comprehensive documentation to help understand the codebase and its functionality: components, APIs, interfaces, and any other relevant information.
- **Usage examples:** Usage examples and code snippets to demonstrate how to use the project and to show the capabilities and potential of the project.
- **Tests:** A comprehensive suite of tests that cover the major functionalities and use cases of the project.
- **Licensing and Acknowledgement:** The licensing terms under which the project is released and the acknowledgement about all contributions to the project (including dependencies).

TRUSTCHAIN members and applicants will add material there (documentation, guides, etc).

6.3 MONITORING TOOL

Specially designed to support the OC2 monitoring activities, a specific template GitHub KANBAN board is available for each project. The responsibility of maintaining the monitoring tool belongs to the core members of the SCRUM team and mainly to the selected OC2 projects. Note that a SCRUM team comprises the OC2 team members and the coach(es) from the TRUSTCHAIN consortium. The main lists of the GitHub KANBAN board are depicted in the figure below. Their detailed description has been provided in Section 6.3 of the deliverable D3.7.

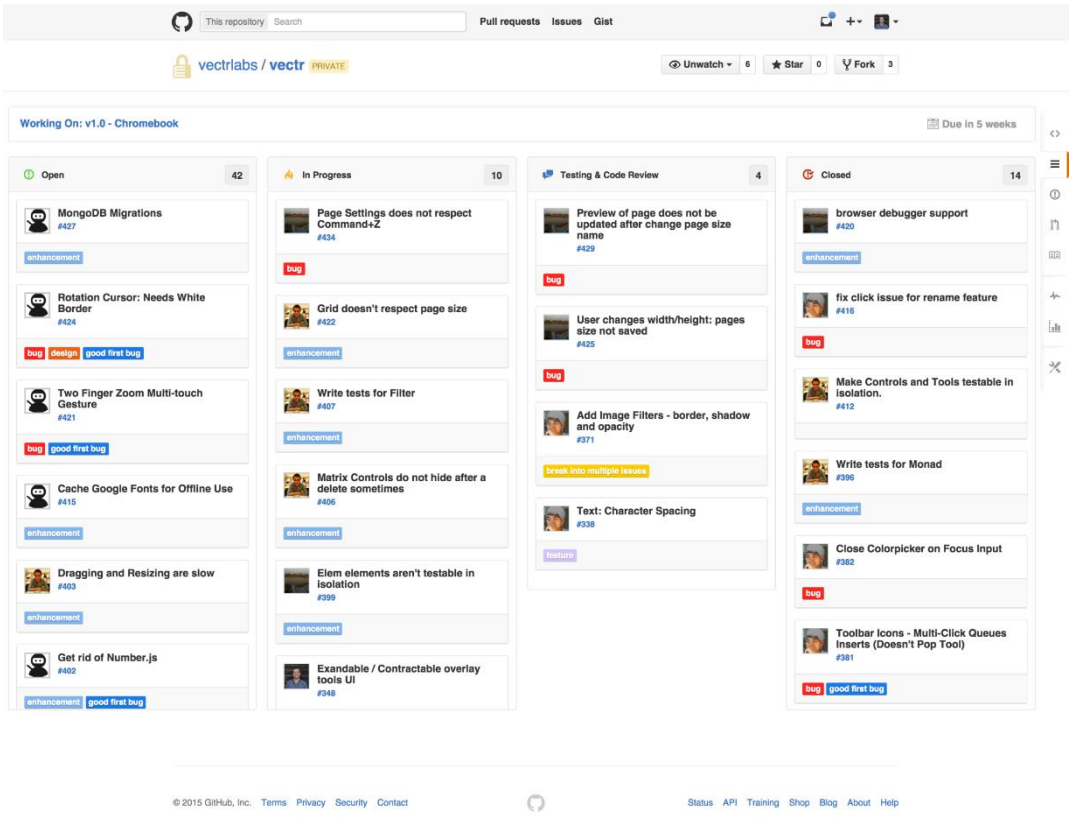

FIGURE 3: GITHUB KANBAN BOARD FOR PROJECT MONITORING

7 MAILING LISTS

OC2 winners' mailing list: TRUSTCHAIN_OC2winners@eurodyn.com

TABLE 4 CONTACT LIST

Project Acronym	Contacts
DOOF	elena.pasquali@ecosteer.com
UtiP-DAM	erel@cs.co.il
MorphMetro	kruno@randomred.eu
SURE	shalini@clearbox.ai
dGUARD	jordi@bloock.com
NG-SC	aleksandar.tosic@innorenew.eu
DUME	nuno.feixa@logimade.pt
AURORA MINDS	tmanos@dotsoft.gr
OIDC PRINCE	bmsousa@dei.uc.pt
PECS	giamp@dmi.unict.it
EIDCMP- eIDAS	filipe.veiga@wallid.io
DID-IMP	bmaisseu@gmail.com
GUEDHS	anac.costa@promptlyhealth.com
ProvenAI	csekas@ctrlspace.dev
LED-UP	manuel.knott@yahoo.de

TRUSTCHAIN coaches' list: TRUSTCHAIN_coaches@eurodyn.com

TABLE 5: COACHES MAILING LIST

TRUSTCHAIN partners	Head Coach details
ALA	Pablo Vela (pablo@alastria.io) Alexander Herranz (alexander@alastria.io)
UL	Vlado Stankovski (vlado.stankovski@fri.uni-lj.si) Petar Kochovski (petar.kochovski@fri.uni-lj.si) Iztok Škof (iztok.skof@fri.uni-lj.si) Gaber Polajnar (gaber.polajnar@fri.uni-lj.si) Pouriya Miri (pouriya.miri@fri.uni-lj.si)
AUEB	Vasilis Siris (vsiris@aueb.gr) George Stamoulis (gstamoul@aueb.gr)
ICS	Muttukrishnan Rajarajan (r.muttukrishnan@city.ac.uk) Michal Krol (michal.krol@city.ac.uk) Veniamin Boiarkin (veniamin.boiarkin@city.ac.uk)
NKUA	Thanasis Papaioannou (atpapaioannou@uoa.gr)
TLX (legal & regulatory aspects)	Ruben Roex (ruben.roex@timelex.eu)
CIB (User Centric design)	Andrés del Álamo (andres.delalamo@cibervoluntarios.org)
ED (administrative duties)	Caroline Barelle (caroline.barelle@eurodyn.com)

APPENDIX

ANNEX 1 - BUSINESS MODEL ANALYSIS METHODOLOGY

The detailed methodology for business model and sustainability analysis was presented in detail in the Annex 1 of the deliverable D3.7.