D2.12 EVALUATION, SELECTION AND CONTRACTING REPORT- OPEN CALL 2

31/12/2023

D2.12 EVALUATION, SELECTION AND CONTRACTING REPORT- OPEN CALL 2

Work package	WP 2
Task	Task 2.12
Due date	31/12/2023
Submission date	05/04/2024
Deliverable lead	ICS
Version	V0.5
Authors	Akanksha Dixit (ICS), Veniamin Boiarkin (ICS)
Reviewers	Thanasis Papaioannou (NKUA), Caroline Barelle (ED)
Abstract	TrustChain Open Call 2 evaluation, selection and contracting report
Keywords	TrustChain Open Call 2, evaluation, selection, contracting

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	08/01/2024	First Draft	Akanksha Dixit (ICS)
0.2	08/01/2024	Version ready for internal review	Akanksha Dixit (ICS)
0.3	18/01/2024	Internal review	Thanasis Papaioannou (NKUA) Caroline Barelle (ED)
0.4	30/03/2024	Integration of internal reviewer comments and consolidated version	Veniamin Bioarkin (ICS)
0.5	05/04/2024	Final version submitted	Caroline Barelle (ED)

DISCLAIMER

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	CITY UNIVERSITY OF LONDON	ICS	UK
9	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	NKUA	EL

EXECUTIVE SUMMARY

This report is the deliverable "D2.12 – Evaluation, Selection and Contracting Report 2" of the European project "TRUSTCHAIN – Fostering a Human Centred, Trustworthy and Sustainable Internet". It recalls the TRUSTCHAIN evaluation approach and methodology which applies in the first open call of TRUSTCHAIN as well as provides the necessary documents for the successful evaluation of the TRUSTCHAIN **Open Call 2 applications**. The documents are included as Annexes and depict the TRUSTCHAIN Background as well as all the specifications and support material for the TRUSTCHAIN Evaluators to manage efficiently the evaluation of this call. It follows the order presented hereafter:

o **Section 1** summarizes the evaluator's role and TRUSTCHAIN evaluation rules including the evaluator code of conduct, the management of the evaluator conflict of interest and confidentiality. This section is completed by the **Annex 1** that provides the contract to be signed by the Open Call Evaluators and ED, the coordinator of the project that acts as contractor on behalf of the TRUSTCHAIN Consortium. It also includes the declaration of honour on exclusion criteria and the declaration of absence of conflict of interest.

o **Section 2** explains the TRUSTCHAIN Open Call 2 key points to be considered by the evaluators for an appropriate evaluation, both organisational, i.e., timelines and contacts, as well as technical, i.e. the TRUSTCHAIN ecosystem. It also documents the whole evaluation process for all the applications received for the considered Open Call in particular the 3 phases i.e., the eligibility check, the proposals evaluation and provide the eligibility requirements for the applications.

o **Section 3** presents the requirements for a proposal to be eligible and the three evaluation reports, i.e., individual and consensus reports related to the written applications, and the evaluation summary report, which also integrate the evaluation of the pitch for the applicants selected for the last part of the evaluation.

o For more specific details, section 2 and 3 are completed by the guide for evaluator (Annex 2) that contains the eligibility check list, the grid for evaluation and report forms, in its **Annex 2**, the administrative form and ethical issues table to be compiled by applicants, whilst its Annex 3 contains the template of the proposals to be compiled by applicants.

o **Section 4** documents the evaluation process in terms of statistic both from the evaluators and applicants/ third parties' perspectives. It is also complemented by the Evaluation Summary Reports of the selected projects in **Annex 3** and the contract model to be filled and signed by the selected projects in **Annex 4.**

o **Section 5** summarizes the ethical principles on which all activities mentioned in this report are based.

TABLE OF CONTENTS

SECTION 1: EVALUATOR ROLE AND GUIDELINE FOR OPEN CALL 2

1.1 THE EVALUATOR'S ROLE IN TRUSTCHAIN

The role of the evaluator in TRUSTCHAIN Open Call 2 is to investigate and justify the value of the received proposals according to the regulatory frame of the Open Calls according to the eligibility, requirement and TRUSTCHAIN specific evaluation criteria. Experts perform evaluations of the TRUSTCHAIN proposals on a personal basis, not as representatives of their employer, their country or any other entity. They are required to be independent, impartial and objective, and to behave throughout in a professional manner. Evaluators should always keep in mind that significant funding decision will be based on their assessment.

There are two types of evaluators in TRUSTCHAIN.

The **External Evaluators** acting for TRUSTCHAIN Open Call 2 are selected after having expressed their interest (evaluators call for interest) among others, according to their expertise and skills related to TRUSTCHAIN Open Call 2 specificities (see section 4). They signed an agreement including a code of conduct and a declaration of non-conflict of interest (see Annex 1) binding them to the TRUSTCHAIN rules. Part of their contractual obligation is also to comply with the deadlines set by the TRUSTCHAIN consortium. They receive a fee of 50€ for each proposal evaluated.

The **Internal Evaluators** are members of the TRUSTCHAIN consortium. They are also requested to respect the code of conduct and confidentiality.

Any conflict of interest, any situation where the impartial and objective evaluation is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest is intended to be avoided. In practice, all Evaluators whether external or internal must declare beforehand to the call coordinator any known conflicts of interest or immediately inform them, should one become apparent during the course of the evaluation.

Evaluators must maintain strict confidentiality with respect to the whole TRUSTCHAIN evaluation process. They must follow any instruction given by TRUSTCHAIN consortium and confidentiality rules must be adhered to, at all times e.g., before, during and after the evaluation. Under no circumstance may an Evaluator:

- Attempt to contact an applicant on his/her own account, either during the evaluation or afterwards
- Disclose any information on proposals/applicants
- Disclose any detail on the evaluation outcomes
- Disclose names of other Evaluators involved.

They must return to the TRUSTCHAIN Consortium and/or erase any confidential documents once the TRUSTCHAIN evaluation exercise is over.

The evaluator's code of conduct applies to all stages of the TRUSTCHAIN evaluation process from the conception to the completion of the evaluation and the release and use of the evaluation results. Any deficiency in conduct may undermine the integrity of the evaluation. TRUSTCHAIN Evaluators are thus asked to be professional at all times of the evaluation process and to respect the following principles:

- Independence
    - Evaluators assess proposals on a personal basis;
    - Evaluators represent neither their employer, nor their country;
- Competence
    - Evaluators shall accurately represent their level of skills and knowledge and should work only within the limits of their professional training and abilities in evaluation;
- Impartiality
    - Evaluators treat all proposals equally and evaluate them impartially on their merits, irrespective of their origin or the identity of the applicants;
- Objectivity
    - Evaluators assess each proposal as submitted, not on its potential if certain changes were to be made;
- Accuracy, Completeness and Reliability
    - Evaluators make their judgment against the official evaluation criteria of the call that the proposal addresses, and nothing else;
    - Evaluators have the obligation to ensure that evaluation reports and presentations are accurate, complete and reliable. Evaluators shall explicitly justify judgements, findings and conclusions and demonstrate underlying rationale in order that stakeholders may assess them.
- Consistency
    - Evaluators apply the same standard of judgment to all proposals considering the specific implementation mode.

TRUSTCHAIN is an H2020 Innovation Action and as such, proposals are not negotiated. This strongly limits the possibility of modifying a proposal after it has been selected for funding. It is therefore very important that the evaluators evaluate them as they are, reflecting all the strengths and weaknesses in the scores. To support and train them for this activity, a guide (Annex 2) is provided to them that is described below.

1.2   THE GUIDE FOR EVALUATOR

This guide aims at supporting the evaluation of proposals submitted to the **TRUSTCHAIN Open Call 2: User Privacy and Data Governance**. It is intended to support independent Evaluators and internal Evaluators embodied in the TRUSTCHAIN Consortium to:

- o Assess on an individual and professional basis and against predefined evaluation criteria, the proposals received in response to the Open Call 2 (All evaluators);

- o Draft Individual Evaluation Reports and Consensus Reports for the proposals (All evaluators);

- o Establish the short list of proposals admissible for online interview (All evaluators);

- o Implement the online interview for the projects shortlisted (Only the internal evaluators);

- o Draft Evaluation Reports for the online interview (Only the internal evaluators);

- o Contribute to the Evaluation Panels to establish and approve the final ranking list of selected projects and the ones that will be part of the reserved list (Only the internal evaluators).

Moreover, this guide contains information on the overall TRUSTCHAIN Innovation Action as well as more specifically on the TRUSTCHAIN Open Call 2, i.e.:

- o The specific requirements for the objectives of the call and their respective topics of the TRUSTCHAIN frame, the evaluation process and its workflow, the eligibility criteria and the specific evaluation criteria for this call.

- o The drafting and the quality of the Individual Evaluation Report and Consensus Report, the latter being also available to the applicants of each proposal.

- o A reminder regarding ethical principles related to H2020 research and innovation activities is presented as well as an evaluation check list.

SECTION 2: THE TRUSTCHAIN OPEN CALL 2 EVALUATION KEY POINTS AND PROCESS

2.1 TRUSTCHAIN OPEN CALL 2 INDICATIVE TIMELINES

Call	Indicative Dates	Who
Call Publication	20th July 2023 at 13:00 CEST	TRUSTCHAIN Consortium
Call Closure	20th September 2023 at 17:00 CEST	TRUSTCHAIN Consortium
Eligibility, Conflict of interest & Contract Signing	20th to 24th of September	TRUSTCHAIN Consortium + External Evaluators
Web Briefing	25th September 2023	TRUSTCHAIN Consortium + External Evaluators
Allocation of Proposals to Evaluators	25th September 2023	TRUSTCHAIN Consortium

Remote Evaluation	Indicative Dates	Who
Evaluators Web Briefing	25th September 2023	TRUSTCHAIN Consortium + External Evaluators
The remote proposal evaluation takes place	From the 25th September 2023 to the 4th December 2023	TRUSTCHAIN Consortium + External Evaluators
100% Individual Evaluation Reports completed	16th October 2023	Internal Evaluators + External Evaluators
100% Consensus Reports completed	30th October 2023	Internal Evaluators + External Evaluators
Panel Review meeting and selection of applicants for the online interview	10th November 2023	TRUSTCHAIN Consortium
Online Interviews	From the 20th November to the 1st December 2023	Internal Evaluators + TRUSTCHAIN Advisory Board Members
TRUSTCHAIN Open Call 2 results publication	Week of the 11th December 2023	TRUSTCHAIN Consortium

Factually the online interviews were organised in 2 sessions of up to 5 hours and a half starting the 04/12/2023 and finishing the 05/12/2023. 23 Applicants were evaluated for a possible number of selected proposals of 19.

The panel meet on the 11th of December 2023 to validate the ranking list.

The Open Call 2 results were announced the 9th of January 2024, allowing then the contracting process of the 15 Open Call 2 innovators.

2.2 TRUSTCHAIN CONTACT POINTS

Contact point	Name	Email
Call coordinator	Caroline Barelle	caroline.barelle@eurodyn.com
	Vlado Stankovsky	vlado.stankovski@fri.uni-lj.si
	Daniel Silva	daniels@f6s.com
	Tajana Medaković	tajana@f6s.com

2.3 TRUSTCHAIN APPLICANT CLASSIFICATION

The target Applicants for the TRUSTCHAIN Call 2 are:

o Internet technologists, researchers and innovators.

o Researchers and developers employed in research centres or enterprises among other SMEs, in third-level education institutes, research infrastructures, non-profit organisations and charitable (scientific) foundations.

These Applicants' profiles were able to apply as team of individuals or linked to a legal entity. Thus, their participation is possible in several ways:

o Legal entity(ies):

These are universities, research centres, NGOs, foundations, micro, small and medium-sized enterprises (see definition of SME according to the Commission Recommendation 2003/361/EC), large enterprises working on Internet or/and other related technologies;

o One or more entities (consortium) established in an eligible country.

o Team of natural persons:

The natural person's part of the team must be established in any eligible countries. This does not consider the country of origin but the residence permit.

Any combination of the aforementioned.

2.4 THE TRUSTCHAIN R&I ACTION AND TECHNICAL FRAMEWORK

The Internet has pushed our existence into the digital era, revolutionising our health, our wellbeing, our social life, our education and our information. Today we approach the Internet with our digital identities. There is a plethora of such digital identities that currently do not properly serve their purpose. Multiple threats related to truthfulness, trust and identity (ID) arise when people interact in this digital world: delusion and manipulation, personal privacy violation and personal data exploitation, unknown provenance of information, anonymity for performing criminal activities, spread of fake news using fake identities, skills mismatches, serious breaches of security are only a few of the threats that have emerged. The spirit of the first-generation Internet based on individual freedom, material progress, and moral community is slowly turning into individualism, materialism, and moralism, diverging from essential ethical and democratic principles that should underline this technology. The design choice of the past, based on a mix of centrally managed networking and device technologies makes today's Internet obsolete when it comes to empowering all citizens to act for a more environmentally friendlier digital transformation, as well as to create a more resilient, inclusive, and democratic society, addressing inequalities and human rights, better prepared for and responsive to threats and disasters.

For TRUSTCHAIN, the current emergence of Internet of Things (IoT), Decentralised Oracles, Artificial Intelligence (AI), Cloud-to-Edge (aka Fog) Computing, Distributed Ledger (DLT) and Digital Twin (DT) technologies created the need to build democratic systems without central points of control that can establish the missing link between universally agreed objectives in the physical world, and the digital representation of the reality, thus contributing to the realisation of trusted relationships in the Next Generation Internet. This can be achieved by using various consensus mechanisms that associate proofs with digital representations and thus help humans understand the objective truth, achieve trusted relationships on the digital world, allowing them to undertake well-informed decisions, in either a manual or automated manner. The ability to arrive at the objective truth by employing democratic governance mechanisms, consensus-based proofs, verification and certification can lead to a Next Generation Trusted Internet supporting humanity in all aspects of life. Today more than ever, challenges faced all over the world push for our society to reorganise itself to survive. The United Nations have called to reach 17 Sustainable Development Goals. Essentially, TRUSTCHAIN must be leveraged to embed in the Next Generation Internet principles of human-rights, sustainability, ethics and other human values that have been developed and maintained through long lasting centuries of human evolution.

The key concept of TRUSTCHAIN is to embed the key humanity principles in the co-creation of the Next Generation Internet and to provide autopoietic, evolutionary, decentralised and therefore democratic, transparent, traceable, and regulatory compliant mechanisms that can support any ecosystem of entities and actors participating with their digital identities. The basis for this to happen is the use of

decentralised digital identity architectures together with IoT, AI, Cloud-to-Edge, DLT and DT. Our intention is to embed in such solution's important societal goals in accordance with objective truth and therefore, trustworthiness.

TRUSTCHAIN - Fostering a Human-Centred, Trustworthy and Sustainable Internet is a European project funded by the European Commission under the European Union's Horizon Europe Research and Innovation Programme and the call topic CL4-2022-HUMAN-01-03. As such, it is part of the **European Commission's Next Generation Internet (NGI) initiative.** Its overall objective is to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised identity management software solutions that is transparent to the user, interoperable, privacy aware and regulatory compliant that can seamlessly integrate and interoperate with any of the existing decentralised applications. **TRUSTCHAIN was launched in January 2023 to address the inherent challenges within the current centralised Internet architecture that is not transparent to the user, does not protect the privacy-by -default and does not scale well through 5 Open Calls and an overall budget of 8,775 M€.**

The 5 Open Calls are the following:

- **Open Call 1- Decentralised digital identity**

    The overall objective of Open Call 2 was to define and develop:

    - A framework for decentralised user-centric identity management;
    - Protocols for trustworthiness assessment of entities and their data by means of verifiable credentials and decentralized reputation systems;
    - Smart oracles assessing the trustworthiness of data.

- **Open Call 2- User privacy and data governance**

    The objective of this OC will be 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 the GDPR and other regulations that implement techniques such as:

    - Multi-party data sharing mechanisms
    - Federated learning mechanisms considering both vertical and horizontal frameworks
    - Encrypted data analytics based on homomorphic encryption
    - Secure and privacy preserving data analytics mechanisms
    - Privacy-preserving usage of Artificial Intelligence, IoT, Digital Twins, Cloud-to-Edge services, or combination of those

    This is the focal point of this document.

○ **Open Call 3- Economics and democracy**

The objective of OC3 will be to define and build mechanisms for smarter data exchange and data trading as well as innovative win-win federated business models' open data.

○ **Open Call 4- Multi chains support for NGI protocols**

OC4 goal will be to design and build the gateways that will make it possible to transfer knowledge/metadata/data/process/requirements from one chain to another in a trustworthy and secure manner. Interoperability across multiple chains will be a cornerstone in this call.

○ **Open Call 5- Green scalable and sustainable DLTs**

This call will build on top of all past OC1-4 calls. Its objective will be to employ digital identities, trustworthy data, and already designed novel mechanisms for the ecosystems' economy, in order to achieve high energy efficiency and optimisation of DLTs. We are looking for the most appropriate, relevant and pertinent trade-offs between the use of technologies, the security of consensus protocols on one side, and the sustainability and energy efficiency requirements on the other.
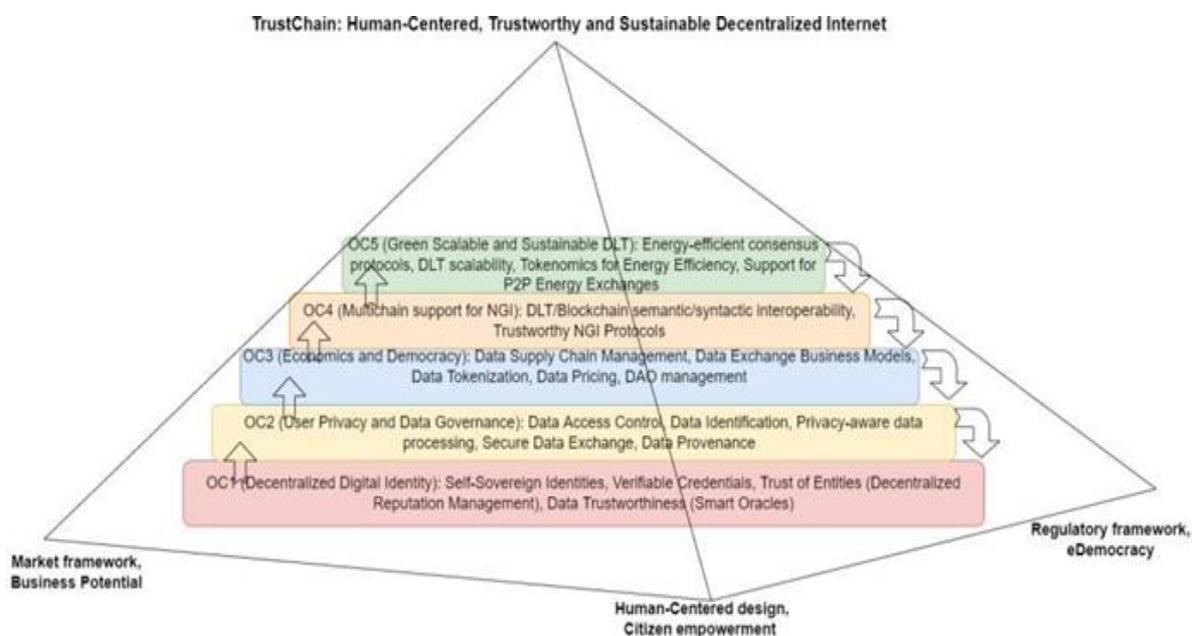
The methodology of TrustChain is carefully designed in a way it is not significantly harming any of the six environmental objectives of the EU Taxonomy Regulation presented hereafter.

2.5   THE TRUSTCHAIN OPEN CALL 2 SCOPE AND OBJECTIVES

2.5.1   Introduction to OC2

Its indicative budget is € 1 755 000 and will be distributed among up to 15 selected projects led and executed by a critical number of developers, innovators, researchers, SMEs and entrepreneurs working on different NGI relevant topics and application domains at the intersection between the technical field (e.g Software Engineering, Network Security, Semantic Web, Cryptography, Blockchain, Digital Twin, Blockchain Security, Digital Identity, Blockchain Protocol), the Social sciences and Humanities (e.g Social Innovation, not-for-profit sector, Social Entrepreneurship, public goods) as well as any others including economics, environment, art, design, which can contribute to NGI TRUSTCHAIN relevant vision.

Selected projects will last for a duration of 9 months. However, TRUSTCHAIN overall action lasting 36 months, their participation at any of the future Joint Meetings after these 9 months for knowledge and know-how transfer to TRUSTCHAIN OC2-5 and for the development of the TRUSTCHAIN ecosystem as a whole is requested.

As part of the TRUSTCHAIN action, experts in diverse fields will also provide to Third party innovators selected technology development guidance, working methodology as well as access to technical infrastructure, training in business model development and data related topics, coaching, mentoring, visibility and community building support.

Applicants are invited to submit their proposals on any topic that serves the overall TRUSTCHAIN OC2 vision and objectives. Their proposed solution should consider as minimal requirement to:

o   Use standard technology for full stack development;

o   Be open source;

o Extends the state-of-the-art in the domain of digital identities, and/or solves existing real-world problems with digital identities and provides new highly usable software solutions.

Using the mandatory TRUSTCHAIN proposal template, applicants are expected in relation to the specific objectives specified hereafter (section 3.2) to explain in their application:

1. The specific technological innovation they propose to develop and how this is clearly different from alternative solutions that are already available in the market, or developed by previous EU research and innovation actions (i.e., EU ONTOCHAIN Project & any other projects);

2. The specific digital identity needs or challenge they propose to address and who would benefit from it immediately and in the longer term;

3. Whether the innovation will focus on the development of new solutions for existing areas, or a totally disruptive approach or idea;

4. Any work they have already done to respond to this need, for example if the project focuses on developing an existing capability or building a new one

5. Any challenges or opportunities relating to equality, diversity, ethics and inclusion arising from their project.

Applicants when applying should **clearly specify the Open Call 2 challenges they are going to address. Those are described in the section 3.3.**

2.5.2 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, to give the control of their online data sharing back to the user and ensure privacy preserving ways of data exchange on the future internet is currently needed. 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:

o Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below,

o Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework,

o Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques,

o Encrypted data analytics based on homomorphic encryption and Trusted Execution environment,

o Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs,

o Protocols to support the digital sovereignty-based data flow and data spaces initiatives.

o 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.

2.5.3 OC2 Challenges to be addressed

In the current Internet, all user data is owned and managed by a few 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:

o 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,

o Privacy is important when user data is employed for training machine learning models and computation. Information leakage in training models is a persistent problem. Local differential privacy with federated learning models can be explored to address this challenge,

o 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,

o Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol,

o Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed,

o 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, needs to be designed,

o In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users,

o 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,

o Data owners currently do not have means 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,

o 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:

o data privacy protection,

o privacy aware data processing,

o data provenance,

o data use policies,

o data retention and data deletion, right to be forgotten, data minimization, and trustworthiness,

o data minimization and user informed data deletion.

2.5.4 OC2 Specific Requirements

o   Technical Requirements

In general, a user centric design and implementation, a co-created process with citizens as well as a use case driven approach will frame the proposed innovative solution development that should carefully consider the needs for security, privacy, human-rights, sustainability, and trustworthiness. Interoperability, scalability, greenness, openness, standards, as well as legal and regulatory compliance should be also considered, calculated, and assured.

The proposed solutions are intended to be co-created with end users focusing on online user privacy and data governance, adopting a user-friendly design. Therefore, they should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. The co-creation and validation approach should be clearly elaborated in the applicants' proposal. A citizen digital vulnerable collectives' approach that puts in the centre the needs of the general population and vulnerable people, instead of technical/experts' users should be considered. It is intended that the solution is accessible for the general population as well as for the marginalized/vulnerable communities.

To this end, the applicant should show collaboration with an EU end-user organisation (i.e., banking, healthcare, education, policing etc.) as well as consider vulnerable groups for the evaluation /validation process if possible.

The focus should be on what is currently missing (e.g., trustworthy data access, ensuring clear and informed user content and expanding what already exists, thus scaling) rather than building something new from scratch. It is desirable that the selected projects be able to demonstrate their solution at TRL 7 in a real end-user setting. If something completely new must be built (see point above), then it should be well motivated why the nature of the problem warrants a new solution and why the state-of-the-art solutions do not solve it today (i.e., barriers to technology adoption).

The proposed solution should work within a specific business context and emphasis should be put on its scalability, on its energy efficiency and its minimum value proposition. Cross-border data sharing, moving data across EU-international borders should be carefully considered. It should be also compatible with existing data sharing frameworks, standards and demonstrate the energy efficiency through measurements that are quantifiable.

Finally, focus should also be put on demonstration of the technology. In particular, the applicant should demonstrate to have access to an infrastructure that is EVM compatible where it can be deployed and piloted.

Link with other Open Calls: This Open Call is closely related to Open Call #1 "Decentralized digital identity". Solutions to be developed in Open Call #2 should consider some of the approaches and outcomes identified in Open Call #1 for digital

identity management. Joint activities between Open Call #1 and Open Call #2 innovators will be facilitated by the Trust Chain consortium.

o   **Sustainability Requirements**

Various emerging technologies currently pose huge environmental impact. This negative impact should be assessed against the benefits from using these technologies. The applicants are requested to provide a short assessment of the trade-offs, considering from one viewpoint the benefits when using the technology, and from another, the potential energy-inefficiency. Various best effort solutions should be used as a baseline for providing such self-assessment.

o   **Regulatory And Standards Requirements**

Applicants are requested to present in a clear and concise manner any existing and/or emerging privacy-enhancing data sharing platform (i.e., GAIA-X & IDS, DECODE) / infrastructure standards with which they intend to comply with, or they wish to contribute to within the course of the proposed project. They should also identify how the project aligns with the Digital Services Act (DSA) and the Digital Market Act (DMA).

o   **User Centricity Requirements**

As mentioned above, the proposed solutions should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. The co-creation and validation approach should be clearly elaborated in the applicant's' proposal and the vulnerable collectives' approach should be used for the user testing.

A first step is to establish target groups of users. Once this is done, the users should be involved in the co-creation process. Then, accessibility standards should be incorporated through the onboarding according to the vulnerable collectives' approach.

Following that, a roadmap with the appropriate methodologies should be set up. The roadmap should include the approach, objectives and phases of the testing, and sample size. The sample needs to be representative and randomized but within the relevant characteristics of the target population.

User should be onboarded in the design process (if applicable). Proposals for improvement and insights should come from the users during the co-creation process. Complementarily, insights can be proposed by non-users (for example developers, or business partners). This decision must be justified in the corresponding deliverable.

2.5.5 Expected Outcomes and Possible Application Domains

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

- o Privacy-preserving data oracles,
- o Privacy-preserving data processing techniques using technologies such as Homomorphic Encryption and Trusted Execution Environments,
- o Data anonymization and perturbation techniques,
- o Privacy-by-design microservice architectures,
- o General-purpose DLT-based solutions for privacy and data governance,
- o Smart contracts for user privacy and data governance.

Possible use-cases and application domains (not limited to) include the following:

- o Records of data processing activities (ROPAs) with verification and certification for GDPR-policy compliance,
- o Data processing in Trusted Execution Environments,
- o Consent management systems,
- o Collaborative secure data sharing platforms,
- o Privacy-preserving social networks,
- o Privacy preserving machine learning models.

2.5.6 OC2 mandatory Deliverables

Projects selected and funded by the TrustChain consortium will have to deliver four mandatory deliverables during their lifetime. The four deliverables are defined below:

- o **D1:** State of the art overview, use case analysis and preliminary technical specification of the solution. The deliverable should clearly specify how the proposed solution extends and/or upgrades the state-of-the-art.
- o **D2:** Detailed technical specification of the solution, software implementation work plan, demo scenarios, number of end users that will be involved in any pilots, and preliminary business plan.
- o **D3:** Implementation, deployment, testing, demonstration, and validation roadmap in a real-life application (e.g., banking, education, healthcare, utilities, defence or cross-border travel) and result of the validation process.
- o **D4:** Modularised software components ready for distribution, full documentation for developers/users, final business plan.

2.6 TRUSTCHAIN OPEN CALL 2 EVALUATION PROCESS

2.6.1 Overall process

Proposals are submitted in a single stage and the evaluation process is composed of three stages as presented hereafter.

- o **Stage 1:** Admissibility & eligibility check
- o **Stage 2:** Proposals evaluation
- o **Stage 3:** Online interviews and final selection
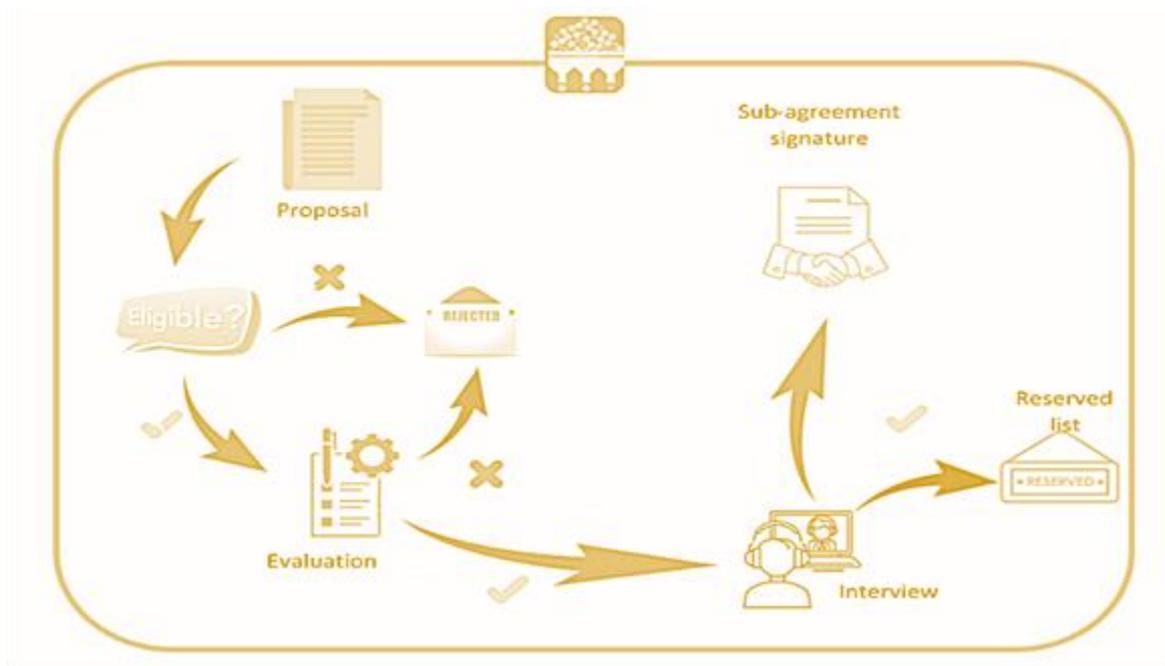
2.6.2 Admissibility and eligibility check

Admissibility and eligibility criteria for each proposal are checked by the TRUSTCHAIN Consortium staff. A proposal may be declared ineligible or inadmissible at any stage.

To be considered admissible, a proposal must be:

- o Submitted in the electronic submission system before the call deadline;
- o Compliant with the specific eligibility conditions set out in the relevant parts of the guide for Applicant, TRUSTCHAIN OC2 Guide for Applicant.pdf (see section 3

of this guide). The eligibility filter enables the creation of a shortlist of proposals to be evaluated;

o Readable, accessible and printable;

o Complete and include the requested administrative data, and any obligatory supporting documents specified in the call (following the template accessible here: Administrative Form Preparation.pdf;

o Include the research proposal description. Applicants must strictly follow the template, instructions as well as pages limitation for drafting the research proposal accessible here: Proposal Description Template.doc (live.com). A proposal will only be considered eligible if its content corresponds specifically to the objectives of the TRUSTCHAIN Open Call 2 and demonstrates that it aims to advance the state of the art especially with regards to the TRUSTCHAIN Framework and application domain.

2.6.3 Proposal evaluation

The evaluation of proposals is carried out by the TRUSTCHAIN Consortium with the assistance of independent experts. TRUSTCHAIN Consortium staff ensures that the process is fair and in line with the principles contained in the European Commission's rules on Proposal submission and evaluation. To facilitate the independent experts and the evaluation process, the EasyChair platform (https://easychair.org/) will be used.

Experts perform evaluations on a personal basis, not as representatives of their employer, their country or any other entity. They are required to be independent, impartial and objective, and to behave throughout in a professional manner. They sign an expert contract, including a declaration of confidentiality and absence of conflict of interest, before beginning their work.

All experts must declare beforehand any known conflicts of interest and must immediately inform the TRUSTCHAIN Consortium staff if they detect a conflict of interest during the evaluation. The expert contract also requires experts to maintain strict confidentiality with respect to the whole evaluation process. They must follow any instruction given by the TRUSTCHAIN Consortium to ensure this. Under no circumstance may an expert attempt to contact an applicant on his/her own account, during the evaluation process. Confidentiality rules must be adhered to at all times before, during and after the evaluation.

Each proposal is evaluated by a set of 2 experts (one from the TRUSTCHAIN Consortium and one external) according to the following criteria:

1- Excellence and innovation (40% weighting)
-Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context and credibility of the proposed methodology including the User Centric Approach.
-Extend that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective (e.g. ground breaking objectives, novel concepts and approach, new products, services, or business and organisational models)
-Excellence, capacity of the Applicant to deliver the proposed solution

2- Expected impact and value for money (30% weighting)
-Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised identity management software solutions that is transparent to the user, interoperable, privacy aware and regulatory compliant.
-Impact of the proposed innovation on the needs of European and Global markets
-Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.

3- Project Implementation (30% weighting)
-Quality and effectiveness of the work plan, including extend to which the resources assigned to the work are in line with its objectives and deliverables
-Quality and effectiveness of the management procedures including risks and mitigation management
-Integration capacity in the TRUSTCHAIN ecosystem

The experts will score each award criterion on a scale from 0 to 5 (half point scores may be given):

0=**Proposal** fails to address the criterion or cannot be assessed due to missing or incomplete information.

1=**Poor**, criterion are inadequately addressed or there are serious inherent weaknesses

2=**Fair**, proposal broadly addresses the criterion but there are significant weaknesses.

3=**Good**, proposal addresses the criterion well, but a number of shortcomings is present.

4=**Very good**, proposal addresses the criterion very well but a small number of shortcomings is present.

5=**Excellent**, the proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

For each criterion, the minimum threshold is 3 out of 5 points. The default overall threshold, applying to the sum of the three criteria scores with the corresponding weight each, is 10.

Each evaluator establishes an individual evaluation report.

Following the individual evaluations by the 2 experts, a consensus activity, typically mediated by the evaluation tool is organised between the 2 experts to find a consensus between them on the quality of the proposal based on the 2 evaluation reports. Comments and scores are validated by the 2 experts in a consolidated evaluation report.

Where necessary, an additional review of projects for which there was a lack of consensus in terms of scoring by individual evaluators or for which additional clarifications are required is undertaken by the TRUSTCHAIN call referent, member of the TRUSTCHAIN Consortium staff. In this case, an additional external evaluator is appointed to review the proposal. The final score is obtained based on the consensus of the 3 evaluators, one internal and 2 externals to the consortium.

The TRUSTCHAIN consortium then formally approves the ranked lists.

The admission to the online interview for applications follows these rules: **the first 20 ranked proposals are admitted to the online interview.**

In any case, all proposals admitted to the online interview must reach the scores threshold.

Regarding the communication of the results, each applicant will receive via e-mail a letter informing of the decision whether a rejection decision motivated by an Evaluation Summary Report or an invitation to the online pitching and interview session.

2.6.4 Online Interview and final selection

According to the rules, the top projects at the end of the proposal evaluation stage will be invited to the final selection stage. The applicants invited to the online interview will receive via e-mail, an invitation letter the online interview as well as relevant guidelines. **It is worth mentioning here that an invitation to the interview is not a formal invitation for funding.** The interview aims to better understand the project concept, scope, and centrality to the TrustChain vision, the team skills and competencies, capacity, and willingness to exploit the results under a commonly agreed plan with the rest of the TrustChain ecosystem and TrustChain partners. Most importantly, the online interview aims to clarify still unclear aspects of the proposal which have been identified during the proposal evaluation. The proposal evaluation report is not circulated to the applicants before the interview but forms the basis for the interaction with them.

In practice, the interview will be carried out by the evaluation board composed of the TrustChain core partners and the TrustChain advisory board members. It will be recorded to assure maximum transparency. It is based on 10 minutes pitch presentation and 20 minutes of Q&As to clarify some aspects regarding the quality of the proposal and its relevance for TrustChain, as well as to reach a final agreement

about scores and the Evaluation Summary Report (ESR). The comments on the ESR are taken into consideration for the preparation of relevant questions during the online interview and they are not communicated beforehand to the applicants.

The ESR will be structured according to the 3 criteria mentioned in the previous section (i.e., excellence and innovation, expected impact and value for money, project implementation) and will consolidate the comment of the proposal evaluation and the clarifications and overall impression obtained during the online interview. Based on the final consolidate score, the short list of winners will be produced and only at this stage the final ESR will be communicated to the applicants.

Remaining proposals will be maintained on a reserve list and potentially be later admitted in case of withdrawal or failure of one of the projects initially admitted to successfully complete any phase of the contract signing process.

The list of selected projects is then submitted to the European Commission for final screening and validation.

2.6.5 Scientific Misconduct and research integrity

Issues of scientific misconduct and research integrity are taken very seriously. In line with the Horizon Europe Rules for Participation, appropriate action such as disqualification of the application, termination of the Grant Agreement Preparation phase or, if the Grant Agreement has been signed, the implementation of liquidated damages and financial penalties, suspension of payments, recoveries and termination of the Grant Agreement, will be taken against any applicants/beneficiaries found to have misrepresented, fabricated or plagiarised any part of their proposal.

2.6.6 Monitoring process all along the sub-project's duration

For the monitoring of the progress and proper evolution of the selected projects, selected Third Parties will have to attend several mandatory internal events organised with the TrustChain Consortium. Indicatively, they are the following:

o Kick-off event devoted to knowing the different selected Third Parties and their foreseen contribution to TrustChain,

o Meeting for setting-up clear KPIs that will be linked to the funding of the selected Third Parties,

o Midterm event devoted to following-up the progress of the Third Parties according to the defined KPIs, with a pitch contest where the Third Parties will present their project outcomes and in particular their prototype and their deployment scenarios,

o Final event with a pitch contest where the Third Parties will present their solutions and in particular their modularised software components ready for distribution and a demo of their solution.

2.7 FINANCIAL SUPPORT

Open Call #2 budget totals 1.989.000,00 € to support up to 17 projects.

2.7.1 Indicative Distribution of the Funds

Selected third party innovators will become part of the TrustChain programme and will go through an exhaustive sequential process which will last 9 months. The maximum amount of the fund will vary depending on the type of team (see sub-chapter 3.1) as indicated in the table below and providing that all the phases have been completed.

Type of team	Maximum funding
Team of natural persons	97K € + 2K €
Legal entity or consortium of legal entities or combination of legal entities and natural persons	115K € + 2K €

Payments will be done in 4 instalments based on concrete results (a prefinancing, two interim payments and a final payment). A detailed evaluation process will be presented in the TrustChain Open Call #2 guide for implementation for the related periods. The 2,000.00 € extra funding will be provided in case of the project outcome results in a peer reviewed journal publication with a minimum impact factor of 2.5.

o **Beginning of the implementation and pre-financing:**

During the first weeks of the project implementation, each team will define with their coaches a set of clear and objective KPIs to be achieved and linked with the funding. These KPIs are different for each team and are related to the solution to be implemented. They will help measure the project progress, but also the commitment and involvement of the third party innovator (i.e., their consistency in attending periodic call meetings with the coaches, meeting the deadlines for reporting, among other criteria). After the definition of the KPIs, a pre-financing of 30% of the sub-grant amount will be released.

o **First midterm review and second instalment:**

At first midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project based on the evaluation of the deliverable D2. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is 20% of the total sub-grant amount. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until the KPIs for the period are assessed as completely reached. If less than 25%, the third party innovators will be automatically disqualified from the process.

o **Second midterm review and third payment:**

At the second midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project based on the evaluation of the deliverable D3. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is 30% of the total sub-grant amount. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until the KPIs for the period are assessed as completely reached. If less than 25%, the third party innovators will be automatically disqualified from the process.

o **Final review and final payment:**

At the end of the project implementation, third parties will be paid according to their overall completion of KPIs materialised by the deliverable D4. A final event will be used to evaluate third parties on a face-to-face pitch contest. The third parties will present their implemented solution, and their business plan in the context of TrustChain. A panel of evaluators consisting of the TrustChain Consortium and Advisory Board members, will assess the third-party innovators to release the final payment (remaining 20% of the sub-grant amount). In the case of an underperformance below 25%, the team will be disqualified, and no further payment will be released.

2.7.2 Summary of the funding per type of beneficiary

	Project			
	Pre- financing 30% of the total funding	Interim Payment 20% of the total funding	Pre- financing 30% of the total funding	Final Payment 20 % of the total funding
Indicative dates	M2	M4	M7	Project end
Team of Natural persons	29 100 €	19 400 €	29 100 €	19 400 €
Legal Entity(ies) or combination of legal entities or combination of legal entity (ies) and individual(s)	34 500 €	23 000 €	34 500 €	23 000 €

These numbers are indicative, detailed payment schedule and payment conditions will be settled in the Sub-grant Agreement (Annex B) at the time of the signature.

2.7.3 Origin of the Funds and specific Provision regarding multiple beneficiaries

Any selected proposer will sign a dedicated Sub-Grant Agreement (Annex B) with the TrustChain project coordinator (on behalf of TrustChain Consortium).

Specific provision regarding contracting in case of multiple beneficiaries:

In the case of projects with multiple beneficiaries (Team of natural persons, combination of legal entities, combination of legal entities and individual(s)), a Team/Consortium Agreement that designates among other the Coordinator/Authorized representative of the Team/Consortium must be adopted and signed by all the beneficiaries prior to the signature of the TrustChain Sub-grant Agreement.

The Coordinator/Authorized representative of the Team/Consortium signs the TrustChain Sub-grant Agreement on behalf of the multiple beneficiaries.

The Coordinator/Authorized representative receives the funding and must distribute the payments between the beneficiaries according to the conditions set in the Team/Consortium Agreement.

The funds attached to the Sub-Grantee Funding Agreement come directly from the funds of the European Project TrustChain, and the TrustChain consortium is managing the funds according to the Grant Agreement Number 101093274 signed with the European Commission.

As will be indicated in the Sub-Grant Agreement, the relation between the sub-grantees and the European Commission through the TrustChain project carries a set of obligations to the sub-grantees with the European Commission. It is the task of the sub-grantees to accomplish these obligations, and of the TrustChain consortium partners to inform about them.

SECTION 3: ELIGIBILITY REQUIREMENTS AND THE THREE EVALUATION REPORTS

3.1 THE ELIGIBILITY CRITERIA

Proposals need to comply both with the eligibility criteria and with all mandatory elements which are specific of the implementation mode of the Open Call 2 specific objectives and related topics. Additionally, aspects relative to page limits may impact on the evaluation and are described below. Annex 1 of this guide provides a checklist which summarise all rules and specific issues to take into account when evaluating an TRUSTCHAIN proposals.

3.1.1 Eligible countries

Only Applicants legally established/resident in any of the following countries (hereafter collectively identified as the "Eligible Countries") are eligible:

o The Member States (MS) of the European Union (EU), including their outermost regions;

o The Overseas Countries and Territories (OCT) linked to the Member States[1];

---

[1] Entities from Overseas Countries and Territories (OCT) are eligible for funding under the same conditions as entities from the Member States to which the OCT in question is linked

o H2020 associated countries (those which signed an agreement with the Union as identified in Article 7 of the Horizon 2020 Regulation): according to the updated list published by the EC[2];

o The UK Applicants are eligible under the conditions set by the EC for H2020 participation and as long as they comply with the same eligibility rules as the other Applicants

3.1.2   Language

English is the official language for TRUSTCHAIN open calls. Submissions done in any other language will be disregarded and not evaluated.

English is also the only official language during the whole execution of the TRUSTCHAIN programme. This means any requested submission of deliverables must be done in English in order to be eligible.

3.1.3   Proposal submission

Proposals must be submitted electronically, using the TRUSTCHAIN Online Submission Service accessible via Open Call #2 - TrustChain (ngi.eu) Proposals submitted by any other means, will not be evaluated.

Only the documentation included in the application will be considered by evaluators. It will be composed by a form with administrative questions to be completed directly in the platform and the proposal description attached in PDF format.

The information provided should be actual, true and complete and should allow the assessment of the proposal.

The preparation and submission of the proposal and other actions that follow this procedure (such as withdrawal) fall under the final responsibility of the Applicant.

The project proposals must strictly adhere to the template provided by the TRUSTCHAIN consortium via the F6S platform, which defines sections and the overall length.

Participants are requested to carefully read and follow the instructions in the form. Evaluators will be instructed not to consider extra material in the evaluation.

Additional material, which has not been specifically requested in the online application form, will not be considered for the evaluation of the proposals. Data not included in the proposal will not be taken into account.

It is strongly recommended not to wait until the last minute to submit the proposal.

---

[2] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf

Failure of the proposal to arrive in time for any reason, including communication delays, automatically leads to rejection of the submission. The time of receipt of the message as recorded by the submission system will be definitive.

TRUSTCHAIN offers a dedicated support channel available for proposers at trustchain@ngi.eu for requests or inquiries about the submission system or the call itself. Those received after the closure time of the call will neither be considered nor answered.

3.1.4   Multiple submission

Given the fact that this call is a competitive one, and one Applicant should focus on only one specific topic the following apply:

o   Only one proposal per **Applicant** should be submitted to this call, and only one proposal per **Applicant** will be evaluated. In the event of multiple submissions by an applicant, only the last one received (timestamp of the system) will enter into the evaluation process. Any other submitted proposals by the same Applicant involving the same Applicant will be declared non-eligible and will not be evaluated in any case.

o   Only one proposal per **Individual** should be submitted to this call whether if he/she applies within as Team of natural persons or as part as part of a consortium member. If an individual is taking part in several teams/consortium, the members of the other teams/consortium will be informed about the participation of an individual in multiple teams/consortiums. Then, only the last proposal received (timestamp of the system) including the individual will enter into the evaluation process. Any other submitted proposals involving this Individual will be declared non-eligible and will not be evaluated in any case.

Note that the regular functioning of the F6S platform limits to one application submission per F6S user in each call. If an F6S user wishes to submit more than one application, **for example on behalf of different Applicants**, the F6S user should request support from the F6S support team (support@f6s.com) at least 10 days prior to the open call deadline.

3.2   THE SPECIFIC REQUIREMENTS

In order to guarantee equal treatment among the proposals, the Applicants are required to respect page limits. The Evaluators are asked to disregard any information contained in the excess pages. Should an Evaluator identify an issue regarding the page limits, they are asked to immediately contact their topic coordinator.

3.3   THE THREE EVALUATION REPORTS

3.3.1   The Individual Evaluation Report

The quality of the Individual Evaluation Report is paramount as it constitutes the basis of the Consensus Report which is sent to the Applicant. It should therefore give a clear assessment of the proposal based on its merit, provide clear feedback on the proposal's weaknesses and strengths with comments which are consistent with the scores. High quality reports are crucial to the success of the consensus phase.

Before starting to draft their Individual Evaluation Report, Evaluators are recommended to know what is expected from the Applicant thus to check the scope of the TRUSTCHAIN Open Call 2, the description of the specific objectives. The challenge, the requirements, the context as well as the expected outcomes to be considered by the Applicant are presented in section 2.5.2, 2.5.3, 2.5.4 of this guides.

The Evaluators must also be aware of how the proposal should be structured. There is 2 distinct parts:

o   The administrative part including any obligatory supporting documents specified in the call and the ethics issues table (see annex 2).

o   The research proposal description according to the TRUSTCHAIN template and instructions set in the TRUSTCHAIN guide for applicant (see annex 3).

The research proposal description is the most important part to be considered by the Evaluator. It should contain a maximum 10 pages and the following sections:

o   **The first page** with the proposal acronym, full title, and the topic(s) selected.

o   **The proposal** with:

Page count starts here

1. Project summary (300 words)
2. Applicant background (Max. 1 pages)
3. Proposal description (Max. 8 pages)
    - 3.1   Concept and objectives (Max. 1 page)
    - 3.2   Proposal solution (Max. 2 pages)
    - 3.3   Expected impact (Max. 2 pages)
    - 3.4   Business model and sustainability (Max. 1 page)
    - 3.5   Implementation (Max. 2 pages)

Page count finishes here

It will be assessed against the evaluation criteria set in section 2.6.3.

Evaluators are strongly advised to refer to the evaluation grid set in annex 1 to draft their IER.

Practically, evaluators should provide comments for each criterion/sub- criterion and list them under a strengths paragraph and a weaknesses paragraph. The assessment must be factual and not an outcome of personal interpretation. All shortcomings should be clearly justified by providing concrete examples related to the proposal. No recommendations should be made.

When comments are set, Evaluators can proceed to scoring each criterion based on the scoring scale provided in section 2.6.3. **The scores must reflect the comments.**

3.3.2 CONSENSUS REPORT

High quality consensus reports are crucial to the success of the overall evaluation and the quality of the TRUSTCHAIN project outcomes. It should demonstrate a consensus of the two evaluators on the quality of the proposal and provide a clear assessment of the proposal based on its merit with clear feedback on weaknesses and strengths.

Practically within the pool of two evaluators per proposal, a rapporteur (from the TRUSTCHAIN staff) will be assigned the task of drafting the consensus report based on the 2 Individual Evaluation Reports.

First the rapporteur aggregates the comments of the 2 Individual Evaluation Reports for each criterion under a strengths paragraph and weaknesses paragraph. When there is disagreement on the quality of some sub criterion, the rapporteur lists the related comments under a paragraph titled "to be discussed". This phase leads to the draft Consensus Report that will be discussed among the 2 evaluators in particular the paragraph "to be discussed" so that to find a consensus.

When a consensus is found, the rapporteur proposed scores for each of the 3 criteria to be discussed. When consensus is obtained both on comments and scores then the consensus report is ready for the ranking phase and later on to be sent to the applicant to motivate the rejection of their proposal. Selected applicant for the online interview receive solely an invitation to the interview.

3.3.3 THE EVALUATION SUMMARY REPORT

The evaluation summary report is the base document for the funding decision to be made. It is composed of the consensus report related to the proposal and the evaluation summary of the online interview. It includes the decision of the evaluation board (TRUSTCHAIN topics referents and the TRUSTCHAIN advisory board members) whether to distribute funding for selected projects or to register the proposal on the reserve list.

The evaluation summary of the online interview is the outcome of a qualitative evaluation according to the evaluation criteria set in section 2.6.3 and in particular to the credibility of the proposed project outcomes, the value for money, the collaborative Spirit/Commitment of the applicant, and the business compatibility. **The score for the**

interview will be the average of the scores of the 4 criteria.

Based on these final scores, the short lists of winners will be produced.

When this phase done, the evaluation summary report is ready to be sent to the applicant to motivate the evaluation board final decision.

SECTION 4: TRUSTCHAIN OPEN CALL 2 EVALUATION STATISTICS & OUTCOMES

4.1   EXTERNAL EVALUATORS SELECTION-STATISTICS & OUTCOMES

4.1.1   CONTEXT

A total of 15 independent experts from all over the world were onboarded in contributing to the evaluation of TRUSTCHAIN Open Call 2. Three webinars were hosted by Trust Chain Consortium to introduce the project and Open Call 2. The webinars also discussed how to ensure the implementation of user-centred approach in TRUSTCHAIN; taking care of ethics aspects in TRUSTCHAIN issues around ARF/digital wallet. The first webinar was hosted on 24th July 2023 followed by a second on 6th September 2023.

The target audience were researchers, innovators and developers whether from the academic sector or private sector with possible experience in open call proposals evaluation and horizon 2020 funding as well as demonstrate expertise in domains such as: Blockchain & distributed systems, smart contracts, cryptography, digital identity, self-sovereign identity, software engineering, computer engineering, multi-agent system, information systems, IoT, digital twin, cloud, security, cyber security, big data, telemetry systems, Artificial Intelligence, Permission less innovation, decentralisation and level playing field, Social good, fairness and ethical behaviour, Sustainability/Eco-friendliness, Ecosystem economics, Well-balanced economy, Green, environmental sustainability, Data Protection, context aware services, Smart Cities, FinTech, digital media, education and training, business services, entertainment, Public sector, Healthcare, logistics & supply chain, business management, innovation management, etc.

So, 15 independent experts (External Evaluators) have contributed to the evaluation of this call. Given the ratio of the evaluators admitted and the number of proposals to evaluate (73), each evaluator evaluates four to five proposals according to their expertise.

4.1.2 Countries Coverage

A large number of countries were covered thanks to the communication and dissemination efforts in getting external evaluators. So, this Open Call 2 received evaluators' interest from 17 countries covering widely Europe as shown in the chart below.

Countries' Representation

Country	Value
Italy	3
Spain	3
Greece	3
Portugal	2
France	2
Malta	1
United Kingdom	1
Bosnia and Herzegovina	1
Deutschland	1
Norway	1
Lithuania	1
Slovenia	1
Ukraine	1
India	1
Bulgaria	1
Austria	1
Albania	1
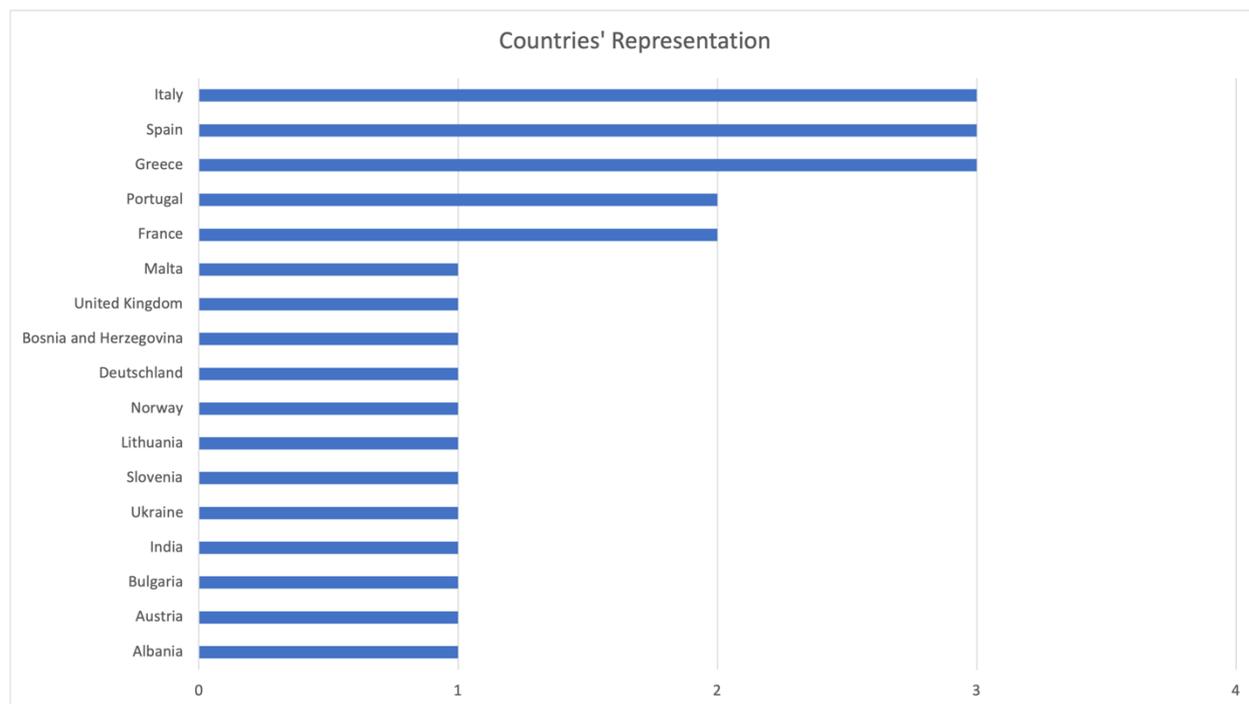
4.1.3 Gender Balance

On the 25 external evaluators, 6 (24%) were females and 19 (76%) were males. Even if gender balance was not achieved, we will try to engage more women from next open calls, thus reaching better distribution than the current trends of the women engage in the ICT sector. Indeed, currently only around 17% of the almost 8 million ICT specialists in Europe are women (Women in the ICT sector | European Institute for Gender Equality (europa.eu)).

4.2 THIRD PARTIES SELECTION-STATISTICS & OUTCOMES

4.2.1 Context

A total of 91 proposals from all over Europe have been submitted to this first TRUSTCHAIN open call. 73 of them were eligible and evaluated.

The target audience were researchers, innovators and developers whether from high tech companies including SMEs, academia or natural person(s) legally established in an EU Member State, H2020 associated countries or Overseas Countries and Territories (OCT) linked to the Member States.

4.2.2 Profile of Applicants and technology domains of expertise

Applicants were asked whether they were applying as:

- o   as a group of individuals (team)
- o   as a group of individual(s) and organization(s)
- o   a group of organisations (consortium)
- o   a single organisation (legal entity)

Out of the 73 applications, 44 were submitted by a single organisation, 19 by a consortium, 5 by a group of individuals, and 5 by a group of individual(s) and organization(s).
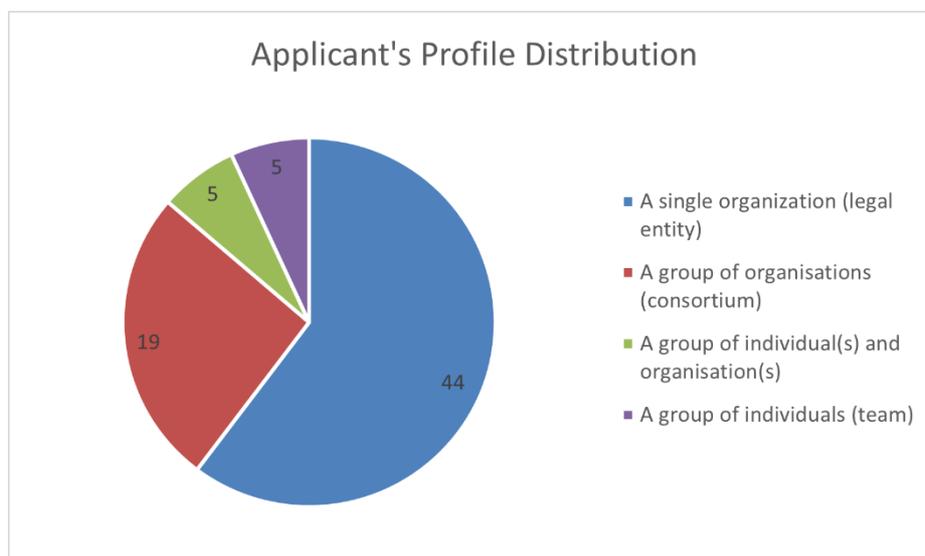
At the same time, applicants were asked to select their technology domain of expertise as follow:

- o   Data & AI
- o   Decentralised solutions, blockchain, distributed ledger

o Measurement, monitoring, analysis & abuse handling

o Middleware, distribution, deployment, operations, DNS, authorisation, authentication, reputation systems

o Services & Applications (e.g. email, instant messaging, search, video chat, collaboration, community)

o Software Engineering (Including protocols, interoperability and fundamentals e.g. cryptography, algorithms, proofs)

o Trustworthy hardware & manufacturing

o Cloud engineering, digital twins, edge and fog computing, Digital twins, edge and fog computing,

o Cryptography, standardisation and security engineering,

o Trustworthiness (Including: transparency, auditability and security),

o Privacy and confidentiality,

o Sustainability/Eco-friendliness, ecosystem economics, Well-balanced economy, Green, environmental sustainability

o Middleware, distribution, deployment, operations, DNS, authorisation, authentication, reputation

o Digital identity management, self-sovereign identity, Inclusiveness, accessibility diversity and democracy

4.2.3 Countries coverage by eligible applications

A large number of countries were covered thanks to the communication and dissemination efforts in getting participants from all eligible countries. So, this Open Call 2 received proposals from 28 eligible countries. Spain (17,0%), Portugal (8%), Romania(8%), Netherlands(7%), Italy(7%), Slovenia(5%), Estonia(4%) and Bulgaria (4%), were the 8 countries the most represented.

Countries' Representation
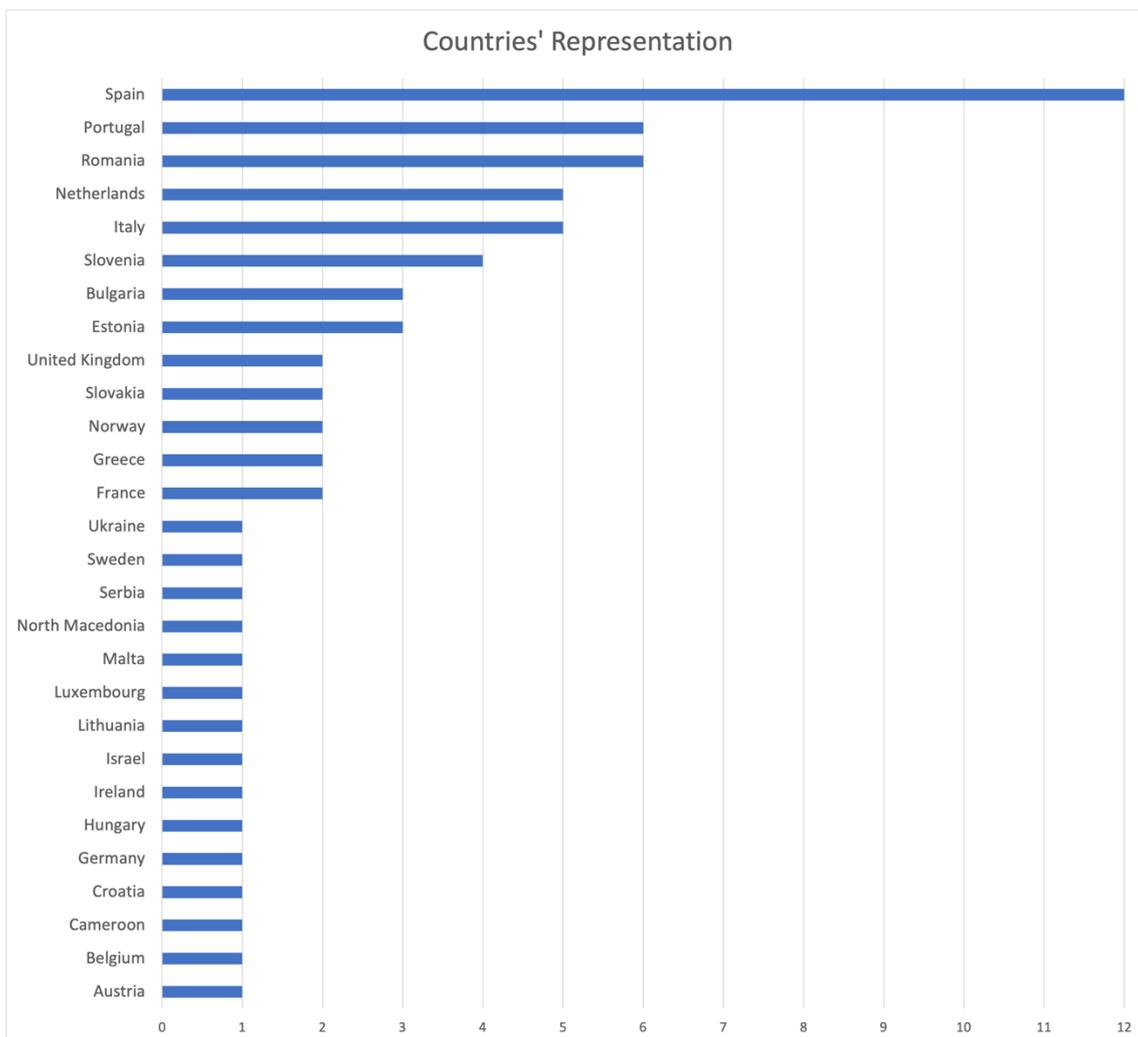
4.2.4 Proposals Selected

After the evaluation process, only 15 proposals were selected from the 73 valid proposals submitted leading to an overall success rate of 20%. The following presents the selected projects by objectives and topics to whom they belong.

o **DOOF - Data Ownership Orchestration Framework**

Country: Italy

Project Abstract:

Today control over data visibility is centralized into the hands of data sharing platforms' owners. Rightful data owners are not actively involved in the data value chain, and this

results in low trust and willingness to share data, hindering the growth of a European data market. Based on a patented multicast end-to-end encryption scheme and smart contracts, Ecosteer decentralized consent management technology – the Data Visibility Control Overlay (DVCO) – allows individuals to unilaterally grant & revoke visibility over data streams generated by their devices to selected stakeholders, as mandated by the GDPR. Additionally, a smart contract implements a compensation mechanism based on tokens, incentivizing data sharing. Within NGI TrustChain Call #2, Ecosteer will develop the Data Ownership Orchestration Framework (DOOF), a set of open SDKs, libraries and Smart Contracts that allows data owners to exercise data ownership rights – i.e. grant, revoke and monetize data visibility. In fact, the DOOF's objective is to facilitate the integration of the DVCO as well as any other consent management technology, e.g. for data sets rather than data streams, with any data source and enterprise IT system, enabling companies and institutions to deploy user-friendly data exchanges privacy-compliant by design. In this project Ecosteer will integrate its technology with smart-home sensors and distribute them among a selected group of citizens in Bolzano. Thanks to a user-friendly interface, citizens will be able to unilaterally control third party visibility over their data and to be compensated for data sharing. Such validated solution will be proposed to Utilities to deploy their own transparent, ethical and GDPR compliant data exchanges, involving their customers and business partners. Additional data sources, e.g. energy meters, other smart home sensors, wearables, etc., can be added over time, expanding data sharing & monetization opportunities without impacting system scalability provided as-a-service by the DOOF.

o UtiP-DAM - Utility-Preserving, Decentralized Anonymity of Mobility data

Country: Israel

Project Abstract:

Understanding crowd mobility is essential for governments and businesses to prepare for long-term challenges like climate change, mid-term challenges like increasing urbanization, and short-term challenges like controlling the spread of diseases. For instance, mobility data is used to optimize public transportation, improve mobile and wireless networks and study human contacts to help public health experts track viral diseases. However, mobility data is a very sensitive type of data, since mapping the movements of individuals can reveal personal information. Anonymization cannot be limited to suppressing metadata containing the subject's identity, because the origin, the destination and even the intermediate points of a trajectory may allow re-identifying the individual who followed it (de Montjoye et al, 2013). Proper anonymization requires masking detailed spatiotemporal Information. Currently, the standard approach to building anonymized datasets is centralized: the subjects send their data to a controller, who takes care of producing an anonymized mobility data set. This requires subjects to blindly trust the controller, which is not acceptable in most cases. There is another risk inherent to mobility data, which is the possibility to re-

identify individuals in anonymized datasets by cross-referencing them with other existing or newly published datasets (Srivatsa et al, 2012). Hence, the requirement for anonymity of mobility data must be controlled in consideration of publicly available data. The goals of our project are threefold: - develop a decentralized method, based on utility-preserving k-anonymity, that will allow anonymization of mobility data in a way that guarantees that even the controller cannot re-identify individuals in their datasets. - create an auditing tool that enables data controllers to audit their proprietary datasets for de-anonymization risks and anonymize the data if risks are uncovered using a centralized k-anonymity algorithm. - create a verification tool enabling individuals and companies to uncover public datasets that contain similar trajectories to theirs.

o <u>MorphMetro - Secure and privacy-preserving exchange and analysis of measured data based on homomorphic encryption</u>

Country: Croatia

Project Abstract:

Measured data obtained by measuring devices and its subsequent analyses (measured data accuracy, errors, measurement uncertainty, regulation compliance, etc.) are pillars for quality assurance (QA) in a wide spectrum of various industries (food industry, pharmacy, etc.). Currently, there is no universally accepted protocol for the machine-interpretable structuring and digital dissemination of measurement data, leading to concerns in data governance and user privacy. Fortunately, the science of measurement (metrology) is undergoing digital transformation, as evidenced by BIPM's recent Joint Statement of Intent. Our solution builds on emerging new standards (SI-Digital, Digital Calibration Certificates, etc.) to add a crucial component for digitalizing QA reliant on measured data. We propose an open-source solution for the secure exchange of data (measured data and subsequent analyses) in use cases where one needs analysis of measured data to be carried out by a third-party data analysis service. This "third party entity" operates independently of the entity (organization, department, team) involved in data collection most often if: - there is a need to ensure an unbiased analytical perspective (often prescribed by metrology regulations) and/or - the analysis is carried out as commercial service offered on the market and/or - there is a separate "in-house" analytical department/team within the same organisation In each case it must be ensured that data security is maintained, reducing the risk of unauthorized access or data misuse, including privacy risks if measured data contains possible Personally Identifiable Information (PII). Shortly said, our proposal has a simple input → measured data, and a simple output → analysis of measured data. However, it will use state-of-the-art technologies (blockchain, homomorphic encryption) and emerging standards and architectures established in the EU space (European Blockchain Service Infrastructure (EBSI), Alastria, Digital Calibration Certificates (DCC)) in order to make the solution trustworthy, scalable and compliant with prevailing and upcoming regulations.

○ SURE - Synthetic Data: Utility, Regulatory compliance, and Ethical privacy

Country: Italy

Project Abstract:

Clearbox AI, an award-winning tech startup based in Turin, Italy, specializes in facilitating AI and Analytics projects through Synthetic Data generation. Their privacy preservation and data augmentation expertise, notably in banking, finance, and healthcare, aligns seamlessly with TRUSTCHAIN's mission to establish secure and dependable data routes for responsible AI adoption. The proposal confronts the challenges posed by the rapid evolution of AI, particularly in safeguarding user privacy and data governance. AI presents distinctive privacy risks, including potential individual identification in anonymized data. Clearbox AI's solution centers on Privacy-enhancing technologies (PETs), focusing on Synthetic Data. This method preserves real-world data's statistical properties and predictive capabilities while ensuring privacy. The project's core goals involve creating an open-source library that harmonizes user privacy and data utility for AI training. It will also provide fine-grained privacy controls and uphold regulatory compliance through GDPR adherence features. Moreover, the project promotes responsible data practices, especially in the financial sector. The proposed product, named SURE, empowers users to evaluate the privacy and utility of anonymized datasets using both traditional anonymization techniques and synthetic data. Its user-friendly interface enables individuals with limited AI knowledge to evaluate and test anonymous and synthetic datasets, preserving privacy without sacrificing utility. The project's impact is poised to be significant. As AI's contributions to the global economy grow, SURE's provision of a customizable, open-source synthetic data library democratizes access to secure and privacy-respecting data solutions. It serves a diverse user base, encompassing fintech and healthcare companies, equipping them with a potent tool to bolster their data privacy practices while maintaining dataset utility. Additionally, the proposed solution dovetails with TRUSTCHAIN's fundamental objectives, cementing its status as a valuable asset in erecting secure and reliable data pathways for responsible AI adoption.

○ dGUARD - Privacy preserving data-sharing platform

Country: Spain

Project Abstract:

Nowadays, there is a widespread perception that data has great value. Harnessing this value and the vast amount of data available can generate huge revenues for online service platform providers. It is common for data owners not to take advantage of this value in an adequate way and often give or share their data for free or pay with it for the use of a service. In general, these platforms offer services without preserving the privacy of users' data, without secure data exchange, without identification of the data

or its provenance, or without providing mechanisms to track, explain and validate the data. The main limitation of data sharing platforms is users' lack of trust in privacy and control to manage their data. The user's perception of helplessness is increased by not knowing how their data is used and with whom it is shared. Therefore, it is necessary to preserve user data privacy and secure data exchange, in order to build trust among participants and ensure data sovereignty. Leveraging the capabilities offered by blockchain technology and the use of advanced cryptographic technologies to ensure data sovereignty in the third-party data sharing, this project will focus on delivering four main components: 1) A consent management system based on self-sovereign digital identity authentications and interactions, 2) A privacy preserving authentication mechanism to enable privacy preserving authentications thus boosting anonymization, 3) A proxy re-encryption scheme to guarantee e2e data privacy 4) A blockchain notarized audit-trail to guarantee traceability, non-repudiation and accountability. dGUARD offers an innovative solution that harnesses the power of self-sovereign digital identity, Zero-Knowledge Proofs and proxy re- encryption with a comprehensive approach designed to revolutionize the way data exchange procedures are carried out, with a primary focus on improving consent management, strengthen data security, privacy and anonymity, while ensuring robust process accountability.

o NG-SC- Next Generation Smart Cities

Country: Slovenia

Project Abstract:

In the rapidly evolving landscape of the Next Generation Internet (NGI), data storage and management are undergoing a profound transformation. Historically, centralized entities and corporations held dominion over vast data stores. However, the NGI heralds a paradigm shift, prioritizing user-centric data governance, where individual users maintain control and ownership of their data, and even more intriguingly, their IoT devices become active contributors to this new ecosystem. In recent years, the idea of smart cities in which the infrastructure layer and data acquisition/storage is made available by government entities has gained significant traction. This is mostly attributed to the higher availability of cost-effective IoT devices/sensors, and growing connectivity and bandwidth of networks. However, the financial investments required to setup, and maintain the infrastructure are a high barrier to entry. Moreover, these infrastructures are commonly centralized into three layers namely, data acquisition layer, storage and computation layer, and finally the application layer in which users and companies participate in by leveraging the data. This project envisions a future where users actively participate and maintain all three core infrastructure layers. To realize this, we propose a decentralized model that allows both users and their smart devices to contribute building a decentralized infrastructure. The solution builds on a paradigm shift in the way data driven computation occurs. As such, data never leaves

the device, instead computation is broken down into independent sets, and migrated across the network. This guarantees data privacy, and ownership whilst at the same time, makes use of the currently untapped computational resources of IoT devices. Our strategy involves harnessing advancements in Multi-Party Computation (MPC) technology, advancing a novel MPC protocol to a demonstrative phase. All software of the platform and the MPC protocol will be made open-source to further establish trust and inclusivity of the solution. In summary, our project seeks to empower users to actively participate and be rewarded in the data economy, fundamentally transforming data ownership in the NGI era. We propose a user-centric data governance model, fortified by cutting-edge technology, and a decentralized resource marketplace that enables users to take control of their data and computational resources. This vision aligns perfectly with the evolving landscape of the NGI, where data is not just a commodity but a democratized and user-empowering currency.

○ DUME - Decentralised User-Centric Media Extension

Country: Portugal

Project Abstract:

Tidy City encourages both individuals and organisations to routinely capture high-resolution images of streets and roads. The images captured with Tidy City app are then analysed by advanced AI models on centralised servers, detecting various urban challenges such as waste mismanagement or signage issues. However, like many contemporary platforms, once users submit their data to Tidy City, they relinquish much of the control over it. Project DUME aims to change the centralised nature of digital platforms like Tidy City by: 1. Extending Solid Protocol that adeptly manages large-scale media datasets with decentralised web platforms. 2. Validating the robustness of the decentralised, user-centric features of the protocol created in 1., by implementing and testing it in Tidy City. The challenges of implementing a protocol capable of handling vast volumes of high-resolution photographs with associated metadata for streets and roads, ready for AI model training, are manyfold:

- For AI model training, swift and efficient data retrieval is essential. This involves implementing parallel data retrieval processes, batch data requests, and caching mechanisms to ensure minimal latency.

- The protocol should support rich metadata annotations, ensuring indexing mechanisms deliver quick searches and filtering based on this metadata.

- Specific AI access control ensures that AI model trainers can access the requisite data without compromising other personal or sensitive data. This involves creating specialised 'views' or 'profiles' of the data specifically curated for AI training.

- Given the dynamic nature of data (new images added constantly), the protocol must support robust versioning mechanisms, allowing users and applications to fetch historical data versions efficiently. DUME aims at creating a validated path not only for Tidy City's evolution, but also for numerous other projects that depend on large amounts of media data, towards a decentralised digital paradigm where users maintain sovereignty over their media contributions.

○ AURORA MINDS - Empowering Children with ADHD Through Privacy-Preserving Data Collection

Country: Greece

Project Abstract:

Aurora Minds represents a groundbreaking initiative aimed at addressing the need to early and accurately diagnose ADHD in children, while prioritizing data privacy and security. In a landscape crowded with assistive technologies for ADHD, this project distinguishes itself by integrating robust privacy measures at its core. Existing ADHD assistive technologies often overlook privacy and security concerns, leaving users vulnerable to data risks and profiling. To counter these challenges, AURORA MINDS implements a multi-layered security framework, including Identity Management (IdM) and Privacy-Enhancing Technologies (PETs). This approach enhances data security, strictly controls access to sensitive information, and ensures compliance with data privacy regulations. The project leverages machine learning techniques such as federated learning and local differential privacy to protect sensitive user data during collection and analysis, aligning with GDPR requirements. Aurora Minds adopts a human-centric design approach, tailoring personal data collection from a child while s/he interacts with a serious tablet animation game to cater a unique ADHD risk assessment process. The project benefits various stakeholders, including children, parents, educators, and clinicians. Children are examined through a specialized application supporting their behavioral unique requirements and independence. Parents receive reassurance regarding data confidentiality, gaining insights into ADHD risk assessment and relevant information to provide better support. Clinicians benefit from enhanced diagnosis capabilities, aided by qualitative and quantitative measurements. Access rights are carefully managed using the Privacy-ABCs (Privacy-Attribute-Based Credentials) approach, ensuring that each entity—child, parent, and clinician—receives appropriate access privileges. By incorporating this proposal into the TRUSTCHAIN framework, AURORA MINDS elevates TRUSTCHAIN's reputation by exemplifying a steadfast commitment to data privacy and security. The emphasis on PETs and federated machine learning not only bolsters data privacy but also mitigates legal risks associated with data sharing, enhancing data quality for effective decision-making.

○ <u>OIDC PRINCE - OpenID Connect with PRIvacy-eNhanced ConsEnts</u>

Country: Portugal

Project Abstract:

The OIDC PRINCE project aims to enhance the privacy support in user consents used in OpenID Connect authentication and authorization processes. Nowadays the consent to access the claims about end-user and authentication events (e.g., gender, birthdate, phone number), may have associated privacy issues. Users need to be informed regarding the potential risk of providing consent for the personal information access by services/entities that may not be trusted by the user and the OpenID Provider, which is responsible to manage the authentication and authorization. OpenID PRINCE introduces the proof of privacy regulations compliance (e.g., compliance with GDPR) in the OIDC discovery and registration processes using data privacy vocabulary (DPV) specification that can be certified by entities external to the OIDC authentication process. These proofs can be stored securely in a EMV compliant blockchain. OIDC PRINCE also enables privacy analysis to assess the risk of services accessing the end-user private information. This analysis, performed by Fuzzy Logic models considers the claims which access is being requested and the profile of the service requesting the access, for instance if it is a service associated with acquisitions or a service for education and learning. OIDC PRINCE contributes to enhance the support of privacy in OpenID connect by enabling informed consents, and by minimizing the data sharing with entities that are not trusted, or that do not provide evidence of being trustworthy in terms of privacy management.

○ <u>PECS - Privacy Enrooted Car Systems</u>

Country: Italy

Project Abstract:

People's privacy control over the personal data that they generate and consume while they drive modern cars is extremely weak at present. There is historical as well as recent evidence that car brands harvest a variety of personal data from drivers and, arguably, full compliance of their processing with the European General Data Protection Regulation is questionable. PECS revolutionises modern car ecosystems for what concerns the processing of personal data. It does so by advancing, tailoring to the specific domain and, ultimately, combining together both soft and hard privacy measures. The project raises drivers' soft privacy through the PECS interface for static and dynamic control of personal data, so that drivers can decide what to share and with whom and when, as well as follow and control the flows of data at service run time by means of multy-sensory media techniques. Hard privacy thrives in the project through a combination of obfuscation techniques including Federated Analytics, Secure Multi Party Computation and Pseudonymisation, so that drivers are enabled to keep their personal data opaque to anyone from the outset. All developments proceed from the

established academic laboratories of UNICT-UNIMORE, then are demonstrated in the operational environment of MASA-UNIMORE, reaching TRL7. The PECS results stem from the open-source, open-Internet approaches, hence bear huge technical, societal and industrial impacts, bringing Europe at the forefront of data protection, at least in the automotive domain. PECS also brings forward a whole new range of business opportunities such as various forms of software support for its technologies, and of renewed car services leveraging privacy-by-design-by-default. Finally, PECS provides the necessary grounds favouring the inception of a new breed of services that would be naturally enrooted on drivers' sensitive data such as sexual, religious and political orientations, e.g. apps for dating, praying and debate on political topics.

o EIDCMP - eIDAS compliant membership platform

Country: Portugal

Project Abstract:

WalliD and the Portuguese Blockchain and Cryptocurrencies Association (APBC) are forging a dynamic partnership to develop an advanced membership platform, poised to revolutionize the verification and credential issuance processes for Professional and Governmental Associations. Our platform will enable these associations to seamlessly verify member IDs and issue dynamic, verified credentials, all while accommodating new data updates. Crucially, this system will operate in full compliance with eIDAS regulations and adhere to the latest industry standards. In this project, our primary approach is to leverage existing technology and established standards, ensuring accessibility for all associations. Our comprehensive system will:

- Verify member IDs with meticulous adherence to eIDAS regulations, harnessing the power of digital IDs and digital wallets.

- Issue verifiable credentials in strict compliance with W3C standards and the eIDAS directive.

- Enable user management and sharing of credentials.

- Safeguard user data throughout the entire process, from verification to credential issuance, ensuring a secure and private environment.

With WalliD and APBC at the helm, this initiative will pioneer a new era of streamlined and secure membership management, providing associations and institutions with a powerful tool to enhance their services and compliance, while safeguarding the privacy of their members.

o **DID-IMP - Decentralized public key Infrastructure for Defended IoT data management and procurement**

Country: France

Project Abstract:

The DID-IMP project is building a decentralized public key infrastructure to allow any connected object to be able to deliver or procure secured and traceable data. To achieve this, Werenode is leveraging blockchain technologies to remove the need for a classical hierarchical structure with players like the Certificate Authority (CA) and the Registration Authority (RA). For DID-IMP, we replace these administrator-like trusted third parties (RA & CA) with a feeless blockchain smart contract. The blockchain is also used as a Certificate Store on which services providers can issue and manage revocable certificates and credentials. Such a lean architecture is especially well adapted for Internet of Things (IoT) Secure Automatic Data Sharing SADS. Indeed, SADS can be used in various ways to simplify and streamline data sharing processes, and to secure and trace data transfers. Some of the main use cases include: Connected Cars: DID-IMP-enabled cars can automatically share data for tolls, parking, vehicle recharging (electricity or hydrogen), and other transportation-related processes, making the service more convenient for drivers. They can automatically deliver maintenance data with selected relevant bodies.

Remote healthcare: SADS systems can enable remote healthcare services, such as telemedicine and patient monitoring, improving access to healthcare. Sensors can also collect data on patient health and behavior and control the delivery of this data with specific accredited personas. Cognitive Cities: IoT plays an important role in creating smarter, environment conscious and more efficient cities. Applications like smart traffic management, water and waste management, and public safety rely on secure data transfer to optimize operations and protect citizens' data. Energy Management: IoT devices in the energy sector, such as smart meters and grid sensors, transmit data about energy consumption and distribution. Secure data transfer helps utilities ensure data accuracy and protect against unauthorized access. It's also a key component to be able to build local and decentralized energy communities. And also, Smart Homes, Maintenance, Logistics... In a nutshell, we build a Trust Chain for IoT secure data sharing, bringing better traceability to data, securing their flow and allowing companies to reduce administrative overhead, save time and money, and offer a better protected data sharing experience for final customers. Indeed, users can retain ownership and control over their IoT data while granting access to specific parties through permissioned credentials. Additionally, our SADS-enabled solution can help to manage the flow of sensitive data and the compliance to the new European and Global regulations, thanks to the native traceability features provided by blockchain technologies combined with the process proposed by this DID-IMP project, which implies a traced blockchain transaction for each data transfer, also tracking the main regulatory characteristics of the data exchanged.

○ GUEDHS - Data Governance and User privacy envisioning an EHDS pilot deployment

Country: Portugal

Project Abstract:

The Covid-19 crisis has significantly raised the urgency for efficient use of health data beyond the healthcare providers' borders. It has also highlighted the importance of joint European health initiatives and data-sharing scenarios, as the ones promoted by the European Health Data Space (EHDS). Data can improve patient outcomes (primary use of data) while fostering research, and accelerating the development of new health services (secondary use of data), but only if it is shared securely and reused by stakeholders. In this process, privacy must be respected, data usage control enforced and transparency ensured. Establishing the EHDS is an integral part of building a European Health Union and the GUEDHS project will pilot it, at an interregional scale. As the epidemic risks increase globally, and to fast-forward crisis preparedness and resilience, GUEHDS project will present a solution leveraging existing concepts and technologies developed for data value-sharing in respiratory infections scenario. Promptly will bring a federated learning framework, while IPN will adapt a cybersecurity tool, for fast deployment of a Federated Network in action. This solution will enable data custodians to grant and revoke permissions on the data they control, and monitor the data used by FL tasks at the different data nodes. The testing data partners — CHUC and CHUdSA – will pilot-test GUEHDS solution within a clinical study on the epidemiological trends of respiratory viruses. This pilot will establish the ground for the Portuguese Observatory for Respiratory Diseases, an initiative that can be scaled at a European level together with Regulators (EMA) and Life Science Companies.

○ ProvenAI - Provenance in AI

Country: Greece

Project Abstract:

Imagine a world where every piece of data, every article, and every contribution has a traceable lineage. Where, instead of AI models indiscriminately assimilating vast volumes of data, every fragment has a unique identifier and provenance. ProvenAI promises such a world, aspiring to construct a Decentralised Provenance Platform tailored specifically for unstructured data. It doesn't stop at mere identification ; the objective is to ensure knowledge creators can trace how their content is utilised while receiving just compensation. Traditional platforms offer limited utility in the evolving realm of Generative AI and semantic searches. ProvenAI distinguishes itself by segmenting massive unstructured datasets into semantically relevant sections, ensuring only pertinent data segments respond to specific AI queries. This not only

promotes data minimization but also protects against unwarranted data exposure. In this rapidly advancing age of information, ProvenAI stands as an ally to ethical AI development and data governance. By valuing the rights of content creators and emphasising user privacy, it seeks to redefine the dynamics of knowledge acquisition and compensation in the AI sphere. With ProvenAI, we're not just building a technology; we're nurturing a vision where innovation aligns seamlessly with integrity, accountability, and respect for every byte of knowledge contributed. As we move forward, ProvenAI seeks to play a pivotal role in shaping a digital landscape that is both equitable and transparent, ensuring that the digital footprints of today become the trustworthy paths of tomorrow.

○ <u>LED-UP - LEVEA's Enhanced Data Governance and User-Centric Privacy in Decentralized Systems</u>

Country: Austria

Project Abstract:

Amid the digital evolution, a pressing need has emerged to bolster user privacy and data governance. This is especially palpable for people forced to live in refugee camps who require robust, private, and transparent health data management. Our groundbreaking proposal, built upon the Alastria B Network, aims to redefine the way we approach these challenges. Using pioneering tools like Decentralized Digital Identity and Homomorphic Encryption, coupled with DAO structures, we offer a framework where data privacy is not just a feature but the very foundation. While the current digital landscape offers decentralized solutions, many fail to put user privacy and data governance at the forefront. Our model diverges, ensuring every data interaction prioritizes user consent, traceability, and security. This commitment extends beyond mere encryption; it reshapes how data is stored, shared, and accessed, always keeping the user's rights at the centre. Through consistent collaboration and feedback loops with users and stakeholders, especially those from vulnerable settings like refugee camps, we craft a solution inherently aligned with their needs. Our co-creation ethos guarantees that our framework is not only technologically advanced but also deeply empathetic, understanding, and responsive to real-world user challenges. Moreover, our proposed framework introduces a paradigm where data sharing is both transparent and potentially beneficial for users, marrying user privacy with data governance seamlessly. This harmony between privacy and governance is pivotal in sectors beyond healthcare, finding resonance in finance, real estate, and more. Together as Hora e.V. with our industry-leading members, we are able to realise a paradigm shift on how user privacy and data governance is handled in a decentralized world. Thereby, we are in sync with TRUSTCHAIN's vision, which seeks to set a transformative benchmark.

4.2.5 Funding allocation per countries

By rules, the TRUSTCHAIN Open Call 2 funds are distributed to the legal representative of the legal entity or of the consortium or to the legal representative of the team of natural persons. In the two last case, a consortium agreement or team agreement is signed by the parties belonging to the consortium or team of individual mentioning amount shared between parties. The figure hereafter shows the funding distribution per countries taking into account only the legal representative's countries. So, Portugal, Italy and Greece are the most funded countries with 26.7%, 20%, and 13.3% of the total OC2 funding distributed to them respectively. Then follow Austria, France, Slovenia, Spain, Croatia, and Israel each taking an approximately 6.7% of the funding each. From a geographical point of view, the funding of TRUSTCHAIN for this Open Call 2 covers well Europe.

Funding Distribution per Country (%)

■ Israel ■ Croatia ■ Spain ■ Slovenia ■ France ■ Austria ■ Greece ■ Italy ■ Portugal
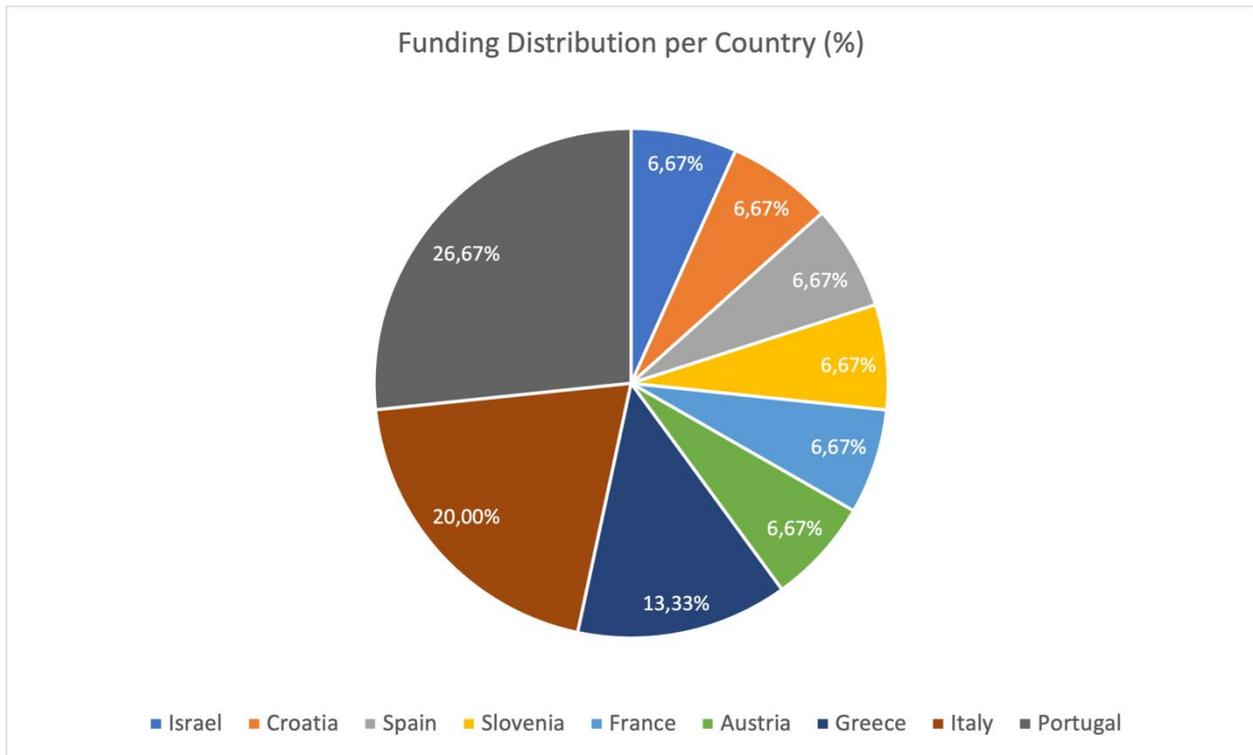
SECTION 5: ETHICAL PRINCIPLES RELATED TO H2020 RESEARCH AND INNOVATION ACTIONS EVALUATION

For the TRUSTCHAIN open calls, the TRUSTCHAIN Consortium aims to strictly follow the ethical principles related to the H2020 research and innovation actions evaluation:

Evaluation must be conducted with integrity and respect for the beliefs, manners and customs of the social and cultural environment, following human rights and gender equality.

Evaluators must respect the right of institutions and individuals to provide information in confidence, ensure that sensitive data are protected and cannot be traced to its source, and validate statements made in the report with those who provided them. Evaluators should obtain informed consent from those who provide private information of its use. When evidence of wrongdoing is uncovered, it must be reported discreetly to a competent body.

These principles have been embedded as much as possible in the evaluation process described above and is reflected by the statistics presented in section 4.

ANNEX 1 - EVALUATOR'S CONTRACT, DECLARATION OF HONOUR ON EXCLUSION CRITERIA AND DECLARATION OF ABSENCE OF CONFLICT OF INTEREST

CONTRACTING PARTIES

This contract ('the Contract') is between the following parties:

On the one part:

EUROPEAN DYNAMICS LUXEMBOURG SA (ED), established in RUE JEAN ENGLING 12, LUXEMBOURG 1466, Luxembourg, VAT number: LU17535424, represented for the purposes of signing the Agreement by Mr. Konstantinos Velentzas, legal representative of ED, hereinafter referred as the "Contractor".

On the other part:

[If you are a natural person]

[First Name] [Last Name], with Tax ID /VAT Number **[Tax ID or VAT NUMBER, please specify the one and provide also a legal proof of it (copy)]**, address **[Adress]**, with Passport Number/ID Number **[Passport Number/ID Number, please provide also a copy of your identity document],** hereinafter referred as the "Evaluator".

[If you are acting on behalf of a compagny]

[company name], address **[Adress]**, VAT Number **[VAT NUMBER and provide also a legal proof of it (copy)],** represented for the purposes of signing by**[First Name] [Last Name of the legal representative]**, legal representative of **[company name]**, hereinafter referred as the "Beneficiary"
And
[First Name] [Last Name] holder of the Passport Number/ID Number **[Passport Number/ID Number, please provide also a copy of your identity document],** valid until [Date], living at **[Adress],** hereinafter referred as the "Evaluator".

[Note that information that you provide above will have to be the same then when providing your invoice whether you are the direct beneficiary or acting on behalf of

The Contracting Parties have agreed to enter this Contract under the terms and conditions below.

By signing this Contract, the Evaluator confirms that she/he has read, understood and accepted the Contract and all its obligations and conditions, including the Code of Conduct set out in Annex 1 and the provisions set out in Annex 2, which form an integral part of this Contract.

The Contract is composed by the following documents:

Annex 1: Code of Conduct.

Annex 2: Declaration of honour on exclusion criteria and absence of conflict of interest.

GENERAL PROVISIONS

The European Commission (hereinafter referred as the "EC") and the Contractor, as a member of the consortium, have signed the Grant Agreement no 101093274 for the implementation of the project "TRUSTCHAIN - Fostering a Human-Centred, Trustworthy and Sustainable Internet" (Acronym: TRUSTCHAIN) within the framework of the European Union's Horizon 2020 Research and Innovation Programme.
The Contractor, following the selection procedure, has chosen the Evaluator to be part of the evaluation team of TRUSTCHAIN.

This Contract sets out the rights and obligations applying to the Evaluator and the Contractor for the purpose of evaluating the proposals submitted to TRUSTCHAIN under the Open Call 2– User Privacy and Data Governance in 2023.

ARTICLE 1 – ENTRY INTO FORCE OF THE CONTRACT AND TERMINATION

This Contract shall enter into force on the 25th of September, date of the webinar for evaluators. The termination of the Contract will be subject to the terms and conditions set out in Article 10.

ARTICLE 2 – TASKS OF THE EVALUATOR

The Evaluator must participate in the evaluation of the proposals submitted in response to Open Call 2 – User Privacy and Data Governance (2023).

The call was launched the 20th July 2023 (12:00 PM CET) with a closing date of 20th September 2023 (17:00 CEST). More information and the open call material can be found on: Apply – TrustChain (ngi.eu)

The evaluation will take place remotely, using tools provided by the TRUSTCHAIN consortium and the indicative schedule will be as follows:

Web briefing, 16:00 CET on the 25th September of 2023.

Individual evaluation, from the date of reception of the proposals to be evaluated till the 16th of October 2023.

(tentative) remote consensus evaluation between the pool of 2 evaluators per proposal from 16th of October 2022 to the 30th of October 2023.

In case of unexpected event and delays, the TRUSTCHAIN consortium reserves the right to slightly modify the aforementioned tentative schedule.

The web briefing will be recorded to share with experts not able to participate. The date and time of the remote consensus evaluation might change based on the availability of evaluators. A consensus meeting may be needed only in case the evaluators have shown significantly different opinions.

Based on the EC rules, the work in supporting TRUSTCHAIN will be reimbursed based on the number of proposals reviewed, with each proposal corresponding to a value of €50, considering 1 hour to evaluate each proposal.

ARTICLE 3 – PERFORMANCE OF THE CONTRACT

The Evaluator must perform the Contract within the set deadlines and in compliance with its provisions and all legal obligations under applicable EU, international and national law.

The Evaluator must ensure compliance with:

The Code of Conduct (see Annex 1).

The terms and conditions of this Contract do not constitute an employment agreement with the Contractor.

In the event an Evaluator cannot fulfil their obligations, s/he must immediately inform the Contractor.

ARTICLE 4 – KEEPING RECORDS AND SUPPORTING DOCUMENTATION

The Evaluator must keep records and other supporting documentation (original supporting documents) as evidence that the Contract is performed correctly, and the expenses were actually incurred. These must be available for review upon the Contractor's request. The Contractor and the EC are entitled to analyse the evidence to determine whether the Contract has been duly performed.

The Evaluator must keep all records and supporting documentation for five years starting from the date of the end of TRUSTCHAIN in case they are needed for on-going checks, audits, investigations, appeals, litigation or pursuit of claims.

ARTICLE 5 – PAYMENT

ARTICLE 5.1. PAYMENT

The payment amount that can be requested by an evaluator is based on the number of evaluated proposals. All the taxes and other costs related to the evaluation process go to the expenses of the evaluators. The request is sent to the Contractor using the dedicated TRUSTCHAIN Evaluator payment request.

ARTICLE 5.2. PAYMENT SCHEDULE

The payment to the total gross amount will be paid after receiving of the complete documentation for payment. Payments are subject to the Contractor's approval of report(s), and of the payment request(s).
Approval does not mean recognition of compliance, authenticity, completeness, or correctness of content.

ARTICLE 5.3. REQUEST FOR PAYMENT

The Evaluator must make a request for payment to obtain their fees.
To do this, the Evaluator shall issue the payment request using the template provided by the TRUSTCHAIN consortium.
The payment request shall be denominated in Euros (EUR) and the payments will be made by bank transfer 30 days from receipt of the payment request, provided that the payment requirements are met.
All the payment requests shall include:

Concept: [Beneficiary Name considering if your are acting on your own or on behalf of a compagny]

Recipient: EUROPEAN DYNAMICS Luxembourg SA
        12 Rue Jean Engling, 1466 Luxembourg
        LUXEMBOURG
        VAT: LU17535424

The Amount requested: [Nb. of proposals evaluated x evaluation fee 50€]

Tax Number/VAT number of the evaluator providing the service : [Number]

ID Number: [Number]

Name of the account holder to which the transfer is to be made: [Beneficiary name depending for who you are acting]

IBAN: [Number]

BIC/SWIFT : [Number]

Name of the Bank: [Name]

The Contracting authority can ask additional documentation if needed for the payment realization. In any case the information provided in this contract should correspond to the one provided when issuing the invoice. An invoice template will be sent to the evaluator to ease the process when services object of the contract are completed.

The evaluator agrees that if s/he does not get any proposal for evaluation, s/he will not have any financial claims towards the Contractor.

The Contractor accepts no responsibility for delays in payments incurred by failure of the Evaluator to provide any of the above information and payment request.

The Evaluator will be liable for all bank charges incurred due to incomplete information they might provide.

ARTICLE 6 – CONFIDENTIALITY

ARTICLE 6.1. PRINCIPLES

With respect to all information of whatever nature or form is disclosed to the Evaluator in the framework of the Contract and identified in writing as confidential, the terms of this Article shall apply.

ARTICLE 6.2. OBLIGATIONS

The Evaluator agrees that such information is communicated on a confidential basis and its disclosure may be prejudicial to the owner of the information, and understands that:

1. It will not, during the term of TRUSTCHAIN and for a period of five (5) years from the expiration date of the Contract; use any such information for any purpose other than in accordance with the terms of the Contract.

2. It will, during the term of the Contract and for a period of five (5) years from the expiration date of the Contract, treat the same as (and to procure that the same be kept) confidential, provided always that such agreement and undertaking shall not extend to any information which the Evaluator can show:

   o was, at the time of disclosure to the Evaluator, published or otherwise generally available to the public, or

- has, after disclosure to the Evaluator, been published or become generally available to the public otherwise than through any act or omission on the part of the Evaluator, or
- was already in the possession of the Evaluator, without any restrictions on disclosure, at the time of disclosure to the Evaluator, or
- was rightfully acquired from others without any undertaking of confidentiality; or
- is subsequently independently developed by the Evaluator without use of the information provided by the Contractor.

In case of breach of the confidential rules hereinabove set, the Evaluator will remain solely liable towards possible claims.

ARTICLE 7 – CHECK, AUDITS AND INVESTIGATIONS

The European Commission may, during the implementation of the action or afterwards, carry out checks and audits to ascertain compliance with the proper implementation of the tasks (including assessment of deliverables and reports) under this Contract and whether the Evaluator is meeting their obligations.

It may do so throughout the Contract's validity and up to five years starting from the date of the end of TRUSTCHAIN. The Evaluator must provide - within the deadline requested - any information and data in addition to reports already submitted. The Evaluator must allow access to sites and premises on which the tasks specified in this Contract are performed.

The EC has the right of access for the purpose of checks and audits.
Findings in checks, audits or investigations may lead to the reduction or rejection of fees, rejection of claims for allowances and expenses, or recovery of undue amounts. Moreover, findings arising from an OLAF investigation may lead to criminal prosecution under national law.

ARTICLE 8 – EFFECTS OF BREACHING CONTRACTUAL OBLIGATIONS

ARTICLE 8.1. SUSPENSION OF THE PAYMENT DEADLINE

1. The Contractor may at any point suspend the payment deadline if a request for payment cannot be processed because it does not comply with the Contract's provisions.
2. The Contractor must formally notify the Evaluator of the suspension and the reasons for it.
3. The suspension takes effect on the date the notification is sent by the Contractor.

4. If the condition for suspending the payment deadline as referred to above is no longer met, the suspension will be lifted - and the remaining period will resume.

5. If the suspension exceeds two months, the Evaluator may ask the Contractor if the suspension will continue.

6. If the payment deadline has been suspended due to the non-compliance of the reports (see Article 3) and the revised report or deliverables or payment request is not submitted or was submitted but is also rejected, the Contracting Party may also terminate the Contract (see Article 10).

ARTICLE 8.2. REDUCTION OR REJECTION OF FEES

1. The Contractor may reject (parts of) the fees if they do not fulfil the conditions set out in Article 4.

2. The Contractor may reduce the fee if the Evaluator is in breach of any of their other obligations under the Contract (including the obligations set out in the Code of Conduct).

3. The Contractor must formally notify the Evaluator of its intention, include the reasons why, and invite him/her to submit any observations within 30 days of receiving notification.

4. If the Contractor does not accept these observations, it will formally notify confirmation of the rejection or reduction.

ARTICLE 9 – SUSPENSION OF THE CONTRACT

1. The Contractor may suspend implementation of the Contract or any part of it, if the Evaluator is not able to fulfil their obligation to carry out the work required.

2. The Contractor must formally notify the Evaluator of its intention, include the reasons why and invite him/her to submit any observations within seven days of receiving notification.

3. If the Contractor does not accept these observations, it will formally notify confirmation of the suspension.

4. The suspension will take effect on the date the notification is sent by the Contractor.

5. If the reasons for suspending implementation of the Contract are no longer valid, the suspension may be lifted and implementation may be resumed. The Contractor will formally notify the Evaluator if the suspension is lifted and the Contract will be amended if necessary (see Article 13), unless it has been terminated (see Article 10).

ARTICLE 10 – TERMINATION OF THE CONTRACT

1. The Contractor may at any moment terminate the Contract if the Evaluator:

   o is not performing their tasks or is performing them poorly; or

- has committed substantial errors, irregularities, or fraud, or is in serious breach of their obligations under the selection procedure or under the Contract, including false declarations and obligations relating to the Code of Conduct.

2. The Contractor must formally notify the Evaluator of its intention, include the reasons why and invite him/her to submit any observations within 30 days of receiving notification. If the Contractor does not accept these observations, it will formally notify confirmation of the termination.

3. The termination will take effect on the date the notification is sent by the Contractor.

4. The Evaluator may at any moment terminate the Contract if s/he is not able to fulfil their obligations in carrying out the work required.

5. The Evaluator must formally notify the Contractor and include the reasons why by giving 15 days' notice.

6. The termination will take effect on the date the Contractor will formally notify confirmation of the termination.

7. Only fees for days worked before termination may be paid.

8. The Evaluator must submit the payment request for the tasks already executed on the date of termination within 30 days from the date of termination.

9. On termination of the Contract, the Contractor may hire another Evaluator to carry out or finish the work. It may claim from the Evaluator all extra costs incurred while doing this, without prejudice to any other rights or guarantees it may have under the Contract.

ARTICLE 11 – LIABILITY FOR DAMAGES

The Contractor cannot be held liable for any damage caused or sustained by the Evaluator during or because of performing the Contract, except in the event of the Contractor's wilful misconduct or gross negligence.

ARTICLE 12 – FORCE MAJEURE

1. 'Force majeure' means any situation or event that:

   - prevents either party from fulfilling their obligations under the Contract.

   - was unforeseeable, exceptional and beyond the parties' control.

   - was not due to error or negligence on their part or on the part of third parties involved in implementing the action, and

   - proves to be inevitable despite exercising due diligence.

2. A force majeure must be immediately and formally notified to the other Party. Notification must include details of the situation's nature, likely duration and expected effects.

3. The Party faced with a force majeure will not be held in breach of its contractual obligations if the force majeure has prevented it from fulfilling them.

ARTICLE 13 – AMENDMENTS TO THE CONTRACT

1. In justified cases - and provided that the amendment does not entail changes to the Contract which would call into question the selection procedure - any party may request an amendment.

2. Amendments must be made before new contractual obligations are enforced.

3. The party requesting an amendment must formally notify the other party the requested amendment in writing with the reasons why.

4. Any amendment to this Contract shall be done in writing and shall be duly signed by both Contracting parties.

ARTICLE 14 – APPLICABLE LAW AND DISPUTE OF SETTLEMENTS

This Contract shall be construed in accordance with and governed by the laws of Belgium.

Disputes concerning the Contract's interpretation, application or validity that cannot be settled amicably must be brought before the courts of Brussels.

The Contracting Parties have caused this Contract to be duly signed by the undersigned authorized representatives in three (3) copies the day and year first below written:

For : (the Beneficiary) If the beneficiary is a company, please insert here the business name, if you are acting on your own insert instead your name	EUROPEAN DYNAMICS Luxembourg SA
	Mr Konstantinos Velentzas,
	legal representative
Mr/Ms : ………………………………………….	**Signature:**
The beneficiary,	
Signature:	
	Done in Luxembourg **on DD/MM/YYYY**
Done in ………………………….. **on DD/MM/YYYY**	

<table>
<tr>
<td>

If the beneficiary is a company, please complete also hereafter :

The Evaluator:

Mr/Ms : ……………………………………

Independent expert,

Signature:

Done in ………………………… **on DD/MM/YYYY**

</td>
<td>

</td>
</tr>
</table>

CODE OF CONDUCT FOR EVALUATORS

ARTICLE 1 – PERFORMANCE OF THE CONTRACT

1. The Evaluator works independently, in a personal capacity and not on behalf of any organization.

2. The Evaluator must:

   o Evaluate each proposal in a confidential and fair way, in accordance with the TRUSTCHAIN Open Call 2 Guidelines for Applicants and the evaluation documents provided by the Contractor in each of the evaluation stages.

   o Assist the Contractor or relevant service to the best of their abilities, professional skills, knowledge and applying the highest ethical and moral standards.

   o Follow any instructions and time-schedules given by the Contractor or relevant service and deliver consistently high-quality work.

3. The Evaluator may not delegate another person to carry out the work or be replaced by any other person.

4. If a legal entity involved in a proposal approaches the Evaluator during the evaluation of this proposal, s/he must immediately inform the Contractor or relevant service.

ARTICLE 2 – OBLIGATIONS OF IMPARTIALITY

1. The Evaluator must perform their work impartially. To this end, the Evaluator is required to:

o Inform the Contractor of any conflicts of interest arising in the course of their work including of any proposal competing with the proposal where the Evaluator may have a conflict of interest.

o Confirm there is no conflict of interest for each proposal s/he is evaluating by signing a declaration of honour included in Annex 2.

Definition of the conflict of interest - For a given proposal, a conflict of interest exists if an Evaluator:

- Was involved in the preparation of the proposal.

- Stands to benefit directly or indirectly if the proposal is accepted.

- Has a close family or personal relationship with any person representing an applicant legal entity.

- Is a director, trustee or partner or is in any way involved in the management of an applicant legal entity.

- Is employed or contracted by one of the applicant legal entities or any named subcontractors.

- Is a member of any of the beneficiaries of the TRUSTCHAIN consortium.

In the following situations the Contractor will decide whether a conflict of interest exists, considering the objective circumstances, available information, and related risks when an Evaluator:

- Was employed by one of the applicant legal entities in the last three years.

- Is involved in a contract or grant agreement, grant decision or membership of management structures (e.g. member of management or advisory board, etc.) or research collaboration with an applicant legal entity or the fellow researcher, or had been so in the last three years.

- Is in any other situation that could cast doubt on their ability to participate in the evaluation of the proposal impartially, or that could reasonably appear to do so in the eyes of an external third party.

2. Consequences of conflicts of interest:

- If a conflict of interest is reported by the Evaluator or established by the Contractor, the Evaluator must not evaluate the proposal

concerned and shall immediately inform the Contractor about the situation.

- If a conflict becomes apparent at any stage of the evaluation, the Evaluator must immediately inform the Contractor. If a conflict is confirmed, the Evaluator must stop evaluating the proposal concerned. Any comments and scores already given by the Evaluator will be discounted. If necessary, the Evaluator will be replaced.

If it is revealed during an evaluation that an Evaluator has knowingly concealed a conflict of interest, the Evaluator will be immediately excluded, and sanctions will apply.

ARTICLE 3 – OBLIGATIONS OF CONFIDENTIALITY

1. The Contractor and the Evaluator must treat confidentially any information and documents, in any form (i.e. paper or electronic), disclosed in writing or orally in relation to the performance of the Contract.

2. The Evaluator undertakes to observe strict confidentiality in relation to their work. To this end, the Evaluator:

   o Must not use confidential information or documents for any purpose other than fulfilling their obligations under the Contract without prior written approval of the Contractor.

   o Must not disclose, directly or indirectly, confidential information or documents relating to proposals or applicants, without prior written approval of the Contractor.

In particular, the Evaluator:

   o Must not discuss any proposal with others, including other Evaluators, the Contractor or any other entity involved in any form on the Project, not directly involved in evaluating the proposal, except during the formal discussion at the meetings moderated by or with the knowledge and approval of the Contractor to this purpose.

   o Must not disclose:

   - Any detail of the evaluation process and its outcomes or of any proposal submitted for evaluation for any purpose other than fulfilling their obligations under the Contract without prior written approval of the Contractor.

   - Their advice to the Contractor or relevant service on any proposal to the applicants or to any other person (including colleagues, students, etc.).

   - The names of other Evaluators participating in the evaluation.

   o Must not communicate with applicants on any proposal during the evaluation.

3. The Evaluator will be held personally responsible for maintaining the confidentiality of any documents or electronic files sent, and for returning, erasing or destroying all confidential documents or files upon completing the evaluation as instructed.

    o   If the Evaluator seeks further information (for example through the internet, specialized databases, etc.) to complete their examination of the proposals, s/he:

    o   Must respect the overall rules for confidentiality for obtaining such information.

    o   Must not contact applicants.

    o   Must not contact third parties without prior written approval of the Contractor.

DECLARATION OF HONOUR ON EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST

The undersigned evaluator in his/her own name:

1. Declares that he/she is not in one of the following situations:

    o   Is bankrupt or being wound up, is having its affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, is the subject of proceedings concerning those matters, or is in any analogous situation arising from a similar procedure provided for in national legislation or regulations.

    o   He/she or persons having powers of representation, decision making or control over have been convicted of an offence concerning their professional conduct by a judgment which has the force of res judicata.

    o   Has been guilty of grave professional misconduct proven by any means which the contracting authority can justify including by decisions of the European Investment Bank and international organizations.

    o   Is not in compliance with its obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed.

    o   He/she or persons having powers of representation, decision making or control over have been the subject of a judgment which has the force of res judicata for fraud, corruption, involvement in a criminal organization or any other illegal activity, where such illegal activity is detrimental to the Union's financial interests.

2. Declares that the natural persons with power of representation, decision-making or control over the above-mentioned legal entity are not in the situations referred to in b) and e) above.

3. Declares that he/she:

   o Is not subject to a conflict of interest as per Article 2 of Annex 1 of the Contract for Evaluators (Code of Conduct for Evaluators).
   o Has not made false declarations in supplying the information required as a condition of being eligible as Evaluator for the assessment of the proposals received under TRUSTCHAIN open call 1 or does not fail to supply this information.
   o Is not in one of the situations of exclusion, referred to in the abovementioned point 1.

Full name of the evaluator: ·· Passport/ID number: ································ Done in ························, …/…/…………	Signature: XXX

ANNEX 2 - GUIDE FOR EVALUATOR

1   INTRODUCTION TO THE ROLE OF EVALUATOR

1.1   THE GUIDE FOR EVALUATOR

This guide aims at supporting the evaluation of expressions of interest submitted to the TRUSTCHAIN Open Call 2: User Privacy and Data Governance. It is intended to support independent External Evaluators and Internal Evaluators embodied in the TRUSTCHAIN Consortium to:

   o Assess on an individual and professional basis and against predefined evaluation criteria, the proposals received in response to the Open Call 2;

   o Draft Individual Evaluation Reports and Consensus Reports;

   o Contribute to establish the ranking list.

This guide contains information on the overall TRUSTCHAIN Innovation Action as well as more specifically on the TRUSTCHAIN Open Call 2.

A second section is dedicated to the evaluation process and especially to the workflow.

A third section outlines the eligibility criteria, the specific requirements for the objectives of OC2, as well as the specific evaluation criteria for this call.

Then, a fourth section is dedicated to the drafting and the quality of the Individual Evaluation Report and Consensus Report, the latter being sent to the applicants of each proposal.

Finally, a reminder regarding ethical principles related to Horizon Europe Research and Innovation activities is presented.

In Annex 1 of this document, you can find a checklist that will help you remember all the important aspects and rules of the evaluation of the TRUSTCHAIN action.

Please keep in mind that TRUSTCHAIN is an Horizon Europe Research and Innovation action and as such, proposals are not negotiated. This strongly limits the possibility of modifying a proposal after it has been selected for funding. It is therefore very important to evaluate them as they are, reflecting all the strengths and weaknesses in the scores.

1.2   THE EVALUATOR ROLE IN TRUSTCHAIN

The role of the Evaluator in TRUSTCHAIN is to investigate and justify the value of the received proposals according to the regulatory frame of the 5 Open Calls in particular according to the eligibility, requirement and evaluation criteria specific of TRUSTCHAIN.

Part of their contractual obligation is also to comply with the deadlines set by the TRUSTCHAIN consortium.

Evaluators should always keep in mind that significant funding decision will be made on the base of their assessment.

1.3   CODE OF CONDUCT

The Code of Conduct provisions here apply to all stages of the TRUSTCHAIN evaluation process from the conception to the completion of the evaluation and the release and use of the evaluation results. Any deficiency in conduct may undermine the integrity of the evaluation. TRUSTCHAIN Evaluators should thus be professional at all times of the evaluation process and respect the following principle:

o   Independence

Evaluators assess proposals on a personal basis;

Evaluators represent neither their employer, nor their country;

o   Competence

Evaluators shall accurately represent their level of skills and knowledge and should work only within the limits of their professional training and abilities in evaluation;

o **Impartiality**

Evaluators treat all proposals equally and evaluate them impartially on their merits, irrespective of their origin or the identity of the applicants;

o **Objectivity**

Evaluators assess each proposal as submitted not on its potential if certain changes were to be made;

o **Accuracy, Completeness and Reliability**

Evaluators make their judgment against the official evaluation criteria of the call that the proposal addresses, and nothing else;

Evaluators have the obligation to ensure that evaluation reports and presentations are accurate, complete and reliable. Evaluators shall explicitly justify judgements, findings and conclusions and demonstrate underlying rationale in order that stakeholders may assess them.

o **Consistency**

Evaluators apply the same standard of judgment to all proposals considering the specific implementation mode.

1.4   CONFLICT OF INTEREST AND CONFIDENTIALITY

1.4.1   Conflict of interest

A conflict of interest can be defined as a situation where the impartial and objective evaluation is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest.

The TRUSTCHAIN Consortium will take any action is necessary to avoid any conflict of interest with the proposals submitted to the TRUSTCHAIN calls.

Evaluators have a conflict of interest with a proposal if they:

o Were involved in the preparation of the proposal;
o Stand to benefit directly should the proposal be accepted;

o Have a close family or personal relationship with any person representing an applicant;

o Are a director, trustee or partner or are in any way involved in the management of an applicant;

o Are employed or contracted by one of the applicants or any named subcontractors.

Such Evaluator may, however, exceptionally be invited to take part in the evaluation session, if all of the following apply:

o The Evaluator works in a different department/laboratory /institute from where the action is to be carried out;

o the bodies operate with a high degree of autonomy; and

o Such a role is justified by the requirement to appoint the best available Evaluators and by the limited size of the pool of qualified Evaluators.

o Are acting as a referee of an applicant;

o Are in any other situation that may compromise impartiality, or might casts doubt, or reasonably appear to do so, on an Evaluator's impartiality.

In practice, all Evaluators will have to declare beforehand to the TRUSTCHAIN Consortium any known conflicts of interest or immediately inform it, should one become apparent during the evaluation.

1.4.2 Confidentiality

TRUSTCHAIN also requires Evaluators to maintain strict confidentiality with respect to the whole TRUSTCHAIN evaluation process. They must follow any instruction given by TRUSTCHAIN consortium and confidentiality rules must be adhered to at all times: before, during and after the evaluation. Under no circumstance may an Evaluator:

o Attempt to contact an applicant on his/her own account, either during the evaluation or afterwards

o Disclose any information on proposals/applicants

o Disclose any detail on the evaluation outcomes

o Disclose names of other Evaluators involved.

The Evaluators must return to the TRUSTCHAIN Consortium and/or erase any confidential documents once the TRUSTCHAIN evaluation exercise is over.

2 TRUSTCHAIN OPEN CALL 2 EVALUATION PROCESS

2.1 TRUSTCHAIN OPEN CALL 2 INDICATIVE TIMELINES

Remote Evaluation	Indicative Dates	Who
Evaluators Web Briefing	25th September 2023	TRUSTCHAIN Consortium + External Evaluators
The remote proposal evaluation takes place	From the 25th September 2023 to the 4th December 2023	TRUSTCHAIN Consortium + External Evaluators
100% Individual Evaluation Reports completed	16th October 2023	Internal Evaluators + External Evaluators
100% Consensus Reports completed	30th October 2023	Internal Evaluators + External Evaluators
Panel Review meeting and selection of applicants for the online interview	10th November 2023	TRUSTCHAIN Consortium
Online Interviews	From the 20th November to the 1st December 2023	Internal Evaluators + TRUSTCHAIN Advisory Board Members
TRUSTCHAIN Open Call 2 results publication	Week of the 11th December 2023	TRUSTCHAIN Consortium

All Evaluators should be available from 25th of September 2023 until the 10th of November 2023, date of the Panel review meeting for the selected projects.

2.2 TRUSTCHAIN CONTACT POINTS

The TRUSTCHAIN members involved in the evaluations and the contact points are the following:

Contact point	Name	Email
Call coordinator	Caroline Barelle	caroline.barelle@eurodyn.com
Technical Aspects	Vlado Stankovsky Raj. Muttukrishnan Iker Ruiz de Infante	vlado.stankovski@fri.uni-lj.si R.Muttukrishnan@city.ac.uk iker@alastria.io
Human Centric Aspects	Andres Delalamo	andres.delalamo@cibervoluntarios.org
Ethical Aspects	Ruben Roex	ruben.roex@timelex.eu
Business Aspects	Thanasis Papaioannou	thanasis.papaioannou@gmail.com

2.3 TRUSTCHAIN APPLICANT CLASSIFICATION

The target applicants of this call are developers, innovators, researchers, SMEs and entrepreneurs working on different NGI relevant topics and application domains at the intersection between the technical field (e.g Software Engineering, Network Security, Semantic Web, Cryptography, Blockchain, Digital Twin, Blockchain Security, Digital Identity, Blockchain Protocol), the Social sciences and Humanities (e.g Social Innovation, not-for-profit sector, Social Entrepreneurship, public goods) as well as any others including economics, environment, art, design, which can contribute to NGI TRUSTCHAIN relevant vision.

Applicants can apply as individuals in a Team of natural persons or linked to a legal entity. Hence, the participation is possible in several ways:

o **Team of natural persons:**

Team of individuals, all established in any eligible country. This does not consider the country of origin but the residence permit.

o **Legal entity(ies):**

One or more entities (consortium) established in an eligible country.

It can be Universities, research centres, NGOs, foundations, micro, small and medium-sized enterprises (see definition of SME according to the Commission Recommendation 2003/361/EC), large enterprises working on Internet or/and other related technologies are eligible.

o **Any combination of the above.**

In addition, the following condition apply:

o **The participating organisations should not have been declared bankrupt or have initiated bankruptcy procedures.**

o **The organisations or individuals (Team of natural persons) applying should not have convictions for fraudulent behaviour, other financial irregularities, and unethical or illegal business practices.**

2.4 TRUSTCHAIN FRAMEWORK

2.4.1 The TRUSTCHAIN Innovation Action in brief

The Internet has pushed our existence into the digital era, revolutionising our health, our wellbeing, our social life, our education and our information. Today we approach the Internet with our digital identities. There is a plethora of such digital identities that currently do not properly serve their purpose. Multiple threats related to truthfulness, trust and identity (ID) arise when people interact in this digital world: delusion and manipulation, personal privacy violation and personal data exploitation, unknown provenance of information, anonymity for performing criminal activities, spread of fake news using fake identities, skills mismatches, serious breaches of security are only a few of the threats that have emerged. The spirit of the first-generation Internet based on individual freedom, material progress, and moral community is slowly turning into individualism, materialism, and moralism, diverging from essential ethical and democratic principles that should underline this technology. The design choice of the past, based on a mix of centrally managed networking and device technologies makes today's Internet obsolete when it comes to empowering all citizens to act for a more environmentally friendlier digital transformation, as well as to create a more resilient, inclusive, and democratic society, addressing inequalities and human rights, better prepared for and responsive to threats and disasters.

For TRUSTCHAIN, the current emergence of Internet of Things (IoT), Decentralised Oracles, Artificial Intelligence (AI), Cloud-to-Edge (aka Fog) Computing, Distributed Ledger (DLT) and Digital Twin (DT) technologies created the need to build democratic systems without central points of control that can establish the missing link between universally agreed objectives in the physical world, and the digital representation of the reality, thus contributing to the realisation of trusted relationships in the Next Generation Internet. This can be achieved by using various consensus mechanisms that associate proofs with digital representations and thus help humans understand the objective truth, achieve trusted relationships on the digital world, allowing them to undertake well-informed decisions, in either a manual or automated manner. The ability to arrive at the objective truth by employing democratic governance mechanisms, consensus-based proofs, verification and certification can lead to a Next Generation Trusted Internet supporting humanity in all aspects of life. Today more than ever, challenges faced all over the world push for our society to reorganise itself to survive. The United Nations have called to reach 17 Sustainable Development Goals. Essentially, TRUSTCHAIN must be leveraged to embed in the Next Generation Internet principles of human-rights, sustainability, ethics and other human values that have been developed and maintained through long lasting centuries of human evolution.

The key concept of TRUSTCHAIN is to embed the key humanity principles in the co-creation of the Next Generation Internet and to provide autopoietic, evolutionary, decentralised and therefore democratic, transparent, traceable, and regulatory

compliant mechanisms that can support any ecosystem of entities and actors participating with their digital identities. The basis for this to happen is the use of decentralised digital identity architectures together with IoT, AI, Cloud-to-Edge, DLT and DT. Our intention is to embed in such solution's important societal goals in accordance with objective truth and therefore, trustworthiness.

TRUSTCHAIN - Fostering a Human-Centred, Trustworthy and Sustainable Internet is a European project funded by the European Commission under the European Union's Horizon Europe Research and Innovation Programme and the call topic CL4-2022-HUMAN-01-03. As such, it is part of the **European Commission's Next Generation Internet (NGI) initiative.** Its overall objective is to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised identity management software solutions that is transparent to the user, interoperable, privacy aware and regulatory compliant that can seamlessly integrate and interoperate with any of the existing decentralised applications. **TRUSTCHAIN was launched in January 2023 to address the inherent challenges within the current centralised Internet architecture that is not transparent to the user, does not protect the privacy-by -default and does not scale well through 5 Open Calls and an overall budget of 8,775 M€.**

The 5 Open Calls are the following:

○ **Open Call 1 - Decentralised digital identity**

The overall objective of Open Call 1 is to define and develop:

   ○ A framework for decentralised user-centric identity management;
   ○ Protocols for trustworthiness assessment of entities and their data by means of verifiable credentials and decentralized reputation systems;
   ○ Smart oracles assessing the trustworthiness of data.

This call is under implementation by 13 selected projects.

○ **Open Call 2- User privacy and data governance**

The objective of this OC will be 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 the GDPR and other regulations that implement techniques such as:

   ○ Multi-party data sharing mechanisms
   ○ Federated learning mechanisms considering both vertical and horizontal frameworks
   ○ Encrypted data analytics based on homomorphic encryption
   ○ Secure and privacy preserving data analytics mechanisms

> o Privacy-preserving usage of Artificial Intelligence, IoT, Digital Twins, Cloud-to-Edge services, or combination of those
>
> This is the focal point of this document.

o **Open Call 3- Economics and democracy**

The objective of OC3 will be to define and build mechanisms for smarter data exchange and data trading as well as innovative win-win federated business models' open data.

o **Open Call 4- Multi chains support for NGI protocols**

OC4 goal will be to design and build the gateways that will make it possible to transfer knowledge/metadata/data/process/requirements from one chain to another in a trustworthy and secure manner. Interoperability across multiple chains will be a cornerstone in this call.

o **Open Call 5- Green scalable and sustainable DLTs**

This call will build on top of all past OC1-4 calls. Its objective will be to employ digital identities, trustworthy data, and already designed novel mechanisms for the ecosystems' economy, in order to achieve high energy efficiency and optimisation of DLTs. We are looking for the most appropriate, relevant and pertinent trade-offs between the use of technologies, the security of consensus protocols on one side, and the sustainability and energy efficiency requirements on the other.

The overall structure of the open calls is summarized in the figure below. Note that each Open Call provides key technologies that can be used as basis for development in the subsequent calls, while also the opposite interaction can be employed by later calls, e.g., Open Call #2 can pose additional requirements for the final outcomes of Open Call #1 projects.
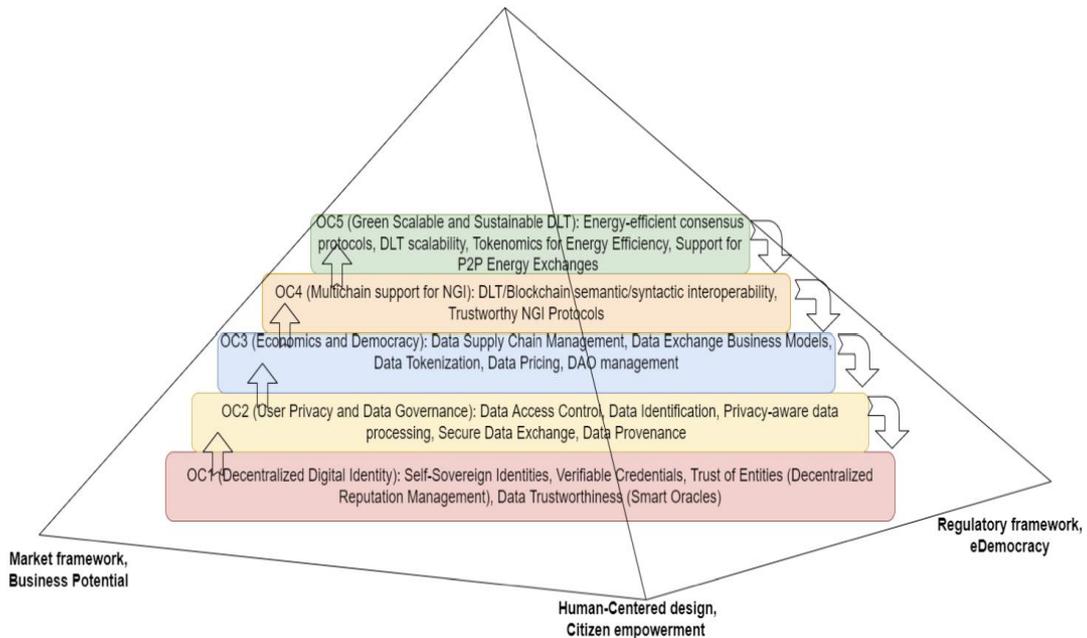
In this technological framework, TrustChain Open Call #2 is thus closely related to Open Call #3 "Economics and democracy" and Open Call #4 "Multi chains support for NGI protocols". Better solutions to user privacy and data governance will ensure better data economics and democracy and subsequently encourage ways for multi-chain interaction to exchange data/assets. Thus, knowledge created within this Open Call #2 will be transferred / integrated into future Open Call #3 and Open Call #4 calls.

Following the spirit of the HORIZON EUROPE Calls for the Next Generation Internet, the TRUSTCHAIN Research and Innovation Action encourages presentation of results as open-source software and open hardware designs, open access to data, standardisation activities, access to testing and operational infrastructures as well as an IPR regime ensuring interoperability, reusability of results, lasting and sustainable with a long-term societal impact.

This guide is specifically dedicated for the evaluation of the Open Call 2.

3 OPEN CALL 2: USER PRIVACY AND DATA GOVERNANCE

3.1 INTRODUCTION

It's indicative budget is 1.989.000 € and will be distributed among up to 17 selected projects led and executed by a critical number of developers, innovators, researchers, SMEs and entrepreneurs among others, actively involved in research, development and application activities in the fields of user privacy, data governance, blockchain, semantic web, ontology engineering, software engineering, Cloud engineering, digital twins, edge and fog computing, ecosystem economics, smart applications, cryptography, standardisation and security engineering.

Selected projects will last for a duration of 9 months. However, the TrustChain overall action lasts 36 months, and the selected projects are requested to participate after these 9 months in future Joint Meetings for knowledge and know-how transfer to TrustChain Open Call #3-5 and for the development of the TrustChain ecosystem.

As part of the TrustChain action, experts in diverse fields will also provide to Third party innovators selected technology development guidance, working methodology as well as access to technical infrastructure, training in business model development and data related topics, coaching, mentoring, visibility, and community building support.

Applicants are invited to submit their proposals on any topic that serves the overall TrustChain Open Call #2 vision and objectives. Their proposed solution should consider as minimal requirement to:

o Use standard technology for full stack development,

o Be open source,

o Extend the state-of-the-art in the domain of user privacy, and/or solve existing real-world problems with data governance and provide new highly usable software solutions.

Using the mandatory TrustChain proposal template, applicants are expected in relation to the specific objectives identified hereafter (section 3.2) to explain in their application:

o The specific technological innovation they propose to develop and how it is clearly different from alternative solutions that are already available in the market, or developed by previous EU research and innovation actions (i.e., the EU ONTOCHAIN Project and any other projects),

o The specific user privacy and data governance needs or challenge they propose to address and who would benefit from it immediately and in the longer term,

o Whether the innovation will focus on the development of new solutions for existing areas, or a totally disruptive approach or idea,

o Any work they have already done to respond to this need, for example if the project focuses on developing an existing capability or building a new one,

o Any challenges or opportunities relating to equality, diversity, ethics, and inclusion arising from their project,

o Explain how their proposed solutions will align with the building blocks developed as part of the Open Call #1 call on digital identity (more details are available on the TrustChain webpage).

Applicants when applying should clearly specify the Open Call #2 challenges they are going to address. Those are described in the section 3.3.

3.2   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, to give the control of their online data sharing back to the user and ensure privacy preserving ways of data exchange on the future internet is currently needed. 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:

o Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below,

o Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework,

o Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques,

o Encrypted data analytics based on homomorphic encryption and Trusted Execution environment,

o Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs,

o Protocols to support the digital sovereignty-based data flow and data spaces initiatives.

o 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.

3.3 CHALLENGES TO BE ADDRESSED

In the current Internet, all user data is owned and managed by a few 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:

o 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,

o Privacy is important when user data is employed for training machine learning models and computation. Information leakage in training models is a persistent problem. Local differential privacy with federated learning models can be explored to address this challenge,

o 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,

o Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol,

o Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed,

o 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, needs to be designed,

o In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users,

o 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,

o Data owners currently do not have means 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,

o 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:

o data privacy protection,

o privacy aware data processing,

o data provenance,

o data use policies,

o data retention and data deletion, right to be forgotten, data minimization, and trustworthiness,

o data minimization and user informed data deletion.

3.4 SPECIFIC REQUIREMENTS

3.4.1 Technical Requirement

In general, a user centric design and implementation, a co-created process with citizens as well as a use case driven approach will frame the proposed innovative solution development that should carefully consider the needs for security, privacy, human-rights, sustainability, and trustworthiness. Interoperability, scalability, greenness, openness, standards, as well as legal and regulatory compliance should be also considered, calculated, and assured.

The proposed solutions are intended to be co-created with end users focusing on online user privacy and data governance, adopting a user-friendly design. Therefore, they should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. The co-creation and validation approach should be clearly elaborated in the applicants' proposal. A citizen

digital vulnerable collectives' approach that puts in the centre the needs of the general population and vulnerable people, instead of technical/experts' users should be considered. It is intended that the solution is accessible for the general population as well as for the marginalized/vulnerable communities.

To this end, the applicant should show collaboration with an EU end-user organisation (i.e., banking, healthcare, education, policing etc.) as well as consider vulnerable groups for the evaluation /validation process if possible.

The focus should be on what is currently missing (e.g., trustworthy data access, ensuring clear and informed user content and expanding what already exists, thus scaling) rather than building something new from scratch. It is desirable that the selected projects be able to demonstrate their solution at TRL 7 in a real end-user setting. If something completely new must be built (see point above), then it should be well motivated why the nature of the problem warrants a new solution and why the state-of-the-art solutions do not solve it today (i.e., barriers to technology adoption).

The proposed solution should work within a specific business context and emphasis should be put on its scalability, on its energy efficiency and its minimum value proposition. Cross-border data sharing, moving data across EU-international borders should be carefully considered. It should be also compatible with existing data sharing frameworks, standards and demonstrate the energy efficiency through measurements that are quantifiable.

Finally, focus should also be put on demonstration of the technology. In particular, the applicant should demonstrate to have access to an infrastructure that is EVM compatible where it can be deployed and piloted.

Link with other Open Calls: This Open Call is closely related to Open Call #1 "Decentralized digital identity". Solutions to be developed in Open Call #2 should consider some of the approaches and outcomes identified in Open Call #1 for digital identity management. Joint activities between Open Call #1 and Open Call #2 innovators will be facilitated by the Trust Chain consortium.

3.4.2 Sustainability requirements

Various emerging technologies currently pose huge environmental impact. This negative impact should be assessed against the benefits from using these technologies. The applicants are requested to provide a short assessment of the trade-offs, considering from one viewpoint the benefits when using the technology, and from another, the potential energy-inefficiency. Various best effort solutions should be used as a baseline for providing such self-assessment.

3.4.3 Regulatory and standards requirements

Applicants are requested to present in a clear and concise manner any existing and/or emerging privacy-enhancing data sharing platform (i.e., GAIA-X & IDS, DECODE) / infrastructure standards with which they intend to comply with, or they wish to contribute to within the course of the proposed project. They should also identify how the project aligns with the Digital Services Act (DSA) and the Digital Market Act (DMA).

3.4.3 Regulatory and standards requirements

As mentioned above, the proposed solutions should be designed, implemented, piloted, and validated using a specific predefined and justified set of end users in an identified use case. The co-creation and validation approach should be clearly elaborated in the applicant's' proposal and the vulnerable collectives' approach should be used for the user testing.

A first step is to establish target groups of users. Once this is done, the users should be involved in the co-creation process. Then, accessibility standards should be incorporated through the onboarding according to the vulnerable collectives' approach.

Following that, a roadmap with the appropriate methodologies should be set up. The roadmap should include the approach, objectives and phases of the testing, and sample size. The sample needs to be representative and randomized but within the relevant characteristics of the target population.

User should be onboarded in the design process (if applicable). Proposals for improvement and insights should come from the users during the co-creation process. Complementarily, insights can be proposed by non-users (for example developers, or business partners). This decision must be justified in the corresponding deliverable.

3.5 EXPECTED OUTCOMES AND POSSIBLE APPLICATION DOMAINS

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

- o Privacy-preserving data oracles,
- o Privacy-preserving data processing techniques using technologies such as Homomorphic Encryption and Trusted Execution Environments,
- o Data anonymization and perturbation techniques,
- o Privacy-by-design microservice architectures,
- o General-purpose DLT-based solutions for privacy and data governance,

o Smart contracts for user privacy and data governance.

Possible use-cases and application domains include the following:

o Records of data processing activities (ROPAs) with verification and certification for GDPR-policy compliance,

o Data processing in Trusted Execution Environments,

o Consent management systems,

o Collaborative secure data sharing platforms,

o Privacy-preserving social networks,

o Privacy preserving machine learning models.

3.6   MANDATORY DELIVERABLES

Projects selected and funded by the TrustChain consortium will have to deliver four mandatory deliverables during their lifetime. The four deliverables are defined below:

o **D1:** State of the art overview, use case analysis and preliminary technical specification of the solution. The deliverable should clearly specify how the proposed solution extends and/or upgrades the state-of-the-art.

o **D2:** Detailed technical specification of the solution, software implementation work plan, demo scenarios, number of end users that will be involved in any pilots, and preliminary business plan.

o **D3:** Implementation, deployment, testing, demonstration, and validation roadmap in a real-life application (e.g., banking, education, healthcare, utilities, defence or cross-border travel) and result of the validation process.

o **D4:** Modularised software components ready for distribution, full documentation for developers/users, final business plan.

4   EVALUATION WORKFLOW

Proposals are submitted in a single stage and the evaluation process is composed of three stages as presented hereafter.

o **Stage 1:** Admissibility & eligibility check

o **Stage 2:** Proposals evaluation

o **Stage 3:** Online interviews and final selection
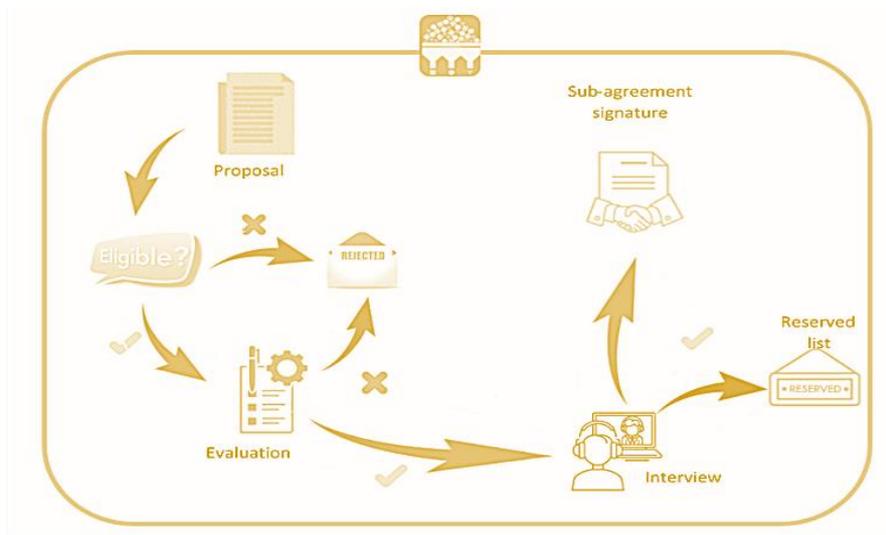
4.1   ADMISSIBILITY AND ELIGIBILITY CHECK

Admissibility and eligibility criteria for each proposal are checked by the TRUSTCHAIN Consortium staff. A proposal may be declared ineligible or inadmissible at any stage.

To be considered admissible, a proposal must be:

o Submitted in the electronic submission system before the call deadline.

o Compliant with the specific eligibility conditions set out in the relevant parts of this guide. The eligibility filter enables the creation of a shortlist of proposals to be evaluated.

o Readable, accessible and printable.

o Complete and include the requested administrative data, and any obligatory supporting documents specified in the call e.g. following the TRUSTCHAIN template.

o Include the research proposal description. **Applicants must strictly follow the template, instructions as well as pages limitation for drafting the research proposal.** A proposal will only be considered eligible if its content corresponds specifically to the objective of the TRUSTCHAIN Open Call 2 or is proposed as "open topic" and demonstrates that it aims to advance the state of the art especially with regards to the TRUSTCHAIN Open Call 2 Framework and application domain.

4.2   PROPOSAL EVALUATION

The evaluation of proposals is carried out by the TrustChain Consortium with the assistance of independent experts. TrustChain Consortium ensures that the process is fair and in line with the principles contained in the European Commission's rules on Proposal submission and evaluation. To facilitate the independent experts and the evaluation process, the EasyChair platform (https://easychair.org/) will be used.

Experts perform evaluations on a personal basis, not as representatives of their employer, their country or any other entity. They are required to be independent, impartial, and objective, and to behave throughout the process in a professional manner. The experts sign an expert contract, including a declaration of confidentiality and absence of conflict of interest, before beginning their work.

All experts must declare beforehand any known conflicts of interest and must immediately inform the TrustChain Consortium if they detect a conflict of interest during the evaluation. The expert contract also requires experts to maintain strict confidentiality with respect to the whole evaluation process. They must follow all instructions given by the TrustChain Consortium to ensure this. Under no circumstance may an expert attempt to contact an applicant on his/her own account, during the evaluation process. Confidentiality rules must be always adhered to before, during, and after the evaluation.

Each proposal is evaluated by a set of 2 experts (one from the TrustChain Consortium and one independent) according to the following criteria:

1-Excellence and innovation (40% weighting)
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context and credibility of the proposed methodology including the User Centric Approach
- Extend that the proposed work is beyond the state of the art, and demonstrates innovation potential in relation to TRUSTCHAIN objective (e.g. ground-breaking objectives, novel concepts and approaches, new products, services or business and organisational models)
- Evaluate the degree to which the human centric methodology is clearly described and sound.
- Evaluate the appropriateness and soundness of the technical approach.

2-Expected impact and value for money (30% weighting)
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised identity management software solutions that is transparent to the user, interoperable, privacy aware and regulatory compliant.
- Impact of the innovation on the needs of European and global markets is clearly provided and relevant KPIs are available.
- Quality of the proposed measures to exploit and disseminate the project results (including management of IPR), and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.

3-Project Implementation (30% weighting)
- Quality and effectiveness of the work plan, including extend to which the resources assigned to the work are in line with its objective and deliverables and milestones.
- Required mandatory deliverables are provided.
- Quality and effectiveness of the management procedures including risks and mitigation management.
- Integration of the solution to the overall TRUSTCHAIN ecosystem.
- Team is properly established and includes the key expertise to achieve the objectives.

Experts will score each award criterion on a scale from 0 to 5 (half point scores may be given):

0=**Proposal** fails to address the criterion or cannot be assessed due to missing or incomplete information.

1=**Poor**, criterion are inadequately addressed or there are serious inherent weaknesses

2=**Fair**, proposal broadly addresses the criterion but there are significant weaknesses.

3=**Good**, proposal addresses the criterion well, but a number of shortcomings is present.

4=**Very good**, proposal addresses the criterion very well but a small number of shortcomings is present.

5=**Excellent**, the proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

For each criterion, the minimum threshold is 3 out of 5 points. The default overall threshold, applying to the sum of the three criteria scores with the corresponding weight each, is 10.

Each expert prepares an individual evaluation report.

Following the individual evaluations by the two experts, a consensus meeting, typically mediated by the evaluation tool is organised between the two experts to achieve a consensus between them on the quality of the proposal based on the two evaluation reports. Comments and scores are validated by the two experts in a consolidated evaluation report.

When necessary, an additional review of projects for which there was a lack of consensus in terms of scoring by the two experts or for which additional clarifications are required is undertaken by the TrustChain Call Referent (member of the TrustChain Consortium). In this case, an additional independent evaluator is appointed to review the proposal. The final score is obtained based on the consensus of the 3 evaluators, one internal and 2 externals to the consortium.

The TrustChain Consortium then formally approves the ranking list.

The admission to the online interview for applications follows this rule: **the 20 highest-ranked proposals are admitted to the online interview.** The TrustChain Consortium may decide to invite more proposals to be part of the online interview stage in case for example of ex-aequo.

In any case, all proposals admitted to the online interview must reach all score thresholds.

Regarding the communication of the results, each applicant will receive via e-mail a letter informing them of the decision, which can be either a rejection decision supported by an Evaluation Summary Report or an invitation to the online interview session.

4.3 ONLINE INTERVIEW AND FINAL SELECTION

According to the rules, the top projects at the end of the proposal evaluation stage will be invited to the final selection stage. The applicants invited to the online interview will receive via e-mail, an invitation letter the online interview as well as relevant guidelines. **It is worth mentioning here that an invitation to the interview is not a formal invitation for funding.** The interview aims to better understand the project concept, scope, and centrality to the TrustChain vision, the team skills and competencies, capacity, and willingness to exploit the results under a commonly agreed plan with the rest of the TrustChain ecosystem and TrustChain partners. Most importantly, the online interview aims to clarify still unclear aspects of the proposal which have been identified during the proposal evaluation. The proposal evaluation report is not circulated to the applicants before the interview but forms the basis for the interaction with them.

In practice, the interview will be carried out by the evaluation board composed of the TrustChain core partners and the TrustChain advisory board members. It will be recorded to assure maximum transparency. It is based on 10 minutes pitch presentation and 20 minutes of Q&As to clarify some aspects regarding the quality of the proposal and its relevance for TrustChain, as well as to reach a final agreement about scores and the Evaluation Summary Report (ESR). The comments on the ESR are taken into consideration for the preparation of relevant questions during the online interview and they are not communicated beforehand to the applicants.

The ESR will be structured according to the 3 criteria mentioned in the previous section (i.e., excellence and innovation, expected impact and value for money, project implementation) and will consolidate the comment of the proposal evaluation and the clarifications and overall impression obtained during the online interview. Based on the final consolidate score, the short list of winners will be produced and only at this stage the final ESR will be communicated to the applicants.

Remaining proposals will be maintained on a reserve list and potentially be later admitted in case of withdrawal or failure of one of the projects initially admitted to successfully complete any phase of the contract signing process.

The list of selected projects is then submitted to the European Commission for final screening and validation.

<u>The indicatives timelines of each phases are provided in section 2.1 of this guide for evaluators.</u>

5   ELIGIBILITY AND REQUIREMENT

Proposals need to comply both with the eligibility criteria and with all mandatory elements which are specific of the implementation mode of the Open Call 2 specific objectives and related topics. Additionally, aspects relative to page limits may impact on the evaluation and are described below. Annex 1 of this guide provides a checklist which summarise all rules and specific issues to take into account when evaluating a TRUSTCHAIN proposals.

5.1   ELIGIBLE COUNTRIES

Only applicants legally established/resident in any of the following countries (hereafter collectively identified as the "Eligible Countries") are eligible:

o The Member States (MS) of the European Union (EU), including their outermost regions.

o The Overseas Countries and Territories (OCT) linked to the Member States3;

o Horizon Europe associated countries, as described in the Reference Documents and the List of Participating Countries in Horizon Europe according to the latest list published by the European Commission.

5.2   LANGUAGE

English is the official language for TRUSTCHAIN open calls. Submissions done in any other language will be disregarded and not evaluated.

English is also the only official language during the whole execution of the TRUSTCHAIN programme. This means any requested submission of deliverables must be done in English in order to be eligible.

5.3   PROPOSAL SUBMISSION

Proposals must be submitted electronically, using the TRUSTCHAIN Online Submission Service accessible via https://www.f6s.com/trustchain-open-call-2. Proposals submitted by any other means, will not be evaluated.

Only the documentation included in the application will be considered by evaluators. It will be composed by a form with administrative questions to be completed directly

---

3 Entities from Overseas Countries and Territories (OCT) are eligible for funding under the same conditions as entities from the Member States to which the OCT in question is linked

in the platform and the proposal description attached in PDF format. To be eligible, Applicants must strictly follow the proposal template provided in the annexes as well as the page limitation.

The information provided should be actual, true and complete and should allow the assessment of the proposal.

The preparation and submission of the proposal and other actions that follow this procedure (such as withdrawal) fall under the final responsibility of the Applicant.

5.3.1 Multiple submissions

Given the fact that this call is a competitive one, and one Applicant should focus on only one specific topic the following apply:

- o Only one proposal per **Applicant** should be submitted to this call, and only one proposal per **Applicant** will be evaluated. In the event of multiple submissions by an applicant, only the last one received (timestamp of the system) will enter the evaluation process. Any other submitted proposals by the same Applicant or involving the same Applicant will be declared non-eligible and will not be evaluated in any case.

- o Only one proposal per **Individual** should be submitted to this call whether he/she applies within as a Team of natural persons or as part as part of a consortium member. If an individual is taking part in several teams/consortiums, the members of the other teams/consortium will be informed about the participation of an individual in multiple teams/consortiums. Then, only the last proposal received (timestamp of the system) including the individual will enter the evaluation process. Any other submitted proposals involving this Individual will be declared non-eligible and will not be evaluated in any case.

Note that the regular functioning of the F6S platform limits to one application submission per F6S user in each call. If an F6S user wishes to submit more than one application, **for example on behalf of different Applicants**, the F6S user should request support from the F6S support team (support@f6s.com) at least 10 days prior to the open call deadline.

5.3.2 Participation to the 5 TRUSTCHAIN Calls and funding rules

TRUSTCHAIN is an opportunity to fund truly multidisciplinary projects involving partners from different (natural and humanistic) disciplines relevant to Internet development. Thus, applicants can apply, participate and benefit from the 5 TRUSTCHAIN open Calls but as the main objective of the action is to support large number of third parties through open calls, the maximum amount to be granted to each third party is EUR 200 000 to allow cases were a given legal entity (e.g. large

research, academic or industrial organisations) may receive several grants (e.g. from different calls).

5.4   SECIFIC REQUIREMENTS

In order to guarantee equal treatment among the proposals, the Applicants are required to respect page limits. The Evaluators are asked to disregard any information contained in the excess pages. Should an Evaluator identify an issue regarding the page limits, they are asked to immediately contact their topic coordinator.

6   EVALUATION REPORTS

6.1   INDIVIDUAL EVALUATION REPORT

The quality of the Individual Evaluation Report is paramount as it constitutes the basis of the Consensus Report which is sent to the Applicant. It should therefore give a clear assessment of the proposal based on its merit, provide clear feedback on the proposal's weaknesses and strengths with comments which are consistent with the scores. High quality reports are crucial to the success of the consensus phase.

Before starting drafting their Individual Evaluation Report, Evaluators are recommended to know what is expected from the Applicant thus to check the scope of the TRUSTCHAIN Open Call 2, the description of the specific objectives. The challenge, the requirements, the context as well as the expected outcomes to be considered by the Applicant are presented in section 3 of this guide.

The Evaluators must also be aware of how the proposal should be structured. There is 2 distinct parts:

o   The administrative part including any obligatory supporting documents specified in the call and the ethics issues table (see annex 2).

o   The research proposal description according to the TRUSTCHAIN template and instructions set in the TRUSTCHAIN guide for applicant (see annex 3).

The research proposal description is the most important part to be considered by the Evaluator. It should contain a maximum 10 pages and the following sections:

o   **The first page** with the proposal acronym, full title, and the topic(s) selected.

o   **The proposal** with:

Page count starts here

4.   Project summary (300 words)
5.   Applicant background (Max. 1 pages)

6. **Proposal description (Max. 8 pages)**
   - 6.1 Concept and objectives (Max. 1 page)
   - 6.2 Proposal solution (Max. 2 pages)
   - 6.3 Expected impact (Max. 2 pages)
   - 6.4 Business model and sustainability (Max. 1 page)
   - 6.5 Implementation (Max. 2 pages)

   Page count finishes here

It will be assessed against the evaluation criteria set in section 4.2.

Evaluators are strongly advised to refer to the evaluation grid set in annex 1 to draft their IER.

Practically, evaluators should provide comments for each criterion/sub- criterion and list them under a strengths paragraph and a weaknesses paragraph. The assessment must be factual and not an outcome of personal interpretation. All shortcomings should be clearly justified by providing concrete examples related to the proposal. No recommendations should be made.

When comments are set, Evaluators can proceed to scoring each criterion based on the scoring scale provided in section 4.2. The scores must reflect the comments.

6.2 CONSENSUS REPORT

High quality consensus reports are crucial to the success of the overall evaluation and the quality of the TRUSTCHAIN project outcomes. It should demonstrate a consensus of the two evaluators on the quality of the proposal and provide a clear assessment of the proposal based on its merit with clear feedback on weaknesses and strengths.

Practically within the pool of two evaluators per proposal, a rapporteur (from the TRUSTCHAIN staff) will be assigned the task of drafting the consensus report based on the 2 Individual Evaluation Reports.

First the rapporteur aggregates the comments of the 2 Individual Evaluation Reports for each criterion under a strengths paragraph and weaknesses paragraph. When there is disagreement on the quality of some sub criterion, the rapporteur lists the related comments under a paragraph titled "to be discussed". This phase leads to the draft Consensus Report that will be discussed among the 2 evaluators in particular the paragraph "to be discussed" so that to find a consensus.

When a consensus is found, the rapporteur proposed scores for each of the 3 criteria to be discussed. When consensus is obtained both on comments and scores then the consensus report is ready for the ranking phase and later on to be sent to the applicant

to motivate the rejection of their proposal. Selected applicant for the online interview receive solely an invitation to the interview.

6.3   THE EVALUATION SUMMARY REPORT

The evaluation summary report is the base document for the funding decision to be made. It is composed of the consensus report related to the proposal and the evaluation summary of the online interview. It includes the decision of the evaluation board (TRUSTCHAIN topics referents and the TRUSTCHAIN advisory board members) whether to distribute funding for selected projects or to register the proposal on the reserve list.

The evaluation summary of the online interview is the outcome of a qualitative evaluation according to the evaluation criteria set in section 2.6.3 and in particular to the credibility of the proposed project outcomes, the value for money, the collaborative Spirit/Commitment of the applicant, and the business compatibility. The score for the interview will be the average of the scores of the 4 criteria.

Based on these final scores, two short lists of winners will be produced.

When this phase done, the evaluation summary report is ready to be sent to the applicant to motivate the evaluation board final decision.

7   ETHICAL PRINCIPLES RELATED TO HORIZON EUROPE RESEARCH AND INNOVATION ACTIONS EVALUATION

Evaluation must be conducted with integrity and respect for the beliefs, manners and customs of the social and cultural environment; human rights and gender equality; and do no harm principles for humanitarian assistance. Evaluators must respect the right of institutions and individuals to provide information in confidence, ensure that sensitive data are protected and cannot be traced to its source, and validate statements made in the report with those who provided them. Evaluators should obtain informed consent from those who provide private information of its use. When evidence of wrongdoing is uncovered, it must be reported discreetly to a competent body.

ANNEX 1- TRUSTCHAIN ELLIGIBILITY CHECK LIST, GRID FOR EVALUATION AND REPORT FORMS

CHECK LIST FOR ELIGIBILITY ASSESSMENT

o GENERAL INSTRUCTIONS ON THE TEMPLATE

This template is to be used for the TRUSTCHAIN Call 3 evaluation procedure by the TRUSTCHAIN team to perform the first check of admissibility and eligibility of the submitted proposals.

It has been designed to ensure a systematic and effective assessment of admissibility and eligibility of the proposals before their distribution to the evaluators. The assessor must both control the administrative form as well as the number of pages of the proposal to fill in the template.

A proposal will only be considered eligible if all the "yes" boxes are ticked.

Note that a proposal can be declared ineligible at any stage of the evaluation process. If there is any doubt on the eligibility of a proposal after the aforementioned first check, the Evaluator should report the case to the specific topic coordinator (see section 2.2).

o ELIGIBILITY ASSESSMENT TEMPLATE

TRUSTCHAIN Open call 2- Assessment grid	Proposal Acronym :	Elligibility	
		yes	**no**
Type of applicant			
A single organisation (Legal entity)			
Secondary or Higher education establishment			
Research organisation			
SME			
Large enterprise			
Public Body			
A non-for profit organisation, association, NGO			
Foundation			
International organisation			
Other?			
VAT number			
Contact mail			
A group of individuals (Team)			
ID information of all the individuals			
Team leader contact mail			

A group of organisations (Consortium)		
Secondary or Higher education establishment		
Research organisation		
SME		
Large enterprise		
Public Body		
A non-for profit organisation, association, NGO		
Foundation		
International organisation		
Other?		
VAT number of the Coordinator		
Contact mail of the Coordinator		
Country		
Member States (MS) of the European Union (EU), including their outermost regions		
The Overseas Countries and Territories (OCT) linked to the Member States		
HORIZON associated countries		
UK applicants		
Language		
English		
Proposal submission		
Electronically via the F6S portal		
Multiple submission		
Latest version on the F6S portal		
Proposal description		
Respect of the page limit		
Acceptance of the TRUSTCHAIN Open Call Terms & Conditions		
Authorisation to apply in the name of		
Conflict of interest avoidance with TRUSTCHAIN consortium		
Fraudulent behaviour avoidance		
Bankruptcy information		
European Commission Regulation No 651/2014, art. 2.18		
Originality and freedom to operate		
Applicant(s) eligibility		

GRID FOR EVALUATION

o   GENERAL INSTRUCTIONS ON THE TEMPLATE

The quality of the Individual Evaluation Report is paramount as it constitutes the basis of the Consensus Report which is sent to the Applicant.

This template is to be used for the TRUSTCHAIN Call 3 evaluation procedure by the Evaluators to draft their Evaluation Reports.

It has been designed to help Evaluators assessed the proposals allocated to them in a structure way. Using this grid will ensure that all aspects required under the three criteria are addressed in the evaluation reports (both the Individual Evaluation Reports and the Consensus Report). Moreover, during the consensus report phase it will help the Evaluators in having a structured discussion on the comments to be included in the Consensus Report and in setting appropriate score that reflect the comments.

The Assessment Grid includes a number of questions under each sub-criterion. For each question, the Evaluator should follow the actions described below:

- o   Check if the specific aspect described by the question is present in the proposal
- o   Assess how that particular aspect is addressed in the Proposal by using the following indicators: "Fail", "Poor", "Fair", "Good", "Very Good", "Excellent".
- o   In parallel, the Evaluator should provide their comments in the evaluation report template (see next template) for each sub criterion and under two sections: "strengths" and "weaknesses" (see next template). When drafting the text, the Evaluator should make sure that the comments and the qualitative assessment indicated in the assessment grid are coherent, by using appropriate synonyms.

o   EVALUATION GRID

TRUSTCHAIN Open call 2- Assessment grid	Proposal Acronym :	Assessment					
		Fail	Poor	Fair	Good	Very good	Excellent
Criterion 1: Excellence and innovation (40% weighting)							
Quality and credibility of the research/innovation project, level of novelty							
1.1 Is the proposed concept clear, pertinent, and sound according to the TRUSTCHAIN topic that should be addressed?							
1.2 Is the proposed technical approach credible including the User-centric approach							
1.3 Is the proposed research beyond the state of the art?							

1.4 Is the innovation potential (e.g ground-breaking objectives, novel concepts and approaches, new products, services or bussiness and organizational models) appropriately demonstrated?	

Criterion 2: Expected impact and value for money (30% weighting)	
Contribution to Trustchain overall goal to create a portfolio of Next Generation Internet protocols and ecosystem of decentralized identity management software solutions that is transparent, interoperable, privacy aware and regulatory compliant	
2.1 Will the planned research contribute to Trustchain overall goal?	
2.2 Will the proposed solution contribute to an ecosystem of decentralized identity management solutions that can seamlessly integrate and interoperate with any of the existing decentralised applications?	
2.3 Is the proposed solution transparent to the users, interoperable, privacy aware and regulatory compliant?	
2.4 Does the proposed solution answers to a real need of the targeted end users?	
Impact of innovation on needs of European and global markets	
2.5 Will the planned research have an impact on the needs of European and Global markets?	
Quality of proposed measure to exploit an disseminate the project results	
2.6 Is the strategy to disseminate and exploit the new knowledge generated by action appropriate?	
2.7 Is the strategy for targeting peers (scientific, industry and other actors, professional organization and policy makers) and the wider community (potential end users) clear, consistent and appropriate?	
2.8 Where applicable, does the proposal describes a potential business strategy/ commercialization plan and how IP property is expected to be dealt within the frame of Trustchain?	
2.9 Where applicable does the proposal describe how research/sensitive data will be managed in the context of Trustchain?	

Criterion 3: Project Implementation (30% weighting)	
Quality and effectiveness of the work plan	
3.1 Is the work plan well structured and appropriate to ensure that the research objectives and requested deliverables are achieved?	
3.2 Are the tasks and activities sufficiently detailed?	
3.3 Are the planned mobilised resources appropriate in relation to the proposed activity?	
Quality and effectiveness of the management procedures including risk and mitigation management	
3.3 Is there appropriate management structure and related procedures?	
3.4 Does the plan ensure quality and effective risk and mitigation management techniques?	
Integration capacity in the Trustchain ecosystem	

3.5 Is there a plan to integrate the work to the overall Trustchain ecosystem? Is the plan appropriately defined and convincing?	
Team excellence and availability	
3.6 Is the experience of the applicant on the research topic well described and adequate to achieve the reaserch goals?	
3.7 When relevant, is the nature of the reaserch team well outlined and adequate to achieve the research goals?	
3.8 Has the applicant demonstrated the capacity to achieve the research goals?	

EVALUATION REPORT TEMPLATE

o GENERAL INSTRUCTIONS ON THE TEMPLATE

High quality evaluation reports are crucial to the success of the overall evaluation and the quality of the TRUSTCHAIN project outcomes. In particular the quality of the Individual Evaluation Report is paramount as it constitutes the basis of the Consensus Report which is sent to the Applicant. This template is to be used for the TRUSTCHAIN Call 3 evaluation procedure by

- o The Evaluators to draft their Individual Evaluation Reports.
- o The Rapporteur that has been assigned the task of drafting the Consensus report based on the 2 Individual Evaluation Reports.

For the Individual Evaluation Report, the Evaluators should provide their comments in the template based on the qualitative assessment done thanks to the assessment grid (see previous template) and that, for each sub criterion according if it is a "strengths" or "weaknesses". When drafting the text, the Evaluator should make sure that the comments and the qualitative assessment indicated in the assessment grid are coherent, by using appropriate synonyms.

When the comments are set, the evaluators can proceed to the scoring of the 3 criteria according to the scoring scale provided in section 2.6.3.

Finally, when asked to do so, the Individual Evaluation Report of the external evaluator is communicated to the Rapporteur.

At the level of the Consensus Report, the designated rapporteur aggregates the comments of the 2 Individual Evaluation Reports for each criterion in a new evaluation report template that will become the Consensus Report. When there is agreement on the quality of some sub criterion, the rapporteur consolidate the comments directly under the strength or weakness paragraphs. In the case of a disagreement on the quality of some sub criterion, the rapporteur lists the related comments under a paragraph titled "to be discussed". This leads to the draft Consensus Report that will be discussed among the 2 evaluators in particular the paragraph "to be discussed" so that to find a consensus.

When a consensus is found, the rapporteur proposed scores for each of the 3 criteria. When consensus is obtained both on comments and scores then the consensus report is ready for the ranking phase and later on to be sent to the applicant to motivate the rejection or the selection for funding.

o EVALUATION REPORT TEMPLATE

CRITERION 1: Excellence and innovation (40% weighting)
C1.1 Quality and credibility of the research/innovation project, level of novelty

C1.1.1 Is the proposed concept clear, pertinent, and sound according to the TRUSTCHAIN topic that should be addressed?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C1.1.2 Is the proposed technical approach credible including the User-centric approach?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C1.1.3 Is the proposed research beyond the state of the art?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C1.1.4 Is the innovation potential (e.g ground-breaking objectives, novel concepts and approaches, new products, services or bussiness and organizational models) appropriately demonstrated?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

-

CRITERION 1- COMMENTS & SCORE. * Structure your text in two parts e.g. Strengths and Weaknesses Enumerate strengths and weaknesses by writing high quality comments.

○ 10: Excellent. The proposal is outstanding and successfully addresses all relevant aspects of the criterion.

○ 9: Almost Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are very minor.

○ 8: Very good. The proposal addresses the criterion very well, but a small number of minor shortcomings are present.

○ 7: Good. The proposal addresses the criterion well and any shortcomings present are not serious.

○ 6: Satisfactory. The proposal addresses the criterion in a satisfactory way, but a small number of shortcomings are present.

○ 5: Almost Sufficient. The proposal almost addresses all relevant aspects of the criterion, but shortcomings are present.

○ 4: Insufficient. The proposal addresses the criterion, but not in a sufficient way and/or serious weaknesses are present.

○ 3: Low. The proposal addresses the criterion overall, but not in a sufficient way and a number of serious weaknesses are present.

○ 2: Poor. The criterion is poorly addressed, and/or there are major inherent weaknesses.

○ 1: Minimal. The criterion is minimally addressed and there are major weaknesses.

○ 0: Bad. The proposal is of very low quality.

CRITERION 2: Expected impact and value for money (30% weighting)

C2.1 Contribution to Trustchain overall goal to create a portfolio of Next Generation Internet protocols and ecosystem of decentralized identity management software solutions that is transparent, interoperable, privacy aware and regulatory compliant

C2.1.1 Will the planned research contribute to Trustchain overall goal?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.1.2 Will the proposed solution contribute to an ecosystem of decentralized identity management solutions that can seamlessly integrate and interoperate with any of the existing decentralised applications?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.1.3 Is the proposed solution transparent to the users, interoperable, privacy aware and regulatory compliant?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.1.4 Does the proposed solution answers to a real need of the targeted end users?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.2 Impact of innovation on needs of European and global markets

C2.2.1 Will the planned research have an impact on the needs of European and Global markets?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.2.2 Are there achievable KPIs in place?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.3 Quality of proposed measure to exploit an disseminate the project results

C2.3.1 Is the strategy to disseminate and exploit the new knowledge generated by action appropriate?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.3.2 Is the strategy for targeting peers (scientific, industry and other actors, professional organization and policy makers) and the wider community (potential end users) clear, consistent and appropriate?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.3.3 Where applicable, does the proposal describes a potential business strategy/ commercialization plan and how IP property is expected to be dealt within the frame of Trustchain?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

C2.3.4 Where applicable does the proposal describe how research/sensitive data will be managed in the context of Trustchain?. Tick the box only if the proposal addresses WELL the requirement.

☐ Y

-

CRITERION 2- COMMENTS & SCORE. * Structure your text in two parts e.g. Strengths and Weaknesses Enumerate strengths and weaknesses by writing high quality comments.

○ 10: Excellent. The proposal is outstanding and successfully addresses all relevant aspects of the criterion.

○ 9: Almost Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are very minor.

○ 8: Very good. The proposal addresses the criterion very well, but a small number of minor shortcomings are present.

○ 7: Good. The proposal addresses the criterion well and any shortcomings present are not serious.

○ 6: Satisfactory. The proposal addresses the criterion in a satisfactory way, but a small number of shortcomings are present.

○ 5: Almost Sufficient. The proposal almost addresses all relevant aspects of the criterion, but shortcomings are present.

○ 4: Insufficient. The proposal addresses the criterion, but not in a sufficient way and/or serious weaknesses are present.

○ 3: Low. The proposal addresses the criterion overall, but not in a sufficient way and a number of serious weaknesses are present.

○ 2: Poor. The criterion is poorly addressed, and/or there are major inherent weaknesses.

○ 1: Minimal. The criterion is minimally addressed and there are major weaknesses.

○ 0: Bad. The proposal is of very low quality.

CRITERION 3: Project Implementation (30% weighting)
C3.1 Quality and effectiveness of the work plan

C3.1.1 Is the work plan well structured and appropriate to ensure that the research objectives and requested deliverables are achieved?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.1.2 Are the tasks and activities sufficiently detailed?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.1.3 Are the planned mobilised resources appropriate in relation to the proposed activity?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.2 Quality and effectiveness of the management procedures including risk and mitigation management

C3.2.1 Is there appropriate management structure and related procedures?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.2.2 Does the plan ensure quality and effective risk and mitigation management techniques?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.3 Integration to the Trustchain ecosystem

C3.3.1 Is there an plan to integrate the work to the overall Trustchain ecosystem? Is the plan appropriately defined and convincing?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.4 Team excellence and availability

C3.4.1 Is the experience of the applicant on the research topic well described and adequate to achieve the reaserch goals?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.4.2 When relevant, is the nature of the reaserch team well outlined and adequate to achieve the research goals?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

C3.4.3 Has the applicant demonstrated the capacity to achieve the research goals?. Tick the box only if the proposal addresses WELL the requirement.
☐ Y

-

CRITERION 3- COMMENTS & SCORE. * Structure your text in two parts e.g. Strengths and Weaknesses
Enumerate strengths and weaknesses by writing high quality comments.

○ 10: Excellent. The proposal is outstanding and successfully addresses all relevant aspects of the criterion.

○ 9: Almost Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are very minor.

○ 8: Very good. The proposal addresses the criterion very well, but a small number of minor shortcomings are present.

○ 7: Good. The proposal addresses the criterion well and any shortcomings present are not serious.

○ 6: Satisfactory. The proposal addresses the criterion in a satisfactory way, but a small number of shortcomings are present.

○ 5: Almost Sufficient. The proposal almost addresses all relevant aspects of the criterion, but shortcomings are present.

○ 4: Insufficient. The proposal addresses the criterion, but not in a sufficient way and/or serious weaknesses are present.

○ 3: Low. The proposal addresses the criterion overall, but not in a sufficient way and a number of serious weaknesses are present.

○ 2: Poor. The criterion is poorly addressed, and/or there are major inherent weaknesses.

○ 1: Minimal. The criterion is minimally addressed and there are major weaknesses.

○ 0: Bad. The proposal is of very low quality.

ANNEX 2- ADMINISTRATIVE FORM

Find hereafter the list of administrative information that you need to fill directly in the F6S portal to apply.

ADMINISTRATIVE FORM

This administrative form has the following mandatory sections:

o SECTION 1: Proposal identification

o SECTION 2: Administrative Data

o SECTION 3: Proposal Description

o SECTION 4: Final questions

Documents to be reviewed when preparing the application:

o TRUSTCHAIN Open Call 2 Text, a document that provides the technical details for the TRUSTCHAIN Open call 2 available at: https://trustchain.ngi.eu/apply.

o TRUSTCHAIN Guide for Applicant, defining the Open Call Terms & Conditions available at: https://trustchain.ngi.eu/apply.

o Proposal Description Template, a mandatory and editable document to describe your proposal, available at: https://trustchain.ngi.eu/apply.

o TRUSTCHAIN Additional Applicant(s) Template, only needed if your proposal involves more than 3 individuals (Natural persons) or/and more than 3 organisations (Legal entities), available at: https://trustchain.ngi.eu/apply.

o Indicative Sub-grant Agreement Form, a template of the sub-grant agreement that the selected applicants will be requested to sign, available at: https://trustchain.ngi.eu/apply. It is not necessary to send this document at the time of application.

If you have any questions, feel free to contact the TRUSTCHAIN team (trustchain@ngi.eu). Failure to provide the required information in all sections will result in disqualification.

SECTION 1: PROPOSAL IDENTIFICATION

1. Proposal Title *

2. Proposal Acronym *

3. Keywords *

Please select the keywords related to your proposal

☐ Trustworthy hardware & manufacturing
☐ Software Engineering (Including protocols, interoperability and fundamentals e.g. cryptography, algorithms, proofs)
☐ Cloud engineering, digital twins, edge and fog computing
☐ cryptography, standardisation and security engineering

- □ digital twins, edge and fog computing
- □ Operating Systems, firmware and virtualisation
- □ Measurement, monitoring, analysis & abuse handling
- □ Middleware, distribution, deployment, operations, DNS, authorisation, authentication, reputation systems
- □ Decentralised solutions, blockchain, distributed ledger
- □ semantic web, ontology engineering
- □ Data & AI
- □ Services & Applications (e.g. email, instant messaging, search, video chat, collaboration, community)
- □ Trustworthiness (Including: transparency, auditability and security)
- □ Resilient, robust and dependable
- □ digital identity management, self-sovereign identity
- □ Privacy and confidentiality
- □ Empowerment and self-determination
- □ Inclusiveness, accessibility diversity and democracy
- □ Permission less innovation, decentralisation and level playing field
- □ Social good, fairness and ethical behaviour
- □ Sustainability/Eco-friendliness
- □ ecosystem economics, Well-balanced economy
- □ Green, environmental sustainability

SECTION 2: ADMINISTRATIVE DATA APPLICANT(S)

4. You are applying as: *

Notice that as team of individuals (two or more natural persons), you will get a maximum of 97K€+ 2 K€.
Any other configuration involving legal entities can obtain up to 115K€+ 2K€.
The funding will be automatically calculated according to the selection below.

- □ A single organization (legal entity)
- □ A group of individuals (team)
- □ A group of organisations (consortium)
- □ A group of individual(s) and organisation(s)

APPLICANT(S) INFORMATION (INDIVIDUAL(S))

Please fill in the following information about the individual(s) applying as a natural person(s).
WARNING: if in the previous question you indicated you apply as a legal entity, or consortium, do not fill the Individuals section.

INDIVIDUAL - NATURAL PERSON 1

5. Name

6. Surname

7. E-mail

8. ID type (Citizen card, passport, or other)

9. ID number

10. Country of residence/work

11. Has been funded by the European Commission through H2020 before? (Grant or subgrant)

  ☐ Yes
  ☐ No

12. Has been funded by other NGI projects?

  ☐ Yes
  ☐ No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

13. Has recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

  ☐ Yes
  ☐ No

If yes, please indicate which one and explain the overlaps and differences with the current proposal.

INDIVIDUAL - NATURAL PERSON 2

14. Name

15. Surname

16. E-mail

17. ID type (Citizen card, passport, or other)

18. ID number

19. Country of residence/work

20. Has been funded by the European Commission through H2020 before? (Grant or sub grant)

  ☐ Yes
  ☐ No

21. Has been funded by other NGI projects?

  ☐ Yes
  ☐ No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

22. Has recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

  ☐ Yes
  ☐ No

If yes, please indicate which one and explain the overlaps and differences with the current proposal

INDIVIDUAL - NATURAL PERSON 3

23. Name

24. Surname

25. E-mail

26. ID type (Citizen card, passport, or other)

27. ID number

28. Country of residence/work

29. Has been funded by the European Commission through H2020 before? (Grant or subgrant)

☐ Yes
☐ No

30. Has been funded by other NGI projects?

☐ Yes
☐ No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

31. Has recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

☐ Yes
☐ No

If yes, please indicate which one and explain the overlaps and differences with the current proposal

APPLICANT(S) INFORMATION (ORGANISATION(S))

Please fill in the following information about the organisation(s) applying as legal entity/ies

ORGANISATION - LEGAL ENTITY 1

32. Entity legal name

33. Legal status of your organisation

☐ Secondary or Higher education establishment
☐ Research organisation
☐ SME
☐ Large enterprise
☐ Public Body
☐ A non-for profit organisation, association, NGO
☐ Foundation
☐ International organisation
☐ Other? Please specify

34. Country

35. VAT number

36. Incorporation year

37. Contact person email

38. Has the legal entity been funded by the European Commission before? (Grant or subgrant)

    ☐   Yes
    ☐   No

39. Has the legal entity been funded by other NGI projects?

    ☐   Yes
    ☐   No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

40. Has the legal entity recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

    ☐   Yes
    ☐   No

If yes, please indicate which one and explain the overlaps and differences with the current proposal

ORGANISATION - LEGAL ENTITY 2

41. Entity legal name

42. Legal status of your organisation

    ☐   Secondary or Higher education establishment
    ☐   Research organisation
    ☐   SME
    ☐   Large enterprise
    ☐   Public Body
    ☐   A non-for profit organisation, association, NGO
    ☐   Foundation
    ☐   International organisation
    ☐   Other? Please specify

43. Country

44. VAT number

45. Incorporation year

46. Contact person email

47. Has the legal entity been funded by the European Commission before? (Grant or subgrant)

    ☐   Yes
    ☐   No

48. Has the legal entity been funded by other NGI projects?

    ☐   Yes
    ☐   No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

49. Has the legal entity recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

    □　　Yes
    □　　No

    If yes, please indicate which one and explain the overlaps and differences with the current proposal

ORGANISATION - LEGAL ENTITY 3

50. Entity legal name

51. Legal status of your organisation

    □　　Secondary or Higher education establishment
    □　　Research organisation
    □　　SME
    □　　Large enterprise
    □　　Public Body
    □　　A non-for profit organisation, association, NGO
    □　　Foundation
    □　　International organisation
    □　　Other? Please specify

52. Country

53. VAT number

54. Incorporation year

55. Contact person email

56. Has the legal entity been funded by the European Commission before? (Grant or subgrant)

    □　　Yes
    □　　No

57. Has the legal entity been funded by other NGI projects?

    □　　Yes
    □　　No

If yes, please indicate which one, explain the overlaps and differences with the current proposal and indicate the total funding amount received.

58. Has the legal entity recently applied to an NGI call or another EC funding instrument that is under evaluation or plans to apply to?

    □　　Yes
    □　　No

    If yes, please indicate which one and explain the overlaps and differences with the current proposal

ADDITIONAL APPLICANT(S)?

59. If your proposal has more than 3 applicants participating as individuals (Natural persons) or/and more than 3 applicants participating as organisations (Legal entities), please upload the Annex 3 – Additional Applicant(s) Template, filled with the information about the applicant(s) that did not fit in this form. (Max file size 30MB.)

UPLOAD FILE

CONTACT PERSON (COORDINATOR)

Contact person for the proposal and coordination of the project what ever the type of Applicant you are.

Notice that the result of the evaluation will be sent to this person.

60. Full Name *

61. Entity (If applicable) *

62. E-mail *

63. Phone number * (Include country code)

SECTION 3: ETHICS

3.1. HUMAN EMBRYOS/FOETUSES

64. Does your innovation project involve Human Embryonic Stem Cells (hESCs)? *

   ☐ Yes
   ☐ No

65. Does your innovation project involve the use of human embryos? *

   ☐ Yes
   ☐ No

66. Does your innovation project involve the use of human foetal tissues / cells? *

   ☐ Yes
   ☐ No

3.2. HUMANS

67. Does your innovation project involve human participants? *

   ☐ Yes
   ☐ No

68. Are they volunteers for social or human sciences research? *

   ☐ Yes
   ☐ No

69. Are they persons unable to give informed consent? *

   ☐ Yes
   ☐ No

70. Are they vulnerable individuals or groups? *

   ☐ Yes
   ☐ No

71. Are they children/minors? *

   ☐ Yes
   ☐ No

72. Are they patients? *

   ☐ Yes
   ☐ No

73. Are they healthy volunteers for medical studies? *

   ☐ Yes
   ☐ No

74. Does your innovation project involve physical interventions on the study participants? *

   ☐ Yes
   ☐ No

3.3. HUMAN CELLS / TISSUES

75. Does your innovation project involve human cells or tissues (other than from Human Embryos/ Foetuses? *

   ☐ Yes
   ☐ No

3.4. PERSONAL DATA

76. Does your innovation project involve personal data collection and/or processing? *

   ☐ Yes
   ☐ No

77. Does it involve the collection and/or processing of sensitive personal data (e.g: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)? *

   ☐ Yes
   ☐ No

78. Does it involve processing of genetic information? *

   ☐ Yes
   ☐ No

79. Does it involve tracking or observation of participants? *

   ☐ Yes
   ☐ No

80. Does your innovation project involve further processing of previously collected personal data (secondary use)? *

   □   Yes
   □   No

3.5. ANIMALS

81. Does your innovation project involve animals? *

   □   Yes
   □   No

3.6. THIRD COUNTRIES

82. In case non-EU countries are involved, do the innovation project related activities undertaken in these countries raise potential ethics issues? *

   □   Yes
   □   No

83. Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)? *

   □   Yes
   □   No

84. Do you plan to import any material - including personal data - from non-EU countries into the EU? *

   □   Yes
   □   No

85. Do you plan to export any material - including personal data - from the EU to non-EU countries? *

   □   Yes
   □   No

86. In case your innovation project involves low and/or lower middle income countries, are any benefits-sharing actions planned? Are they children/minors? *

   □   Yes
   □   No

87. Could the situation in the country put the individuals taking part in the innovation project at risk? *

   □   Yes
   □   No

3.7. ENVIRONMENT & HEALTH AND SAFETY

88. Does your innovation project involve the use of elements that may cause harm to the environment, to animals or plants? *

   □   Yes

☐ No

89. Does your innovation project deal with endangered fauna and/or flora and/or protected areas? *

☐ Yes
☐ No

90. Does your innovation project involve the use of elements that may cause harm to humans, including innovation project staff? *

☐ Yes
☐ No

3.8. DUAL USE

91. Does your innovation project involve dual-use items in the sense of Regulation 428/2009, or other items for which an authorisation is required? *

☐ Yes
☐ No

3.9. EXCLUSIVE FOCUS ON CIVIL APPLICATIONS

92. Could your innovation project raise concerns regarding the exclusive focus on civil applications? *

☐ Yes
☐ No

3.10. MISUSE

93. Does your innovation project have the potential for misuse of innovation project results? *

☐ Yes
☐ No

3.11. OTHER ETHICS ISSUES

94. Are there any other ethics issues that should be taken into consideration? *

☐ Yes
☐ No

If yes, please specify

95. Ethics issues *

☐ I confirm that I have taken into account all ethics issues described above

96. Does your innovation require prior approval by a competent ethics or data protection body?

☐ No
☐ Yes, i.e. * (please specify which ethics/data protection body as well as the time period required for such approval)

Please note that seeking and obtaining the mandatory approvals in a timely manner from competent ethics and/or data protection bodies are the applicant's sole and exclusive responsibility and that the absence of such approvals, when and where legally required, may void the eligibility of the applicant's proposal.

SECTION 4: PROPOSAL DESCRIPTION

97. Please upload your proposal in Portable Document Format (pdf). Use the official template available at: https://trustchain.ngi.eu/apply/*. Applicants using other kind of template/ document structure will be automatically ineligible.

UPLOAD PROPOSAL (Max file size 30MB.)*

SECTION 5: FINAL QUESTIONS

98. Acceptance of the TRUSTCHAIN Open Call Terms & Conditions Full call documents available at https://trustchain.ngi.eu/apply/*

   o By ticking this box, I/we confirm that we have reviewed, accept and comply with the TRUSTCHAIN Open Call Terms & Conditions as defined in the Guide for Applicant

99. Authorisation to apply in the name of

   o By ticking this box, I confirm the information submitted within this application is true. I am authorised to apply in the name of my entity/group of natural persons.

100. Conflict of interest avoidance with TRUSTCHAIN consortium

   □ By ticking this box, I confirm the members of the team involved in the proposal are not employees of any of the legal partners or their associated/linked-entities identified in the Grant Agreement No. 101093274 with the EC.

101. Fraudulent behaviour avoidance

   □ By ticking this box, I confirm the organisation(s) or individual(s) applying do not have convictions for fraudulent behaviour, other financial irregularities, unethical or illegal business practices.

102. Bankruptcy information

   □ By ticking this box, I confirm the participating organisation(s) do(es) not have been declared bankrupt or have initiated bankruptcy procedures.

103. Multiple submissions

   □ By ticking this box, I confirm that all the members involved in the proposal (natural persons/legal entities) are only submitting one proposal under this open call

104. European Commission Regulation No 651/2014, art. 2.18

   □ By ticking this box, I confirm the applicant(s) is not under liquidation or is not an enterprise under difficulty accordingly to the Commission Regulation No 651/2014, art. 2.18.

105. Originality and freedom to operate

   □ By ticking this box, I confirm the project is based on original works and going forward any foreseen developments are free from third party rights, or they are clearly stated.

106.Applicant(s) eligibility

☐ By ticking this box, I confirm the applicant(s) is not excluded from the possibility of obtaining EU funding under the provisions of both national and EU law, or by a decision of both national or EU authority.

107.TRUSTCHAIN Sub-grant Agreement

☐ By ticking this box, I confirm the principal investigator involved in the proposal agrees with the terms presented in the Indicative Sub-grant Agreement Form.

108.Double funding and operational capacity

☐ By ticking this box, I confirm the applicant(s) has not received funding for a similar project and that the applicant(s) has enough Operational Capacity to carry out the work. In addition, the applicant(s) gives consent to the TRUSTCHAIN consortium to share the needed information (such as entities names and project details (abstract or the full proposal)) with other NGI RIAs projects for the only purpose of cross-checking that there is no double funding or operational capacity conflict.

109.How did you hear about TRUSTCHAIN?

☐ News/Media
☐ Event
☐ E-mail
☐ NGI portal
☐ Referral
☐ Social media
☐ Through an TRUSTCHAIN partner
☐ F6S portal
☐ European Commission portal
☐ Other

ANNEX 3 - PROPOSAL DESCRIPTION TEMPLATE

PROPOSAL DESCRIPTION TEMPLATE
SECOND OPEN CALL FOR PROPOSALS

Call closure for proposals: 20 September 2023 at 17:00 CEST

Version 1.0 – 20 July 2023

GENERAL INSTRUCTIONS ON THE TEMPLATE

This template is to be used for the TRUSTCHAIN Open Call #2 submission procedure.

The structure of this template must be strictly followed when preparing your proposal. It has been designed to ensure that the important aspects of your planned work are presented in a way that will enable the experts to make an effective assessment against the evaluation criteria.

All proposers should organise their information as focused as possible, explaining at least the following aspects of their projects: overall description of the application; potential users/customers and markets; methods and approaches for users/customer engagement; resolution of the ownership (including preferably open source licensing approach for the results); positioning on the market against existing similar solutions/services; clear description of the added value; data quality properties that will be achieved by the application solution; time to market of the proposed solution/application.

Please be aware that proposals will be evaluated as they were submitted, rather than on their potential if certain changes were to be made. This means that only proposals that successfully address all the required aspects will have a chance of being funded. There will be no possibility for significant changes to content, budget and team composition during the grant preparation.

Total page limit: 11 pages. Sections 1, 2 and 3, together, should not be longer than 10 pages.

All tables, figures, references and any other element pertaining to these sections must be included as an integral part of these sections and are thus counted against this page limit.
The total page limit will be applied automatically; **therefore, you must remove this instruction page before submitting.**

After the deadline, excess pages (in over-long proposals/applications) will not be taken into consideration by the experts. **Final pdf must not be longer than 11 pages.**

The proposal is a self-contained document. Experts will be instructed to ignore hyperlinks to information that is specifically designed to expand the proposal, thus circumventing the page limit. Please, do not consider the page limit as a target! It is in your interest to keep your text as concise as possible, since experts rarely view unnecessarily long proposals in a positive light.

The following formatting conditions apply: The reference font for the body text is Arial. The use of a different font for the body text is not advised and is subject to the cumulative conditions that the font is legible and that its use does not significantly shorten the representation of the proposal in number of pages compared

TRUSTCHAIN
SECOND OPEN CALL FOR PROPOSALS

Acronym of your proposal
Full title of your proposal

Table of Contents

1. PROJECT SUMMARY

(Maximum 300 words)
-Describe your proposal at a high level.
Please note that this information may be used for dissemination purposes (only if your proposal is accepted and funded by the TRUSTCHAIN program).

Insert text here.

2. APPLICANT BACKGROUND

(Maximum 1 page)
1. Organisation profile (If applicable, in case a single organisation apply)
-Describe the organisation proposing the collaboration (size of organization, type of organization, how many people, capital, and market),), main expertise and business area as well as its main business interest in this proposal.
- Document the organisation previous related experience including the main publications, projects, product/service portfolio, patents and relevant contributions in line with your proposal.
- Justify the relevance of our organisation's strategy to the specified TRUSTCHAIN 2nd Call topic.

2. Team/consortium profile (If applicable, in case a team of natural persons/ consortium of legal entities apply)
-Describe the team, its main expertise and business area.
-List the members of the participating organisations that will directly work on the project (name, job title, main expertise & role in the project) and provide evidence of the main publications, projects, product/service portfolio, patents and relevant contributions of the different natural persons/organisations part of the team/consortium in line with your proposal.
-Describe the team/consortium partners' synergies and their relevance for the proposed project and TRUSTCHAIN 2nd Call.

Insert text here.

3. DETAILED PROPOSAL DESCRIPTION

(Maximum 8 pages)

3.1 CONCEPT AND OBJECTIVES

(Maximum 1 page)
-Describe the specific objectives of your proposal and explain the overall concept underpinning your proposed solution considering the TRUSTCHAIN overall goals and specific OC2 objective on User Privacy and Data Governance
-It should be clear:
- • What are the needs and what are the relevant market trends?
- • What TRUSTCHAIN OC2 challenges are you addressing and what is the methodology you are adopting?

- What existing solutions (including your own) from industry and from the scientific literature partly address the challenges?
- What is the human centric approach you are going to follow and how this is relevant for the work proposed
- What new value proposition are you offering, to which target group?
- What would be the benefits for TRUSTCHAIN Large Scale Pilot.

Insert text here.

3.2 PROPOSAL SOLUTION

(Maximum 2 pages)
-Give a description of the product/prototype with which you want to face the challenge.
-Indicate:
- How the solution will approach the challenge. You should particularly take care of the relevance of your solution according to current challenges related to User Privacy and Data Governance as well as to TRUSTCHAIN objectives and requirements
- Clearly the originality and novelty elements.
- Present and justify the current maturity of your product/prototype and the expected maturity at the end of the project (current and expected Technology Readiness Level)
- What will be the approach to better understand users' needs and to validate your proof of concept? Indicate and justify the size of the deployment, the test you intend to conduct (ethical clearance, number of users, devices …)

Insert text here.

3.3 EXPECTED IMPACT

(Maximum 2 pages)
-Describe how your proposal will contribute to:
- The objectives of the TRUSTCHAIN project as well as to better acceptance of User Privacy and Data Governance solutions by specific groups of end users
- Add value to the TRUSTCHAIN established impact mentioned in the call text and the TRUSTCHAIN and NGI Ecosystem.
- Outline the industrial impact at the European level and worldwide you are expecting to achieve. Provide measurable indicators and the rationale for the targets established.
- Provide arguments for how this work will advance your own business and competitiveness.
- Present the socio- economic and environmental impact of your work, when relevant.
-Present your dissemination and communication plan to maximise the impact foreseen
-Outline the data that you generate and a brief Data Management Plan

Insert text here.

3.4 BUSINESS MODEL AND SUSTAINABILITY

(Maximum 1 page)

-What is the business potential of the proposal?
-What is the business model? Explain how you will make money with this product or service (revenue model, etc.).
-Explain the next steps towards economic sustainability of your project and towards deploying your solution at a larger scale.
-Justify how your solution is going to comply with environmental sustainability.

Insert text here.

3.5 IMPLEMENTATION

(Maximum 2 pages)
-Provide an overview of your overall work plan considering the 9 months' timeframe of TRUSTCHAIN Open Call #2.
-Analyse the activities you plan to execute in each task and the functionality/services you are going to deliver: objective, duration, implementation steps, resources available. Illustrate the timing of your activities using a Gantt diagram or similar. The co-creation approach should be made evident. Please note that if relevant seeking and obtaining the mandatory approvals in a timely manner from competent ethics and/or data protection bodies are the applicant's sole and exclusive responsibility and that the absence of such approvals, when and where legally required, may void the eligibility of the applicant's proposal.
-Outline a relevant risk management plan.
-Oultine the management procedures and overall resources you are aiming to employ.
-Use the table hereafter in order to help you present the requested information.

Insert text here.

TABLE 1: EXAMPLE TABLE

Work plan tasks	Description	Starting Month	Ending Month

3.5.1 Deliverables and milestones

Please add a list of deliverables and milestones using the table provided. 4 deliverables are mandatory for TRUSTCHAIN, please consider them in the list of deliverables (e.g., documents, reports, user manual, a tool …) you intend to submit. Justify each of them with a small description and state the relevant TRL level for each deliverable.

TABLE 2: TABLE OF DELIVERABLES AND MILESTONES

No.	Deliverable or milestone name	Description	Type	Delivery Month	TRL level delivered

-Indicate how you intend to manage your activities during your project lifecycle (9 months) including progress monitoring and risks management procedures

Insert text here.

----Pages count finishes here----

ANNEX 3 - EVALUATION SUMMARY REPORTS OF THE 15 PROJECTS SELECTED

DOOF - DATA OWNERSHIP ORCHESTRATION FRAMEWORK

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 013_2179131

Proposal acronym: DOOF

Proposal title: Data Ownership Orchestration Framework

Contact: elena.pasquali@ecosteer.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 38,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 4**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The concept is strong and clear and aligns seamlessly with TRUSTCHAIN's topic, emphasizing data sovereignty and decentralized digital identity.

- A convincing technical approach is leveraged, utilizing proven and patented technology, ensuring a solid technical base. The technical approach is credible with a user-centric focus, as it allows individuals to control, grant, and revoke data visibility. It is designed to facilitate user-friendly data exchanges and aims to engage end-users in the co-creation process through workshops and feedback collection, making it aligned with a user-centric approach.

- The contribution beyond the state of the art is clearly detailed as it envisions a new decentralized data governance framework with unique software components like DVCO. It credibly presents a novel consent management system using blockchain, transforming the traditional data-sharing model.

- The innovation potential is well justified and demonstrated through tangible examples and a technical approach which allows the solution to be retrofitted to relevant data flows.

Weaknesses:

- The proposal could provide more detailed competitive analysis to assess the market readiness against other emerging technologies and similar solutions.

- The extent to which the proposal integrates with or builds upon existing tools as encouraged by TRUSTCHAIN could be more detailed.

Criterion 2 - Expected impact and Value for Money	**Score: 3**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The expected impact of TRUSTCHAIN of promoting decentralized, privacy-centric, and regulatory compliant data governance solutions is well documented. It justifies how the framework will enhance the TRUSTCHAIN ecosystem by enabling a set of tools allowing data owners to exercise data ownership rights and for ecosystem suppliers to deploy data exchanges with privacy by design.

- The modular design facilitates integration and interoperability with existing and future decentralized applications.

- The solution addresses a real need of the targeted end users by providing a decentralized, privacy-centric data exchange platform which aligns with the emerging demand for better data control and privacy.

- The strategy to disseminate and exploit the new knowledge generated by the action is appropriate, including the creation of a webpage, regular updates through videos, pilot results, end user testimonials, articles and the publication of open-source code on Github.

- The strategy for targeting peers and the wider community is clear, consistent, and appropriate. The proposal plans to reach out to various stakeholders through industry events, conferences, and social media channels. It also intends to engage end users and collect feedback through focus groups, monitoring user interactions, and involving them in co-creation workshops.

- The business strategy and commercialization plan is ambitious and relevant to the market opportunity presented. A revenue model based on a yearly software license priced per number of devices is presented where the DVCO API is installed, with a projection of achieving 4.6 million DVCO enabled devices by 2026.

- Sensitive data management related to citizens is well outlined and a Data Management Plan (DMP) mentions that personal information collected for activities proprietary to each citizen and won't be shared or used for other purposes. The DMP also states that EcoSteer will comply with the requirements of Regulation (EU) 2016/679 and the Council of 27/04/2016 on the protection of personal data.

Weaknesses

- Progression from TRL 3 to TRL 7 in 9 months is too ambitious and not fully justified. Capacity to achieve KPIs highly dependent on the operational plan, which is still pending development as referenced in the proposal's risk management plan.

- Noting the ambitious scalability plan, the dissemination approach does not elaborate sufficiently on the outreach to key partners and ecosystem suppliers and any potential agreements or collaboration opportunities.

- The business plan is too ambitious and not fully credible.

- The exact mechanisms of IP management within the context of TRUSTCHAIN are poorly described.

- The specific Key Performance Indicators (KPIs) to better measure and evaluate the success and impact over time are not adequately established.

Criterion 3 - Project Implementation	**Score: 4,5**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The plan is well-structured, delineating clear steps and deliverables across various stages. The allocation of tasks and resources corresponds well to the proposed activities, promoting an effective pathway towards reaching the end goals.

- The mobilized resources are appropriate in relation to the activities. The allocation of resources is aligned with the requirements of each task, ensuring that there are sufficient resources to effectively carry out the activities and achieve the objectives of the project.

- The management structure and procedures are well-suited for overseeing the execution, ensuring accountability, and facilitating communication among the team.

- The risk and mitigation management plan identifies potential challenges, their likelihood, impact, and strategies to manage them, demonstrating foresight and preparedness.

- The experience of the team on the research topic is well-described and adequate to achieve the research goals. The team's previous work, expertise, and their background aligns well with the objectives. The Capacity of the team to deliver is credible, particularly when noting the existence of two patents, one of which is highly relevant.

- There is a clear justification for the integration capacity into the overall Trustchain ecosystem, supported by standards and a reference framework.

Weaknesses:

- Some tasks within the work plan are not adequately detailed.

- The risk and mitigation management is not sufficient in terms of the contingency plans.

UTIP-DAM - UTILITY-PRESERVING, DECENTRALIZED ANONYMITY OF MOBILITY DATA

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 031_2180349

Proposal acronym: UtiP-DAM

Proposal title: Utility-Preserving, Decentralized Anonymity of Mobility data

Contact: erel@cs.co.il

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 42 (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4,5
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The relevance to TRUSTCHAIN topics based on the focus on the development of a decentralised method for the anonymisation of mobility data while preserving its usability is appropriate.

- The concept is clear and sound. It includes a user-centric approach in an indirect manner.

- The idea is innovative, pertinent, and well described by quoting recent research in this domain.

- The maturity of the proposed services is well addressed and justified.

Weaknesses:

- Existing solutions and the competition are not adequately described.

- All the pilots will be performed on buses and trains, probably leading to biased results that are not sufficiently considered.

Criterion 2 - Expected impact and Value for Money	Score: 4
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The potential impact of overcoming the limitations of centralised methods, where data controllers have full access to the raw data, is appropriate.

- The added value to TRUSTCHAIN and NGI ecosystem and the contribution to a decentralized ecosystem, is well described.

- The contribution to TRUSTCHAIN Objectives by addressing user privacy and data governance acceptance is adequately described. The socio-economic and environmental impacts are adequately described.

- The data generation and management plan are adequately addressed. The business model is clear.

- The steps towards economic sustainability are adequately described. The Environmental sustainability compliance is well addressed, and it is a positive point of the proposal. The strategy for targeting peers is adequately described.

Weaknesses:

- The contribution to an ecosystem of decentralized identity management that can seamlessly integrate and interoperate with any of the existing decentralised applications, is not carefully elaborated.
- Quantitative and/or qualitative KPIs for measuring/ verifying the impact are not sufficiently documented.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan and task breakdown are reasonable and appropriate for the project size.
- Planned mobilised resources are appropriate in relation to the proposed activity.
- There is a management and risk mitigations task running through the entire project time.

Weaknesses:

- The implementation plan, although it is well structured, is too brief in the description of the tasks.
- The integration part with the overall TRUSTCHAIN ecosystem is not adequately described.

MORPHMETRO - SECURE AND PRIVACY-PRESERVING EXCHANGE AND ANALYSIS OF MEASURED DATA BASED ON HOMOMORPHIC ENCRYPTION

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 033_2155987

Proposal acronym: MorphMetro

Proposal title: Secure and privacy-preserving exchange and analysis of measured data based on homomorphic encryption

Contact: ivica.lukic@gmail.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 37 (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 4**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The innovative approach that has presented credibly the potential to push the boundaries of the current state of the art.

- A clear, pertinent, and sound concept is proposed.

- The technique is novel and includes aspects of user privacy and data governance.

Weaknesses:

- A well-defined plan for testing, validation, and demonstration is not sufficiently defined for a strong research methodology and the users to be involved in the testing, validation and demonstration phases, are not appropriately established.

- The way to move from TRL 2 to TRL 7 in just 9 months, is not sufficiently credible as specific information on testing, validation, and demonstration scenarios, is not carefully elaborated.

Criterion 2 - Expected impact and Value for Money	**Score: 4**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The alignment with broader objectives of TRUSTCHAIN is credible, aiming to contribute to the ecosystem of decentralized identity management solutions that are transparent, interoperable, and compliant.

- A compelling vision for its potential impact has been articulated, both in European and global markets, convincing on the value for money.

- A seemingly effective strategy to disseminate and exploit new knowledge, targeting an array of peers including scientific and industry actors, which shows forethought and planning.

- The planned research will contribute to the overall TRUSTCHAIN ecosystem to preserve the privacy of users while sharing data.

- The proposed solution credibly addresses a real need of the targeted end users and will have an impact on the needs of European markets

- The strategy for targeting peers, academic and industry experts is adequately presented.

- The potential business strategy/ commercialization plan is adequately detailed.

- The management of sensitive data in the context of TRUSTCHAIN is well addressed.

Weaknesses:

- The intellectual property (IP) strategy is poorly addressed and this is a significant shortcoming.

- The user-centric approach is not adequately detailed and not appropriately structured.

- The KPIs are not defined explicitly.

Criterion 3 - Project Implementation	Score: 3
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The general alignment with the broader goals of TRUSTCHAIN, suggesting that it could integrate into the ecosystem to some extent is appropriately documented.

- The work plan is well structured and the nature of the research team is well outlined which gives confidence in their adequacy to achieve the outlined goals.

- The experience of the applicant on the research topic is well-described.

Weaknesses:

- The resources needed for successful project implementation are overall underestimated.

- Encryption expertise is not clearly demonstrated, which is a shortcoming given its likely relevance to the project.

- The risk and mitigation strategies, are not adequately detailed.

- The plan to integrate the work with the overall TRUSTCHAIN ecosystem are insufficiently documented.

SURE - SYNTHETIC DATA: UTILITY, REGULATORY COMPLIANCE, AND ETHICAL PRIVACY

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 040_2173278

Proposal acronym: SURE

Proposal title: Synthetic Data: Utility, Regulatory compliance, and Ethical privacy

Contact: shalini@clearbox.ai

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 41,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The concept is clearly explained. It focuses on addressing privacy and data governance challenges in the development of AI, using privacy-enhancing technologies (PETs) and focusing on synthetic data.

- The real problem to be addressed is credibly described.

- The involvement of end-users in the process is adequately presented.

Weaknesses:

- It is not clearly demonstrated how the proposed approach differs from alternative state-of-the-art approaches for synthetic data generation.

- The data sets generation and the certification processes are not explained in detail.

Criterion 2 - Expected impact and Value for Money	Score: 4
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- Good synergies with the TRUSTCHAIN goals are presented.

- Concrete and realistic KPIs are provided.

- There is a good identification of potential clients/partners.

- The partner engagement strategy is convincing with a relevant community targeted.

- The real-world need for such platforms is well explained and backed by realistic examples.

- High impact potential is expected and highlighted and good synergy with existing projects.

Weaknesses:

- The engagement strategies ignore engagement with the academia. This is a minor shortcoming.

- The handling of sensitive data, that might be needed for creating synthetic data is insufficiently detailed.

Criterion 3 - Project Implementation - Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	**Score: 4,5** Threshold: 3 Weight: 30%

Strengths:

- The team demonstrates skills which give confidence in their ability to achieve the projected goals.

- Multiple existing partnerships/clients have been presented, which is an asset for the credibility of the team's potential exploitation strategies.

- The solution is credibly described at TLR 3-4, hence significant progress during the course of the project implementation is expected.

- A realistic plan to reach the project outcomes has been documented.

- Realistic risk management is also presented.

Weaknesses:

- The tasks and risk management plan are not sufficiently detailed.

DGUARD - PRIVACY PRESERVING DATA-SHARING PLATFORM

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 051_2180559

Proposal acronym: dGUARD

Proposal title: Privacy preserving data-sharing platform

Contact: jordi@bloock.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 40   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 4**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The proposal addresses well the criterion providing technical, scientific and operational details.

- The technical scope is credibly described as: 1) A consent management system based on self-sovereign digital identity authentications and interactions, 2) A privacy-preserving authentication mechanism to enable privacy-preserving authentications, thus boosting anonymization, 3) A proxy re-encryption scheme to guarantee e2e data privacy, 4) A blockchain notarized audit-trail to guarantee traceability, non-repudiation and accountability.

- The concept is clear, pertinent, and sound according to the TRUSTCHAIN topic.

- It is credible that a user-centric approach will be implemented. It is well described, depicting several functional flows.

- The innovation potential is convincing because it addresses user anonymity in interactions with services, using W3C DIDs.

Weaknesses:

- The way that the proposed solution advances the state of the art is not clearly presented.

- The decentralised nature is not fully credible as the DID will be stored in a centralised cloud. This is not sufficiently described.

Criterion 2 - Expected impact and Value for Money	**Score: 4**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The contribution to the TRUSTCHAIN goal and mission is clearly presented. The solution will become a part of the identity management ecosystem as it is generic enough to be used in different contexts.

- The solution is transparent, interoperable, privacy-aware, and regulatory compliant to the users that is appropriate.
- The contribution of the expected needs at the European level and worldwide is appropriately documented.
- A potential business strategy and commercialization plan are present and credible.

Weaknesses:

- It is unclear how the proposed solution answers to a real need of the targeted end users.
- KPIs to be achieved are not fully appropriately detailed, e.g., the number of end users using the solution.
- The dissemination strategy is not sufficiently detailed, this is a shortcoming.
- The strategy for targeting peers is not elaborated in detail, beyond the plan to have signed consent agreements with the end-users or their representatives.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan is appropriately structured and appropriate to the size of the project.
- The tasks and activities are sufficiently detailed.
- The planned mobilized resources are appropriate.
- There are quality and effective management procedures in place.
- The proposed platform seamlessly integrates with other solutions to address anonymity and privacy concerns by employing zero-knowledge technology in authentication and data minimization processes.
- The team is experienced with the proposed research topic and will credibly achieve the research goals.

Weaknesses:

- The description of how this proposal will be integrated into the TRUSTCHAIN ecosystem is weakly documented.
- The risk and mitigation management techniques foreseen are not adequately elaborated.

NG-SC - NEXT GENERATION SMART CITIES

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 058_2173626

Proposal acronym: NG-SC

Proposal title: Next Generation Smart Cities

Contact: aleksandar.tosic@innorenew.eu

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 40   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 4**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The concept is clear, pertinent, and sound according to the OC2 TRUSTCHAIN topics. The proposed solution will contribute to an ecosystem of decentralized identity management solutions seamlessly integrating and interoperating with any existing decentralized applications.

- The direct alignment to the TRUSTCHAIN OC2 challenge is clear: "Data owners currently do not have means to be compensated or enable fair data value sharing with the big players in the market".

- The user-centric approach is credibly presented, empowering users to participate and get rewarded actively in the data economy.

- A data-sharing model is proposed, aided by an advance in privacy-preserving distributed computing.

- The "privacy by design" methodology is appropriate, integrating SSI and ensuring user-centric data governance where data is secured on the user's device. This directly aligns with TRUSTCHAIN OC2's emphasis on championing privacy from the very design phase of data protocols.

- The approach to gain significant traction in machine learning and federated artificial intelligence is adequately presented.

- The current state-of-the-art is well-analyzed, and the novelty of this project is in the integration between the Decentralized Identifier (DID) and Verifiable Credentials (VC) within the multi-party computation (MPC) protocol. The innovation potential of this project, as it is set in smart city environments, is potentially huge.

- The proposed technical approach is credible as it is based on the proposer's experience with decentralized network protocols. Moreover, the technical approach is clear and achievable. The research group has made significant contributions to network protocol design, blockchain networks, and wireless sensor networks, as evidenced by their published research works.

Weaknesses:

- The proposed architecture is missing details.

- The technical details (methods and tools) are not sufficiently explained.

- The final evaluation and demonstration that will be part of the pilot are not sufficiently presented.

Criterion 2 - Expected impact and Value for Money	Score: 4
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The planned research will significantly contribute to the overall goal of TRUSTCHAIN by being set in smart cities and developing a new decentralized privacy-preserving technology.

- The need to manage private data in smart city scenarios is vast. Hence, the proposed solution addresses these needs.

- The proposed solution is based on DIDs and VCs and will credibly contribute to an ecosystem of decentralized identity management solutions. The new protocol can be used beyond the smart city scenario in any context.

- The planned research will credibly have a global impact based on existing standards, e.g. W3C (DIDs) and protocols.

- A particular focus is put on privacy preservation, through the innovative MPC protocol. The solution, therefore, complies with relevant regulations and standards related to private data management.

- The strategy to disseminate and exploit the new knowledge generated by action is appropriate. Testing within real-world environments/networks is foreseen, which is commendable.

- The strategy for targeting peers (scientific, industry, other actors, professional organizations, and policymakers) and the wider community (potential end users) is clear, consistent, and appropriate. Letter of support from the public sector and the industry are also provided to confirm their interest in utilizing the outcomes of the proposed solution.

- The business strategy and commercialization plan are clear and appropriate for the size of the project.

- The open-source license for the proposed solution allows its usage in large pilot scenarios once the project is finished.

Weaknesses:

- The software delivered at the end will allow devices to interconnect to their system. Hence, it is not clear whether the software will be indeed standalone or require connection to their system.

Criterion 3 - Project Implementation	**Score: 4**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan is well structured and appropriate to ensure that the research objectives and requested deliverables are achieved.

- The tasks and activities are clear and sufficiently detailed.

- The planned mobilized resources are appropriate concerning the proposed activity. The project will deliver a solution at TRL 7 that will be tested in operational settings for which sufficient resources are reserved.

- The quality and effectiveness of the management procedures, including risk and mitigation management measures, are clear.

- The applicant has the relevant expertise to conduct the project activities and has an excellent past track in research and innovation projects. The applicant has also published works in the domain concerned, particularly in protocols, blockchain and privacy preservation, which is appropriate.

- The integration of the solution in the overall TRUSTCHAIN ecosystem is clear and appropriate.

- The team collaborates closely with the Humans Interacting with Computers laboratory, which will aid the project team with any questions related to the applicable methodologies for enhanced human-centricity, gathering user requirements, feedback and preparation of user questionnaires.

Weaknesses:

- The overall use case is not sufficiently clear.

DUME - DECENTRALISED USER-CENTRIC MEDIA EXTENSION

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 062_2180698

Proposal acronym: DUME

Proposal title: Decentralised User-Centric Media Extension

Contact: nuno.feixa@logimade.pt

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 38,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The proposal's concept is highly innovative. It tackles the critical issue of centralized control over user-contributed data in contemporary platforms by extending the Solid Protocol for media dataset management and implementing user-centric features.

- Data privacy and user control are well considered.

- The proposal showcases deep understanding of the technical challenges involved in managing vast volumes of high-resolution photographs and associated metadata. The focus on swift and efficient data retrieval, rich metadata annotations, AI access control, and versioning mechanisms is commendable.

- The emphasis on user sovereignty and control over their media contributions is a strong point. This aligns with the current trend of giving users more ownership and control over their data, fostering trust and privacy.

Weaknesses:

- Challenges in data retrieval efficiency and AI model training integration are not sufficiently considered.

- The strategy in handling rich metadata and access control is weakly presented.

Criterion 2 - Expected impact and Value for Money	Score: 3,5
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The potential impact digital media platforms by enhancing user sovereignty is significant.

- Alignment with TRUSTCHAIN objectives in data privacy and decentralization appropriately documented.

- The focus on protocol development, AI integration, and user-centric features indicates a clear path to value creation.
- The expected impact, emphasizing the shift towards decentralization, user sovereignty, and control over data contributions is effectively described alignment with contemporary trends and user expectations is clearly presented.

Weaknesses:

- While the expected impact is clearly described, specific, measurable impact metrics and key performance indicators (KPIs) are not appropriately defined.
- Risks in market adoption and user acceptance in the decentralized digital paradigm are not fully considered.
- The economic viability and long-term sustainability are not sufficiently detailed.
- A more detailed cost-benefit analysis could benefit the proposal. While it outlines the expected impact, a comprehensive description of how TRUSTCHAIN funding will align with the anticipated returns and benefits is not appropriately documented.

Criterion 3 - Project Implementation	**Score: 4**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables	Threshold: 3
- Quality and effectiveness of the management procedures including risks and mitigation management	Weight: 30%
- Quality of the integration plan in the TRUSTCHAIN ecosystem	
- Excellence/Capacity of the applicant to deliver the proposed solution	
- Integration capacity in the TRUSTCHAIN ecosystem	

Strengths:

- A detailed technical plan, incorporating advanced tools like edge AI analytics, Zero-Knowledge Machine Learning (ZKML), and blockchain is presented.
- The appropriate consideration of complex technologies is demonstrated, particularly ZKML, indicates high level of technical expertise of the team which is competent in decentralized technologies and data management.

Weaknesses:

- While expressing interest in integration with TRUSTCHAIN, the feasibility and advantages of such integration, are not fully detailed.
- A more comprehensive risk management strategies is not appropriately considered. Potential risks in the practical implementation of the Solid Protocol on a large scale are insufficiently considered.

AURORA MINDS - EMPOWERING CHILDREN WITH ADHD THROUGH PRIVACY-PRESERVING DATA COLLECTION

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 067_2180054

Proposal acronym: AURORA MINDS

Proposal title: Empowering Children with ADHD Through Privacy-Preserving Data Collection

Contact: tmanos@dotsoft.gr

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 38,5   (Threshold: 30/50)

<table>
<tr>
<td>
Criterion 1 - Excellence and Innovation

- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context
- Credibility of the proposed methodology including the user centric approach
- Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective
</td>
<td>
Score: 4

Threshold: 4

Weight: 40%
</td>
</tr>
</table>

Strengths:

- A very important topic on how to support research and medical diagnostics at the example of ADHD is presented.
- The technical approach focuses on measures to ensure security and privacy for highly critical data (special PII acc. Art. 29 and 35 GDPR). It implements advanced use of machine learning and privacy technologies. In parallel it recognizes currently regulative developments like eIDAS 2.0 by adopting technologies like W3CVC, DID etc. on decentralized identity management.
- Research focused on special medical subject beyond the state of the art. approach combining technology and healthcare for ADHD is innovative. The proposed solution has a significant potential for advancement beyond current healthcare practices.

Weaknesses:

- Potential challenges in practical application and user acceptance are insufficiently considered.
- Potential for technology integration in healthcare contexts is insufficiently evaluated.

<table>
<tr>
<td>
Criterion 2 - Expected impact and Value for Money

- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant.
- Impact of the proposed innovation on the needs of the European and global markets.
- Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.
</td>
<td>
Score: 3,5

Threshold: 3

Weight: 30%
</td>
</tr>
</table>

Strengths:

- The proposal aligns well with privacy and security goals of TRUSTCHAIN.
- A high impact on global ADHD management practices is likely to happen as the request for security and privacy and proven data on medical subjects is increasing in Europe and beyond. Moreover, the proposed solution can credibly be extended to other areas.
- The regulative and strategic initiatives in Europe is well considered.

- Interaction with stakeholders are clearly described.
- A sufficient data management plan is presented.

Weaknesses:

- Uncertainties in market adoption and integration with existing healthcare systems is insufficiently considered.
- The applicant approach to global market penetration is inadequately detailed.
- The dissemination strategy is not carefully elaborated upon.

Criterion 3 - Project Implementation	**Score: 4**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- A detailed and well-structured plan ensuring objective achievement is depicted.
- The applicant has the relevant expertise to achieve the project goal.
- Weaknesses:
- Risk management strategies is not adequately detailed for unforeseen challenges.
- The integration of the proposed solution with the TRUSTCHAIN ecosystem is not fully clarified.

Weaknesses:

- None.

OIDC PRINCE - OPENID CONNECT WITH PRIVACY-ENHANCED CONSENTS

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 070_2180770

Proposal acronym: OIDC PRINCE

Proposal title: OpenID Connect with PRIvacy-eNhanced ConsEnts

Contact: bmsousa@dei.uc.pt

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 38,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The concept is clear and relevant and aligns well with TRUSTCHAIN objectives.

- The technical approach is credible, using innovative privacy assessment models.

- Advances beyond the current state of the art in identity and privacy management are clearly depicted and convincing.

- The innovation potential is high with practical applications and benefits.

Weaknesses:

- The ambitious integration of new privacy compliance methods are insufficiently considered in the methodology.

Criterion 2 - Expected impact and Value for Money	Score: 3,5
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- There is a strong alignment with TRUSTCHAIN goals and the contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions is fair.

- The proposed solution is likely to have a high impact on privacy standards in the market.

- The dissemination and exploitation strategies are comprehensively documented and appropriate.

Weaknesses:

- Interoperability with existing decentralized applications is insufficiently detailed.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan is well structured and comprehensive.

- The expertise of the team is strong and appropriately documented.

- The integration plan with TRUSTCHAIN is sufficiently explained.

Weaknesses:

- Some tasks details are insufficiently specified.

- The management and risk mitigation strategies are insufficiently detailed.

PECS - PRIVACY ENROOTED CAR SYSTEMS

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 071_2180650

Proposal acronym: PECS

Proposal title: Privacy Enrooted Car Systems

Contact: giamp@dmi.unict.it

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 37,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4,5
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- A clear and relevant concept, with credible technical and user-centred approaches are presented.
- aspects beyond the state of the art and innovation in products and business models are well documented.
- The alignment with other TRUSTCHAIN projects is pertinent.

Weaknesses:

- The users' engagement in the co-creation process lacks sufficient details.

Criterion 2 - Expected impact and Value for Money	Score: 3,5
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The contribution to TRUSTCHAIN's overall objectives and high potential impact on European and global markets is clearly presented.
- The achievable KPIs and a well-defined dissemination and exploitation strategy are appropriately defined.

Weaknesses:

- The marketing strategy and management of sensitive data are insufficiently detailed.
- The use of any kind of DLT is not appropriately considered which is a minor shortcoming.

Criterion 3 - Project Implementation	**Score: 3**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The roadmap for implementation and deployment is detailed and efficient, with a clear focus on achieving the project objectives.
- The applicant is well experienced in the research area ensuring that objectives are met.

Weaknesses:

- The risk and mitigation plans are lacking specific details.
- While the proposed solution has the potential to engage with other TRUTCHAIN projects, plan to achieve this is not comprehensively described.

EIDCMP- EIDAS COMPLIANT MEMBERSHIP PLATFORM

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 073_2179335

Proposal acronym: EIDCMP

Proposal title: eIDAS compliant membership platform

Contact: filipe.veiga@wallid.io

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 36,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 3,5**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The proposed solution focuses on member identity and member card issuance for professional, institutional and governmental associations. Focusing on association needs and requirements is a good target, if it is not covered by other TRUSTCHAIN projects.

- The proposed technical approach is credible.

- A User Centric Approach is credibly considered.

Weaknesses:

- The concept insufficiently addresses the objective of OC2, which is privacy-preserving data handling and sharing in compliance with regulation. Rather, it focuses on digital identity and verifiable credentials, which was the topic of OC1.

- The user involvement in the tests and pilot, such as number of users, method for selecting users, specific questions and feedback sought are insufficiently described.

Criterion 2 - Expected impact and Value for Money	**Score: 3,5**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- Measurable indicators that are relevant have been appropriately established.

- Although at a high-level, the dissemination and communication actions are sufficient, the dissemination and communication capabilities are reinforced with the background of the second partner - Portuguese Blockchain and Cryptocurrencies Association (APBC) - on training action and promotion events and overall dissemination is appropriate.

- Business model and sustainability issues are sufficiently addressed.

- The plan to comform with W3C standards together with eIDAS and GDPR is appropriate. Moreover, the solution will be built upon an existing EBSI wallet that is appropriate in the frame of TRUSTCHAIN.
- Legal and data protection matters are well considered.

Weaknesses:

- The added value for TRUSTCHAIN and Europe in general has not been convincingly discussed considering that digital wallets are already being developed in OC1 and by other large-scale projects.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The leading organisation Wallid has credibly presented its prior experience with development and integration activities related to digital identity, web3, PKI, ZKPs, and it has partners and customers from the government sector (infrastructure and middleware of the Portuguese government digital ID) and industry.
- The expertise and background of the two proposing organisations add credibility to achieving positive results in digital identity adoption, interoperability, and user data protection.
- The second partner - Portuguese Blockchain and Cryptocurrencies Association (APBC) - has experience on blockchain related training actions and promotion events since 2017.
- Risk management actions are described in sufficient detail for such a duration project.
- The existing system is at TRL 6 and by the end of the project it will reach TRL 9.
- The implementation plan is overall well-structured and broken into tasks with sufficient detail.

Weaknesses:

- A specific task for integration with the Trustchain ecosystem is not appropriately considered.

DID-IMP - DECENTRALIZED PUBLIC KEY INFRASTRUCTURE FOR DEFENDED IOT DATA MANAGEMENT AND PROCUREMENT

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 077_2180679

Proposal acronym: DID-IMP

Proposal title: Decentralized public key Infrastructure for Defended IoT data Management and Procurement

Contact: bmaisseu@gmail.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 36,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 3,5**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- Multiple of the TRUSTCHAIN OC2 objectives around the privacy and traceability of the identity credentials once shared with a third party are appropriately addressed and a trusted and open certificate issuance and revocation mechanism is credibly described.

Weaknesses:

- The innovation is not adequately demonstrated, since using a blockchain as a distributed PKI, and for certificate storage and revocation is not appropriately considered.
- -The privacy enhancing mechanisms, other than access control/revocation, which can be important since it involves IoT measurements that can contain private user information is not sufficiently detailed.
- The technical approach highlighting the difficulties and challenges to be addressed is not comprehensively evaluated.

Criterion 2 - Expected impact and Value for Money	**Score: 3,5**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions is convincing.
- Many aspects of the TRUSTCHAIN OC2 objectives are well addressed.
- The high impact in many fields is well demonstrated.

Weaknesses:

- The KPIs for the project success are inadequately presented.

- The strategy for targeting peers is insufficiently detailed.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The team demonstrates credibly its excellence and strength in the areas of work.
- A good overall implementation plan is presented.
- The deliverables are appropriately defined.

Weaknesses:

- The integration with the Trustchain ecosystem is not sufficiently discussed.
- Pilot details are not adequately documented.

GUEDHS - DATA GOVERNANCE AND USER PRIVACY ENVISIONING AN EHDS PILOT DEPLOYMENT

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 080_2180300

Proposal acronym: GUEDHS

Proposal title: Data Governance and User privacy envisioning an EHDS pilot deployment

Contact: anac.costa@promptlyhealth.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 38,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	**Score: 4**
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context	Threshold: 4
- Credibility of the proposed methodology including the user centric approach	Weight: 40%
- Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	

Strengths:

- The relevance to TRUSTCHAIN topics such as data provenance in federated learning in a health care environment is credibly presented.
- The approach is sufficiently detailed and involves the end users in managing consent and overall data governance.
- The contribution beyond the SOTA is credible as it aims at extending the capabilities of PySyft federated learning platform to include data provenance.
- The originality and novelty are appropriately demonstrated multiple of TRUSTCHAIN OC2 objectives by developing an open-source solution for multiparty data visiting under a secure, private, traceable and transparent environment are considered.
- Broad concepts that will foster innovation are addressed.

Weaknesses:

- The innovation potential does not appropriately some EU projects already very well advanced which present federated data sharing and federated learning with use cases related to the diagnosis and the management of cancer.

Criterion 2 - Expected impact and Value for Money	**Score: 4**
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant.	Threshold: 3
- Impact of the proposed innovation on the needs of the European and global markets.	Weight: 30%
- Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	

Strengths:

- The data-sharing tools such that privacy is ensured in a decentralized manner can have high impact on the intended application (tracking epidemics), which is important and timely and addresses real needs. The regulatory compliance as one of their targets is well considered.

- An impact to the European markets for health data by allowing transparent sharing of health data. To that end, several KPIs are explicitly defined.
- The dissemination strategy is reasonable and sufficiently addressed. Handling of sensitive data will comply to GDPR, HIPAA, ISO 27001 and other regulations. A business plan is described in broad terms.

Weaknesses:

- The subjects of interoperability and coexistence with other applications lacks more details.

Criterion 3 - Project Implementation	**Score: 3,5**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan is reasonable and feasible, given the set of mobilized resources. The tasks and activities are clear.
- Management and risk mitigation procedures are sufficiently considered.
- The consortium and the members involved form a capable mix of technical and health-specific personnel and experience on past and ongoing EU projects as well as in technical solutions in health data sharing.

Weaknesses:

- The details about how the work will be integrated to the TRUSTCHAIN framework are poorly presented, e.g., high level view of architecture.

PROVENAI - PROVENANCE IN AI

TRUSTCHAIN OPEN CALL 2
EVALUATION SUMMARY REPORT

Proposal number: 082_2180619

Proposal acronym: ProvenAI

Proposal title: Provenance in AI

Contact: vasilis.tsolis@cognitivplus.com

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 40   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The proposal is relevant to TRUSTCHAIN topics as it addresses provenance and privacy in AI data.
- The approach is credible and centers around content creators and users. End user pilots will be considered in the validation phase.
- The proposed solution is beyond SOTA as it plans to apply data provenance to individual semantically related segments. The innovation potential is clear, e.g., as content creators can seek fair compensation.

Weaknesses:

- There is insufficient information about previous achievement regarding the proposed solution, to clearly identify the contributions of the current proposal.
- The user co-creation process is not sufficiently detailed, e.g., the identification of use cases and plans to achieve user engagement already since the design phase.

Criterion 2 - Expected impact and Value for Money	Score: 4,5
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The proposal will clearly contribute toward TRUSTCHAIN's overall goal as it will provide SSIDs for data provenance in AI. This will be transparent for the users.
- The proposed solution is planned to comply to relevant regulations that is appropriate. The proposal solves a real-world problem, e.g., data tracking in the realm of AI that is pertinent.
- The proposed solution is likely to have a good market impact as it deals with intellectual property issues. An appropriate set of KPIs is identified. The dissemination plan is reasonable and adequate.
- The data management plan is adequately addressed.

Weaknesses:

- How trustworthy data governance and sharing will be achieved is not enough detailed.

Criterion 3 - Project Implementation	**Score: 3,5**
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The workplan and task breakdown is reasonable and appropriate to achieve project goals.
- Planned mobilised resources are appropriate in relation to the proposed activity.
- Adequate management and risk mitigations activities running through the entire project time are planned.
- The team members include both technical and legal expertise that clearly match with the project needs.
- The proposal refers to a specific OC1 project which can be useful in the proposed implementation demonstrating a willingness to integrate with TRUSTCHAIN ecosystem.

Weaknesses:

- Integration plan with TRUSTCHAIN ecosystem lacks sufficient details.

LED-UP - LEVEA'S ENHANCED DATA GOVERNANCE AND USER-CENTRIC PRIVACY IN DECENTRALIZED SYSTEMS

TRUSTCHAIN OPEN CALL 2

EVALUATION SUMMARY REPORT

Proposal number: 090_2180807

Proposal acronym: LED-UP

Proposal title: LEVEA's Enhanced Data Governance and User-Centric Privacy in Decentralized Systems

Contact: manuel.knott@yahoo.de

Overall Comments

The proposal is selected for funding.

Form information

SCORING

Scores are assigned on a scale from 0 to 5.

Interpretation of the score:

0 – The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 – Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 – Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 – Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 – Very good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 – Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Evaluation result

Total score: 41,5   (Threshold: 30/50)

Criterion 1 - Excellence and Innovation	Score: 4
- Clarity, pertinence, soundness of the proposed solution in the TRUSTCHAIN context - Credibility of the proposed methodology including the user centric approach - Extent that the proposed work is beyond the state of the art and demonstrate innovation potential in relation to TRUSTCHAIN objective	Threshold: 4 Weight: 40%

Strengths:

- The project has a clear and well-defined vision, and it is aligned with the goals of the TRUSTCHAIN Open Call #2.

- The proposal includes a strong user-centric approach.

- The proposed solution is innovative in its use of cutting-edge technologies such as decentralized digital identities, homomorphic encryption and zero-knowledge proofs to ensure data privacy and security.

- The Applicant's commitment to user research and feedback is evident in its planned approach to developing and deploying the proposed solution in refugee camps.

- The project has the support of a number of key stakeholders, including the UNHCR and EY- Parthenon DAO Team.

Weaknesses:

- The project is ambitious and complex, and it may be challenging to achieve all of its goals within the nine-month timeframe.

Criterion 2 - Expected impact and Value for Money	Score: 4,5
- Contribution to TRUSTCHAIN overall goal to create a portfolio of Next Generation protocols and ecosystem of decentralised identity management software solutions that is transparent to the users, interoperable, privacy aware and regulatory compliant. - Impact of the proposed innovation on the needs of the European and global markets. - Quality of the proposed measures to exploit and disseminate the project results (including management of IPR) and to manage research/sensitive data where relevant in the context of TRUSTCHAIN.	Threshold: 3 Weight: 30%

Strengths:

- The proposal's deployment in refugee camp has the potential to improve data management, resource allocation, and living condition, making a significant social and economic impact.

- The project is good value for money, with a reasonable budget for a complex project.

- The project has the support of a number of key stakeholders, who can help to maximise its impact.

- The privacy and security of refugees personal data are paramount. The team possesses relevant experience, having successfully deployed health applications in refugee camps in the past.

Weaknesses:

- No major weaknesses.

Criterion 3 - Project Implementation	Score: 4
- Quality and effectiveness of the work plan including extent to which the resources assigned to the work are in line with its objectives and deliverables - Quality and effectiveness of the management procedures including risks and mitigation management - Quality of the integration plan in the TRUSTCHAIN ecosystem - Excellence/Capacity of the applicant to deliver the proposed solution - Integration capacity in the TRUSTCHAIN ecosystem	Threshold: 3 Weight: 30%

Strengths:

- The work plan is well-structured with clear timeline for project milestones and deliverables.
- The management procedures including risks and mitigation management are comprehensive and appropriate.
- The experience of the applicant matches well with the needs of the solution development.

Weaknesses:

- The integration plan with the TRUSTCHAIN ecosystem lacks at this stage sufficient details.

ANNEX 4 - TRUSTCHAIN OC2 CONTRACT MODEL FOR THIRD PARTIES SELECTED

STANDARD RESEARCH CONTRACT

1.CONTRACTING PARTIES

The rights and obligations contained in this Funding Agreement derived from the TRUSTCHAIN Grant Agreement and Consortium Agreement.

This TRUSTCHAIN Funding Agreement for providing financial support to the Selected Third Party, hereinafter referred to as the "Agreement", is entered into by and between:

EUROPEAN DYNAMICS LUXEMBOURG SA (ED), established in rue Jean Engling 12, Luxembourg 1466, Luxembourg, VAT number: LU17535424, represented for the purposes of signing the Agreement by Mr. Konstantinos Velentzas, legal representative of ED, hereinafter referred to as "**Cascade Funding Partner**",

And

- *[if a legal entity]:*

[OFFICIAL NAME OF THE SELECTED THIRD PARTY (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

- *[if a Team of Natural persons]:*

[FIRST AND LAST NAME OF THE NATURAL PERSON 1],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

[FIRST AND LAST NAME OF THE OF THE NATURAL PERSON 2],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

[FIRST AND LAST NAME OF THE OF THE NATURAL PERSON 3],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

- [if a Consortium of legal entities]:

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 1 (Acronym)], Project Manager and Authorized representative of the consortium,

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 2 (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 2 (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

Referred to as "**Selected Third Party**",

Hereinafter sometimes individually or collectively referred to as "**Party**" or "**Parties**".

Whereas European Dynamics and its partners according to the TRUSTCHAIN Consortium Agreement, (hereinafter sometimes collectively referred as the "**TRUSTCHAIN Beneficiaries**" and individually and alternatively referred as a "**TRUSTCHAIN Beneficiary**") participate to the H2020 project entitled "**TRUSTCHAIN - Fostering a Human-Centred, Trustworthy and Sustainable Internet**" (hereinafter the "TRUSTCHAIN Project").

Whereas the TRUSTCHAIN Beneficiaries entered into a Grant Agreement N° 101093274 with the European Commission (the "**Grant Agreement**" or "GA") and signed together in 2023 a Consortium Agreement with respect to the TRUSTCHAIN Project (the "**Consortium Agreement**" or "**CA**").

Whereas the TRUSTCHAIN Project involves financial support to selected third parties through a cascade funding scheme (hereinafter "**Cascade Funding**").

Whereas further to an open call for specific research as described in Annex 1 "**TRUSTCHAIN Specific Contract**", the Selected Third Party has been selected to implement such research.

Whereas the Selected Third Party will be in charge of the implementation of such research with also the participation of the TRUSTCHAIN Beneficiaries identified in Annex 1 "**TRUSTCHAIN Specific Contract**".

Whereas the Cascade Funding Partner is willing to provide technical and financial support to the Selected Third Party for the implementation of such Research and the Selected Third Party is willing to receive such funding under the terms and conditions of this Agreement.

Whereas in accordance with the Grant Agreement and the Consortium Agreement, the Cascade Funding Partner shall sign an agreement with the Selected Third Party compliant with the GA and CA, after validation by the other Participating Partners.

Whereas the Cascade Funding Partner is responsible for the execution of this Agreement with the Selected Third Party and for the monitoring of the Research.

Now therefore it has been agreed as follows:

2. DEFINITIONS

Words beginning with a capital letter shall have the meaning defined in the preamble of the Agreement or in this Section:

o **Access Rights** means rights to use Results or Background in accordance with the stipulations of the H2020 General MGA – Multi and under the terms and conditions laid down in this Agreement.

o An **Affiliated Entity** of a TRUSTCHAIN Beneficiary means any legal entity shown in Attachment 4 to the CA, directly or indirectly Controlling, Controlled by, or under common Control with that Party, for so long as such Control lasts.

o **Agreement** means this Funding Agreement, together with its Annexes.

o **Background** means any and all, data, information, know-how– whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights – listed in Annex 1 "TRUSTCHAIN Specific Contract" – that is Needed to implement the Project or exploit the Results and that is:

- owned or controlled by a Party or a TRUSTCHAIN Beneficiary prior to the date of signature of the Specific Contract (Annex 1); or
- developed or acquired by a Party or a TRUSTCHAIN Beneficiary independently from the work in the Research even if in parallel with the performance of the Research, but solely to the extent that such data, information, know-how and/or intellectual property rights are introduced into the Industrial Experiment by the owning Party.

- o **Controlled Licence Terms** means terms in any licence that require that the use, copying, modification and/or distribution of Software or another work ("Work") and/or of any work that is a modified version of or is a derivative work of such Work (in each case, "Derivative Work") be subject, in whole or in part, to one or more of the following:
  - (where the Work or Derivative Work is Software) that the Source Code or other formats preferred for modification be made available as of right to any third party on request, whether royalty-free or not;
  - that permission to create modified versions or derivative works of the Work or Derivative Work be granted to any third party;
  - that a royalty-free licence relating to the Work or Derivative Work be granted to any third party.

  For the avoidance of doubt, any Software licence that merely permits (but does not require any of) the things mentioned in a) to c) is not under Controlled Licence Terms (and so is under an Uncontrolled Licence).

- o **Exploitation** or **Exploit** means the use of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities;

- o **Financial Support** means the cash element of the financial support to be given by the Cascade Funding Partner to the Selected Third Party for the implementation of the Industrial Experiment as detailed in Annex 1 "TRUSTCHAIN Specific Contract".

- o **Research** means the research detailed in Annex 1 "TRUSTCHAIN Specific Contract" to be carried out by TRUSTCHAIN Beneficiaries and the Selected Third Party.

- o **Result** means the outcome of the Research, which may entail the generation of Works protected by intellectual property rights.

- o **Participating Partners** means the entities and organisations participating in the Research, as listed in Annex 1.

3. CONDITIONS FROM THE GRANT AGREEMENT AND THE CONSORTIUM AGREEMENT REFLECTED IN THE AGREEMENT

The Cascade Funding Partner receives funding from the European Commission for organizing the Research. Under the TRUSTCHAIN Grant Agreement or the Consortium Agreement, some of the obligations have to be imposed on the Selected Third Party. Those obligations are reflected in this Agreement. The specific obligations that the Selected Third Party must ensure are described in the Multi-Beneficiary General Model Grant Agreement (H2020 General MGA – Multi), available at: http://ec.europa.eu/research/participants/data/ref/h2020/mga/gga/h2020-mga-gga-multi_en.pdf, in articles 6, 22, 23, 35, 36, 38 and 46. These articles are part of the Agreement, by reference only.

The Selected Third Party acknowledges and agrees that these obligations comprised in this Agreement including Annex 1 and in the Multi-Beneficiary General Model are fully applicable to it and shall do everything that is necessary to comply with these obligations, it being understood that the Selected Third Party is only bound by this Agreement and not by the GA or CA.

4. TERMS AND CONDITIONS FOR THE FINANCIAL SUPPORT

4.1 The Selected Third Party shall take part in the Research in accordance with the state of the art. The Selected Third Party shall carry out the tasks according to the schedule set forth in Annex 1 "TRUSTCHAIN Specific Contract" at the latest and shall report to the Cascade Funding Partner on the activities' progress in regular intervals as indicated in Annex 1 "TRUSTCHAIN Specific Contract".

4.2 The Selected Third Party shall attend all group and individual coaching and mentoring sessions provided by the TRUSTCHAIN Beneficiaries or the Cascade Funding Partner over the course of the Research.

4.3 The Cascade Funding Partner shall give Financial Support for the Research carried out by the Selected Third Party, within the limits and in accordance with the Guide for Applicants and schedule of payments specified in Annex 1 "TRUSTCHAIN Specific Contract" and always subject to:

o A favourable resolution by the evaluators and coaches responsible for assessing the Project in each of the stages (a set of deliverables and KPIs will be set-up by coaches and sub-grantees and their achievement monitored during the projects' execution)

o The availability of funds in TRUSTCHAIN bank account during the relevant payment period

o The prior written notice to the Selected Third Party of the date and amount to be transferred to its bank account

o Payments to the Selected Third Party will be made by the Cascade Funding Partner. In particular:

- The Cascade Funding Partner reserves the right to withhold the payments in case the Selected Third Party does not fulfil its obligations and tasks as per the Guide for Applicant.

- Banking and transaction costs related to the handling of any financial resources made available to the Selected Third Party by the Cascade Funding Partner shall be covered by the Selected Third Party.

- Payments will be released no later than fifteen (15) calendar days after the notification by the Cascade Funding Partner.

- The Selected Third Party is responsible for complying with any tax and legal obligations that might be attached to this financial contribution.

4.5 A written payment request must be sent by the Selected Third Party to the Cascade Funding Partner after reception of the favourable resolution by the evaluators and coaches.

4.6 The Selected Third Party shall complete in a comprehensive manner Annex 4 "Selected third party financial information"to the Agreement and shall notify any changes to the Cascade Funding Partner as soon as it has occurred. The Cascade Funding Partner shall not in any case be liable for any late payment incurred by a change in the financial identification of the Selected Third Party.

5. LIABILITY

5.1 The Selected Third Party shall comply with all applicable laws, rules and regulations, including, but not limited to safety, security, welfare, social security and fiscal laws, rules and regulations.

5.2 Selected Third Party shall not be entitled to act or to make legally binding declarations on behalf of the Cascade Funding Partner or any other TRUSTCHAIN Beneficiary and shall indemnify all of the latter from any third-party claim resulting from a breach of these obligations.

5.3 The contractual liability of the Cascade Funding Partner under this Agreement shall in any case be limited to the amount of the Financial Support provided to the Selected Third Party hereunder and the Cascade Funding Partner. The Cascade Funding Partner shall not in any case be liable for any indirect or consequential damages such as:

o loss of profits, interest, savings, shelf-space, production and business opportunities.

o lost contracts, goodwill, and anticipated savings;

o loss of or damage to reputation or to data;

o costs of recall of products; or

o any other type of indirect, incidental, punitive, special or consequential loss or damage.

5.4 This limitation of liability shall not apply in cases of wilful act or gross negligence.

5.5 The Selected Third Party shall fully and exclusively bear the risks in connection with the Research for which Financial Support is granted by the Cascade Funding Partner. The Selected Third Party shall indemnify the

TRUSTCHAIN Beneficiaries and the Cascade Funding Partner for all damages, penalties, costs and expenses which the TRUSTCHAIN Beneficiaries or the Cascade Funding Partner as a result thereof would incur or have to pay to the European Commission or any third parties with respect to such Research financially supported and/or for any damage in general which the TRUSTCHAIN Beneficiaries or the Cascade Funding Partner incur as a result thereof. In addition, should the European Commission have a right to recover against the Cascade Funding Partner or another TRUSTCHAIN Beneficiary regarding the Financial Support granted under this Agreement, the Selected Third Party shall pay the sums in question in the terms and the date specified by the Cascade Funding Partner. Moreover, the Selected Third Party shall indemnify and hold the TRUSTCHAIN Beneficiaries and the Cascade Funding Partner, their respective officers, directors, employees and agents harmless from and against all repayments, loss, liability, costs, charges, claims or damages that result from or arising out of any such recovery action by the European Commission.

5.6 In respect of any information or materials (including Results and Background) supplied by one Party to another Party or to a TRUSTCHAIN Beneficiary, or by a TRUSTCHAIN Beneficiary involved in the applicable Research to a Party, no warranty or representation of any kind is made, given or implied as to the sufficiency, accuracy or fitness for purpose nor as to the absence of any infringement of any proprietary rights of third parties.

Therefore,

o   the recipient shall in all cases be entirely and solely liable for the use to which it puts such information and materials (including Results and Background), and

o   there is no liability in case of infringement of proprietary rights of a third party resulting from any Access Rights.

6. INTELLECTUAL PROPERTY RIGHTS POLICY

The Selected Third Party acknowledges the terms of the "Intellectual Property Rights Policy" defined hereinafter. The Selected Third Party agrees that it will comply with the TRUSTCHAIN Intellectual Property Rights Policy to ensure that the Cascade Funding Partner will always be able to comply with such terms towards the other TRUSTCHAIN Beneficiaries.

"**Intellectual Property**" means the Background and the Results (foreground) generated in the project.

The background of the third party(ies) is described in Annex 1.1 "TRUSTCHAIN Specific Contract" Article 1.

The background of TRUSTCHAIN partners is described in Annex 1.4 "TRUSTCHAIN consortium background".

6.1. GENERAL PRINCIPLE REGARDING OWNERSHIP

Results are owned by the Party or by the TRUSTCHAIN Beneficiary that generates them.

6.2. JOINT RESULTS

As requested in the Consortium Agreement signed between the TRUSTCHAIN Beneficiaries and the Cascade Funding Partner, all Results generated in the course of the Research within the framework of the project by the Selected Third Party with one or several TRUSTCHAIN Beneficiaries shall be jointly owned between the Selected Third Party and the respective TRUSTCHAIN Beneficiaries.

One or more TRUSTCHAIN Beneficiaries may contribute ideas, knowhow, concepts and other insights (together referred to as "Input") which, while not in themselves protected under intellectual property rights, are conducive to the generation of the Results. The TRUSTCHAIN Beneficiaries and the Selected Third Party agree that any Results which

have been generated on the basis of the Input, shall be construed as Results jointly owned by the TRUSTCHAIN Beneficiary (or -ies) which provided the Input and the Selected Third Party which generated the Result.

Where such joint Result is covered by intellectual property rights, the joint owners shall execute a joint ownership agreement regarding the allocation and the terms and conditions of Exploitation of the joint Results as soon as possible and before any industrial or commercial Exploitation.

Unless otherwise agreed:

o   each of the joint owners shall be entitled to use their jointly owned Results for internal non-commercial research activities and educational purposes on a royalty-free basis, and without requiring the prior consent of the other joint owner(s), and

o   each of the joint owners shall be entitled to otherwise exploit the jointly owned Results, including by granting non-exclusive licences to third parties (without any right to sub-license), if the other joint owners are given:

> (a) at least 45 calendar days advance notice; and

> (b) fair and reasonable conditions compensation taking into account the specific circumstances of the request for access, for example the actual

> or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged.

The joint owners shall agree on all protection measures and the division of related cost in advance.

6.3. ACCESS RIGHTS

6.3.1 The Selected Third Party endeavours to detail in Annex 1.1 "TRUSTCHAIN Specific Contract" Article 1 the Intellectual Property under Controlled License Terms that will be used in the Research.

During the Research, the intended introduction of Intellectual Property (including, but not limited to Software) under Controlled Licence Terms in the Research requires the prior approval of the Cascade Funding Partner and of the Participating Parties to implement such introduction.

6.3.2 Due to provisions of the Consortium Agreement signed between the TRUSTCHAIN Beneficiaries, Access Rights to Background and Results may be requested by the Selected Third Party from a Participating Partner only in the following case and if the following conditions are fulfilled:

* Selected Third Parties have Access Rights to Background and Results if and when such Access Rights have been agreed upon on a case-by-case basis in a separate written agreement between the Selected Third Party and the TRUSTCHAIN Beneficiary/ies concerned. Such separate agreement shall not affect any legitimate right of another TRUSTCHAIN Beneficiary nor violate any of the provisions as set out in the GA and/or CA. The separate agreement shall ensure that the other TRUSTCHAIN Beneficiaries have access to the Background and Results of the Selected Third Parties if needed for the Implementation of the Project or Exploitation of its own Results.
* Selected Third Parties which obtain Access Rights in return shall fulfil confidentiality obligations at least as stringent as the obligations stated in the Consortium Agreement to be arranged in a separate confidentiality agreement between the Selected Third Parties and the TRUSTCHAIN Beneficiaries concerned.
* Access Rights may be requested by the Selected Third Party up to twelve (12) months after the end of the Research.

6.3.3 The Selected Third Party shall grant Access Rights on its Background and/or Results to the TRUSTCHAIN Beneficiaries as far as such Background and/or Results are needed for implementation of the Research and/or implementation of the TRUSTCHAIN Project, and/or exploitation of the TRUSTCHAIN Beneficiaries' Results.

6.3.3.1 Where any TRUSTCHAIN Beneficiary has Access Rights on the Selected Third Party's Results and/or Background for implementation of the Research, such Access Rights shall be granted on a royalty-free basis.

6.3.3.2 Where Access Rights on Results and/or Background of the Selected Third Party are needed by TRUSTCHAIN Beneficiaries in order to implement the TRUSTCHAIN Project:

o Access Rights to the Selected Third Party's Results shall be granted on a royalty-free basis and shall comprise the right to sublicense such Results to the other selected third parties participating in the TRUSTCHAIN Project;

o Access Rights to the Selected Third Party's Background shall be granted only if such Background is needed to use the Selected Third Party's Results to implement the TRUSTCHAIN Project. Such Access Rights shall be granted on a royalty-free basis, and shall comprise the right to sublicense such Background to the other selected third parties participating in the research under the TRUSTCHAIN Project:

o as far as these other selected third parties need to have access to such Background to use the Selected Third Party's Results to carry out their own research under the TRUSTCHAIN Project; and

o if no major interest opposes.

6.3.3.3 Where Access Rights on the Selected Third Party's Results and/or Background are needed by TRUSTCHAIN Beneficiaries in order to exploit their Results, the conditions on which Access Rights will be granted shall be negotiated between the Selected Third Party and the TRUSTCHAIN Beneficiary concerned and agreed in a separate written agreement.

Access Rights may be requested by the TRUSTCHAIN Beneficiaries up to twelve (12) months after the end of the Research.

6.4. OPEN SOURCE

Without detriment to the provisions stated in article 6.1, any Result (including documentation, source code and application programming interfaces), shall be published with a permissive open-source licence (e.g., Apache v2.0 or equivalent) within the TRUSTCHAIN file repository (ies).

If part of the Result is delivered under a proprietary license it shall be duly identified and justified in advance by the Third Party. TRUSTCHAIN beneficiaries will have the right to access to it for evaluating the progress of activities during the TRUSTCHAIN project. Non-disclosure of these proprietary result shall be ensured.

6.5. EXPLOITATION OF THE RESULTS

Selected Third Parties are required for up to 4 years after the Research to use their best efforts to exploit their Results directly or to have them exploited indirectly by another entity, in particular through transfer or licensing. The Selected Third Party can request the TRUSTCHAIN Beneficiaries to assist in the exploitation of the Results. To this end, the TRUSTCHAIN Beneficiaries will implement during the TRUSTCHAIN Project an exploitation mechanism based on tailor-made cryptocurrency. During the course of the TRUSTCHAIN Project such assistance will be provided free of charge, whereas TRUSTCHAIN Beneficiaries shall have the right to charge a reasonable fee for their assistance with the exploitation after the TRUSTCHAIN Project's end.

If, despite the Selected Third Party's best efforts, the Results are not exploited within one year after the end of the Research, the Selected Third Party must request the TRUSTCHAIN Beneficiaries to assist in the exploitation. The TRUSTCHAIN Beneficiaries shall then use best efforts to assist in such exploitation.

7. CONFIDENTIALITY

7.1 All information in whatever form or mode of communication, which is disclosed by a Party or an TRUSTCHAIN Beneficiary (the "Disclosing Partner") to the other Party or to any TRUSTCHAIN Beneficiary (the "Recipient") in connection with the Project during its implementation and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 15 calendar days from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information".

7.2 The Recipients hereby undertake for a period of four (4) years after the end of the Research:

o   not to use Confidential Information otherwise than for the purpose for which it was disclosed;

o   not to disclose Confidential Information to any third party (other than to its Affiliated Entities and Subcontractors) without the prior written consent by the Disclosing Partner, wherein the Recipient must ensure that an arrangement is in place prior to such disclosure that subjects the Affiliated Entities and/or Subcontractors to provisions at least as strict as provided in this Section 10;

o   to ensure that internal distribution of Confidential Information by a Recipient, its Affiliated Entities, Subcontractors shall take place on a strict need-to-know basis; and

o   to return to the Disclosing Partner, or destroy, on request all Confidential Information that has been disclosed to the Recipients including all copies thereof and to delete all information stored in a machine readable form to the extent practically possible. The Recipients may keep a copy to the extent it is required to keep, archive or store such Confidential Information because of compliance with applicable laws and regulations or for the proof of on-going obligations provided that the Recipient comply with the confidentiality obligations herein contained with respect to such copy for as long as the copy is retained.

7.3 The recipients shall be responsible for the fulfilment of the above obligations on the part of their employees, its Affiliated Entities or third parties involved in the Project having access to Confidential Information pursuant to this Section and shall ensure that they remain so obliged, as far as legally possible, during and after the end of the Project and/or after the termination of the contractual relationship with the employee or third party.

7.4 The above shall not apply for disclosure or use of Confidential Information, if and in so far as the Recipient can show that:

o   the Confidential Information has become or becomes publicly available by means other than a breach of the Recipient's confidentiality obligations;

o   the Disclosing Partner subsequently informs the Recipient that the Confidential Information is no longer confidential;

o   the Confidential Information is communicated to the Recipient without any obligation of confidentiality by a third party who is to the best knowledge of the Recipient in lawful possession thereof and under no obligation of confidentiality to the Disclosing Partner;

o   the disclosure or communication of the Confidential Information is foreseen by provisions of the Multi-Beneficiary General Model Grant Agreement;

o   the Confidential Information, at any time, was developed by the Recipient completely independently of any such disclosure by the Disclosing Partner;

o   the Confidential Information was already known to the Recipient prior to disclosure without any confidentiality obligation to the Disclosing Partner, or

o   the Recipient is required to disclose the Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order.

7.5 The Recipient shall apply the same degree of care with regard to the Confidential Information disclosed within the scope of the Project as with its own confidential and/or proprietary information, but in no case less than reasonable care.

7.6 Each Party shall promptly advise the other Party or the concerned TRUSTCHAIN Beneficiary in writing of any unauthorised disclosure, misappropriation or misuse of Confidential Information after it becomes aware of such unauthorised disclosure, misappropriation or misuse.

7.7 If any Party becomes aware that it will be required, or is likely to be required, to disclose Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order, it shall, to the extent it is lawfully able to do so, prior to any such disclosure:

o   notify the Disclosing Partner, and

o   comply with the Disclosing Partner's reasonable instructions to protect the confidentiality of the information.

8. DISSEMINATION

o   Each Party agrees that any dissemination activity (including publications, presentations, contributions to any standards organisation or open-source code) by the Selected Third Party is subject to the prior written approval of the other Participating Partners and upon proper citation of the TRUSTCHAIN project (cf. paragraph 6.4).

o   By 30 days from its dissemination request the Selected Third Party will receive the approval to disseminate or the indication of how/when to proceed in the requested dissemination activity. The Selected Third Party has to be aware that a premature dissemination activity could negatively affect IPRs, as patent applications. Moreover, dissemination activities should be compliant with suggested EU commission guidelines about open access publishing.

o   The Selected Third Party and the other TRUSTCHAIN Beneficiaries are entitled to include the main issues and information regarding the Research in their reporting towards the European Commission, subject to prior written notification to the Cascade Funding Partner.

o   Unless explicitly agreed by the Cascade Funding Partner, any dissemination of results (in any form, including electronic) must display the NGI emblem and the following text: "This project has received funding from the European Union's Horizon 2020 research and innovation program through the NGI TRUSTCHAIN program under cascade funding agreement No. 101093274."

9. CHECKS AND AUDITS

9.1 The Selected Third Party undertakes to provide any detailed information, including information in electronic format, requested by the European Commission or by any other outside body authorised by the European Commission to check that the Research and the provisions of this Agreement are being properly implemented.

9.2 The Selected Third Party shall keep at the European Commission disposal all original documents, especially accounting and tax records, or, in exceptional and duly justified cases, certified copies of original documents relating to the Agreement, stored on any appropriate medium that ensures their integrity in accordance with the applicable national legislation, for a period of five years from the date of payment of the balance specified in the grant agreements.

9.3 The Selected Third Party agrees that the European Commission may have an audit of the use made of the Financial Support carried out either directly by the European Commission staff or by any other outside body authorised to do so on its behalf. Such audits may be carried out throughout the period of implementation of the Agreement until the balance is paid and for a period of five years from the date of payment of the balance. Where appropriate, the audit findings may lead to recovery decisions by the European Commission.

9.4 The Selected Third Party undertakes to allow European Commission staff and outside personnel authorised by the European Commission the appropriate right of access to the sites and premises of the Selected Third Party and to all the information, including information in electronic format, needed in order to conduct such audits.

9.5 In accordance with Union legislation, the European Commission, the European Anti-Fraud Office (OLAF) and the European Court of Auditors (ECA) may carry out spot checks and inspections of the documents of the Selected Third Party, and of any recipient of Cascade Finding, including at the premises of the Selected Third Party, in accordance with the procedures laid down by Union law for the protection of the financial interests of the Union against fraud and other irregularities. Where appropriate, the inspection findings may lead to recovery decisions by the European Commission. The Articles 22 and 23 of the Multi-Beneficiary General Model Grant Agreement, also apply to the Selected Third Party.

10. EXPLOITATION

Without prejudice to clause 6.5 above, as also mentioned in the previous chapter, the EU Commission gives high priority that results of RIA projects generate sustainable business. Most importantly, TRUSTCHAIN aims towards the development of a sustainable blockchain ecosystem. Hence, before the end of this subproject, an exploitation agreement will be signed between the TRUSTCHAIN consortium and the third party about common exploitation activities of the subproject results, subject to a negotiation process.

11. TERMINATION

11.1 The Cascade Funding Partner can terminate this Agreement with immediate effect through written notice to the Selected Third Party and to the other Participating Partners:

o   if the Selected Third Party is in breach of any of its material obligations under this Agreement, which breach is not remediable, or, if remediable, has not been remedied within thirty (30) days after written notice to that effect from the party not in breach,

o   if, to the extent permitted by law, the Selected Third Party is declared bankrupt, is being wound up, is having its affairs administered by the courts, has entered into an arrangement with its creditors, has suspended business activities, or is the subject of any other similar proceeding concerning those matters, or

o   if the Selected Third Party is subject to an Event of Force Majeure, which prevents the Selected Third Party from correct performance of its obligations hereunder and such circumstances have lasted or can reasonably be expected to last more than 3 months.

11.2 Access Rights granted to the Selected Third Party shall cease immediately upon the effective date of termination.

12. CONCLUDING CONDITIONS

12.1 The Parties will not sign Annex 1, and the terms of this Agreement (for the sake of clarity this includes Annex 1) will not be effective, until the Cascade Funding Partner has received written confirmation from each Participating Partner that it agrees to their content. This written confirmation can be given by each Participating Partner sending by email or facsimile to the Cascade Funding Partner.

Once each written confirmation is given by each Participating Platform Partner, any ancillary agreements, amendments, additions or modifications to this Agreement shall be made in writing and signed by the Parties but will only become effective after the Cascade Funding Partner has received written confirmation from each Participating Partner that it agrees to their content, such written confirmation to be given in the manner set out at the above paragraph.

12.2 The Selected Third Party's consistent level in its respective field of expertise played a key role in the selection of the Selected Third Parties to implement the Research. Any total or partial transfer of provisions and the rights and duties it entails in the prior formal approval of all signatories.

12.3 Any subcontract by the Selected Third Party concerning some of its tasks under this Agreement requires the prior written consent of the Cascade Funding Partner and does not affect its own obligations resulting from this Agreement. The Selected Third Party shall secure that the subcontractor will comply with all obligations – especially coming from the Multi-Beneficiary General Model Grant Agreement, and with regard to confidentiality – resulting from this Agreement and that the results attained by the subcontractor will be available in accordance with Section 5.

12.4 The Agreement will enter into force on the date of the last signature by the Parties.

12.5 This Funding Agreement shall continue in full force and effect until complete fulfilment of all obligations undertaken by the Parties. However, this Funding Agreement or the participation of one or more Parties to it may be terminated in accordance with the terms of this Funding Agreement.

12.6 Parties that fail to meet reporting/mandatory activities deadlines must be aware that their non-respect of reporting/mandatory activities deadlines may lead to their costs being considered zero for the corresponding period and they will be excluded from the respective payment.

12.7 In the event that a breach by a Party of its obligation under this contract is identified by the Cascade funding Partner such as improper implementation of the research, the Cascade funding Partner will formally notify the considered Party to remedy this breach. If it is not remedied in reasonable time, the Cascade funding Partner may decide to declare the Party to be a defaulting Party and, on the consequences, thereof which may include termination of its participation and reimbursement of all or part of the financial provision.

12.8 In the event of the termination of the contract by a Party before its legal termination as set in the Annex 1, the Cascade funding Partner may decide to declare the Party to be a defaulting Party and, on the consequences, thereof which may include reimbursement of all or part of the financial provision.

12.9 If any provision of this Agreement is determined to be illegal or in conflict with the applicable law, the validity of the remaining provisions shall not be affected. The ineffective provision shall be replaced by an effective provision which is economically equivalent. The same shall apply in case of a gap.

12.10 This Agreement shall be governed by and construed in accordance with the laws of Belgium.

12.11 Any disagreement or dispute which may arise in connection with this Agreement and which the Parties are unable to settle by mutual agreement will be brought before the courts of Brussel, Belgium.

Done in two originals, one for each Party.

On behalf of the Cascade Funding Partner: European Dynamics Luxembourg SA	On behalf of the Selected Third Party (Authorized representative in case of Team/Consortium): [Complete]
Signature of the authorized representative:	Signature of Selected Third Party (Authorized representative in case of Team/Consortium):

Name:	Name: [Complete]
Title:	Title: [Complete]
Date:	Date: [Complete]

ANNEX 1.1 – TRUSTCHAIN SPECIFIC CONTRACT

This TRUSTCHAIN Specific Contract for implementation of Research by the Selected Third Party, hereinafter referred to as the "Specific Contract", is entered into by and between:

EUROPEAN DYNAMICS LUXEMBOURG (ED), established in rue Jean Engling 12, Luxembourg 1466, Luxembourg, VAT number: LU17535424, represented for the purposes of signing the Agreement by Mr. Konstantinos Velentzas, legal representative of ED, hereinafter referred to as "**Cascade Funding Partner**",

and

- [if a legal entity]:

[OFFICIAL NAME OF THE SELECTED THIRD PARTY (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

- [if a Team of Natural persons]:

[FIRST AND LAST NAME OF THE NATURAL PERSON 1],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

FIRST AND LAST NAME OF THE OF THE NATURAL PERSON 2],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

[FIRST AND LAST NAME OF THE OF THE NATURAL PERSON 3],

ID card/Passport Number: [Number]

Date of issue: [Date]

Taxpayer identification Number: [Number]

Legal address: [ADDRESS and COUNTRY]

- [if a Consortium of legal entities]:

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 1 (Acronym)], Project Manager and Authorized representative of the consortium,

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 2 (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

[OFFICIAL NAME OF THE SELECTED THIRD PARTY 2 (Acronym)],

VAT Number: [VAT]

Legal Status: [XXX]

PIC Number: [PIC NUMBER]

Name of the legal signatory: [Name]

Legal office address: [ADDRESS and COUNTRY]

Hereinafter referred to as "**Selected Third Party**";

Hereinafter sometimes individually or collectively referred to as "Party" or "Parties".

Whereas the Cascade Funding Partner and the Selected Third Party have agreed the main terms and conditions to implement the Research in the course of the TRUSTCHAIN Project by signing the Standard Research Contract to which this Specific Contract is annexed.

Now therefore it has been agreed as follows:

1.ENTRY INTO FORCE

The specific contract shall enter into force on the day of its signature by the last Contracting Party as a rule of thumbs no more than 15 days after the announcement of the selection. The Cascade Funding Project Manager/ Authorized representative of the consortium shall sign this contract, only after all of the following documents have been received from the Selected Third Party:

- [if a legal entity]:

-The original signed Declaration of Honour (as given in Annex 6 of the Standard Research Contract) by the Project Manager/Authorized representative;

-The SME Declaration form (as given in Annex 7 of the Standard Research Contract);

-The copy of the original Extract of SME;

-The Proof of VAT;

-The Bank Information Form (as given in Annex 3 of this Contract).

-The Estimated budget for the action (as given in Annex 2 of this Contract)

- [if a Team of Natural persons]:

-The original signed Declaration of Honour (as given in Annex 6 of the Standard Research Contract) by the Project Manager/Authorized representative;

-Copy of ID-card or Passport of the legal representative(s) of the Team;

-Bank Information Form (as given in Annex 3 of this Contract).

-Estimated budget for the action (as given in Annex 2 of this Contract)

-A copy of the signed team agreement with the denomination of the Authorized representative.

- [if a Consortium of legal entities]:

-The original signed Declaration of Honour (as given in Annex 6 of the Standard Research Contract) by the Project Manager/Authorized representative;

-SME Declaration form (as given in Annex 7 of the Standard Research Contract) if applicable;

-Copy of the original Extract of SME if applicable;

-Proof of VAT;

-Bank Information Form (as given in Annex 3 of this Contract).

-Estimated budget for the action (as given in Annex 3 of this Contract)

-If a group of legal entities, copy of the signed consortium agreement with the denomination of the Authorized representative.

2. TERMS AND CONDITIONS FOR THE RESEARCH

The Selected Third Party shall implement the Research in accordance with the following:

Description of the Research	
Acronym	[Complete]
Full Title	[Complete]
TRUSTCHAIN call identification	TRUSTCHAIN Open Call 2
Starting date of the Research:	[Complete]
Duration of the Research:	9 months
Date of selection of the Selected Third Party(ies)	[Complete]

Participating Partners involved in the Research	
Cascade Funding Project Manager	European Dynamics Luxembourg SA
Name & surname	Caroline Barelle
Tel:	+35 220 40 08 90
Email:	caroline.barelle@eurodyn.com
Selected Third Party 1 Project Manager Authorized representative	[Complete]
Role	The authorized representative is the intermediary between the party (ies) and the Cascade funding project Manager. In particular, the authorized representative shall be responsible for : -Setting a team agreement of all the Third Party(ies) Partners involved in the Research if relevant -Monitoring compliance with obligations stipulated in this contract. -Keeping partners when relevant, updated. -Collecting, reviewing and submitting reports/deliverables and specific requested documents to the Cascade funding project Manager on time. -Transmitting documents and information connected with the research to any other party (ies) concerned. -Administering the financial contribution related to the research and fulfilling the financial tasks related to the research.
Name & surname	[Complete]
Tel:	[Complete]
Email:	[Complete]
Selected Third Party 2	[Complete]

Role	**[Complete]**
Name & surname of the Representative	**[Complete]**
Tel:	**[Complete]**
Email:	**[Complete]**
Selected Third Party 3	**[Complete]**
Role	**[Complete]**
Name & surname of the Representative	**[Complete]**
Tel:	**[Complete]**
Email:	**[Complete]**

Implementation of the Research	
WP 1	**[Complete]**
Task 1.1	**[Complete]**
Starting date	**[Complete]**
Duration	**[Complete]**
Objectives	**[Complete]**
Description	**[Complete]**
Expected outcomes	**[Complete]**
Task 1.2	**[Complete]**
Starting date	**[Complete]**
Duration	**[Complete]**
Objectives	**[Complete]**
Description	**[Complete]**
Expected outcomes	**[Complete]**
WP 2	**[Complete]**
Task 2.1	**[Complete]**
Starting date	**[Complete]**
Duration	**[Complete]**
Objectives	**[Complete]**
Description	**[Complete]**
Expected outcomes	**[Complete]**
Task 2.2	**[Complete]**
Starting date	**[Complete]**
Duration	**[Complete]**
Objectives	**[Complete]**
Description	**[Complete]**
Expected outcomes	**[Complete]**
[Add as many tasks as necessary]	

The expected research outcomes are listed hereafter

Expected research outcomes	
Expected results in terms of Research	<mark>[Complete]</mark>
Expected results in terms of IPR, software, know-how	<mark>[Complete]</mark>

The following deliverables are mandatory. They are linked to the release of the funding.

Mandatory deliverables and reports		
Deliverable (number)	**Deliverable/ Report name**	**Delivery date**
D1	State of the art overview, use case analysis and preliminary technical specification of the solution. The document should clearly specify how the new solution extends and/or upgrades the state-of-the-art.	M2
D2	Detailed technical specification of the solution, software implementation work plan, and demo scenarios and preliminary business plan.	M4
D3	Implementation, deployment in appropriate TRUSTCHAIN platform, testing, demonstration and validation roadmap in a real-life application (i.e., banking, education, healthcare, utilities, defence or cross-border travel) and result of the validation process.	M7
D4	Modularised software components ready for distribution, full documentation for developers/users, final business plan.	M9

The following complementary activities are also linked to the release of the funding.

Mandatory complementary activities
The selected third Party(ies) attend several mandatory internal events organised with the TRUSTCHAIN Consortium: -Kick-off event devoted to knowing the different Third Parties and their foreseen contribution to TRUSTCHAIN. - Meeting for the set-up of clear KPIs that will be linked to the funding of the selected Third party (ies). - Midterm event devoted to the follow up of the progress of the Third Party (ies) according to the defined KPIs with a pitch contest where the Third Party (ies) will present their project outcomes in particular their prototype and their deployment scenarios. -Final event with pitch contest where the Third Parties will present their solution in particular their modularised software components ready for distribution

The IPR background of the third party (ies) is described hereafter:

Third party(ies) IPR Background	
Selected Third Party Partner 1 - Project Manager	**[Complete]**
Selected Third Party Partner 2	**[Complete if relevant]**
Selected Third Party Partner 3	**[Complete if relevant]**

Financial conditions	
Financial Support	-Team of natural persons: 97K € + 2K € -Legal entity(ies): 115K €+ 2K €
Schedule of payment	**-** Pre-financing:M2 - First Interim payment:M4 - Second interim payment: M7 - Final payment: End of the project
Payment conditions	o **Beginning of the implementation and Pre-financing:** During the first weeks of the project implementation, each team will define with their coaches a set of clear and objective KPIs to be achieved and linked with the funding. These KPIs are different for each team and are related to the solution to be implemented. These KPIs will help measure the progress if any, but also the commitment and involvement of the teams (i.e., attending periodic call meetings with the coaches, meeting the deadlines for reporting, etc.). After this KPIs definition, a pre-financing of **30%** will be released. o **First midterm review linked to the delivery of deliverable D2 and 2nd payment:** At first midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project on the basis of the evaluation of the deliverable D2. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is **20%** of the total amount. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until KPIs for the period are assessed as completely reached. If less than 25%, the teams will be automatically disqualified from the process.

	o **Second midterm review linked to the delivery of deliverable D3 and 3rd payment:**
	At the second midterm of the project implementation, the coaches will assess the KPI's percentage of execution of the project on the basis of the evaluation of the deliverable D3. A 100% completion of the KPIs for the related period will unlock the total of the 2nd payment which is **30%** of the total amount. A lower completion of the tasks will launch the proportional payment. If the KPIs for the related period are met by less than 50%, the payment will be retained until KPIs for the period are assessed as completely reached. If less than 25%, the teams will be automatically disqualified from the process.
	o **Final review and last payment:**
	At the end of the project implementation, third parties will be paid according to their overall completion of KPIs materialised by the deliverable D4. A final event will be used to evaluate third parties on a face-to-face pitch contest. The third parties will present their implemented solution, and their business plan in the context of TRUSCHAIN.
	Overall, failing to meet any of the research conditions and milestones aforementioned may result to an early discontinuation of the project and the corresponding disruption of the funding.
	o **Extra payment for project outcomes publication:**
	2K € extra funding will be released at the end of the project only if part of all outcomes of the project are published in a peer review journal with a minimum impact factor of 2,5. Proof of acceptance of such publication must be provided by the third party to the TRUSTCHAIN consortium to get paid.

3. MISCELLANEOUS

3.1 This Specific Research Contract, supplemented by the Standard Research Contract and its Annexes 1 to 8 included, constitutes the sole and complete understanding of the Parties with respect to its subject matter and supersedes all prior or contemporaneous communications between the Parties concerning such subject matter. This Specific Research Contract will be governed and construed according to the choice of governing and constructive law set forth in the Standard Research Contract.

3.2 Save to the extent expressly modified in this Specific Research Contract, all of the terms of the Standard Contract and Annexes 1-8 included shall apply to this Specific Contract. Save to the extent expressly specified in this Specific Contract, all capitalized terms used in this Specific Contract which are defined in the Standard Research Contract shall have the meaning given in the Standard Research Contract.

3.3 The terms of Clause 11.1 of the Standard Research Contract will apply to the signing and enforceability of this Specific Research Contract.

Done in two originals, one for each Party.

On behalf of the Cascade Funding Partner:	On behalf of the Selected Third Party:
European Dynamics Luxembourg SA	[Complete]
Signature of the authorized representative: Name: Title: Date:	Signature of the authorized representative: [Complete] Name:[Complete] Title:[Complete] Date:[Complete]

ANNEX 1.2 ESTIMATED BUDGET FOR THE ACTION

Expenditures	Total in EUR
A.1. Staff costs (where applicable)	[Complete]
A.2. Travel and subsistence	[Complete]
A.3. Equipment and materials	[Complete]
A.5. Conferences and seminars	[Complete]
Total	[Complete]
Revenues	**Total in EUR**
R.1. TRUSTCHAIN Grant	[Complete]
R.2. Income generated by the action	[Complete]
Total	[Complete]

All amounts should be provided in euro.

Staff costs will be calculated on the basis of the actual daily salary/fees of the employee/service provider, multiplied by the number of days to be spent on the project. This calculation may include, if necessary, all the normal charges paid by the employer, such as social security contributions and related costs, but must exclude any bonus, incentive and profit-sharing arrangements or running costs. Staff costs may not exceed the normal costs for each staff category in the country concerned.

Name of the Authorized representative of the Selected Third Party (ies):

[Complete]

Function of the Authorized representative of the Selected Third Party (ies):

[Complete]

Signature of Authorized representative the Selected Third Party (ies):

[Complete]

H2020 HORSE Funding Agreement

ANNEX 4 - SELECTED THIRD PARTY 'S FINANCIAL IDENTIFICATION

FINANCIAL IDENTIFICATION

PRIVACY STATEMENT   http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm#en

Please use CAPITAL LETTERS and LATIN CHARACTERS when filling in the form.

BANKING DETAILS ①

ACCOUNT NAME ②	
IBAN/ACCOUNT NUMBER ③	
CURRENCY	
BIC/SWIFT CODE	BRANCH CODE ④
BANK NAME	

ADDRESS OF BANK BRANCH

STREET & NUMBER	
TOWN/CITY	POSTCODE
COUNTRY	

ACCOUNT HOLDER'S DATA
AS DECLARED TO THE BANK

ACCOUNT HOLDER	
STREET & NUMBER	
TOWN/CITY	POSTCODE
COUNTRY	

REMARK

BANK STAMP + SIGNATURE OF BANK REPRESENTATIVE ⑤	DATE (Obligatory)
	SIGNATURE OF ACCOUNT HOLDER (Obligatory)

① Enter the final bank data and not the data of the intermediary bank.

② This does not refer to the type of account. The account name is usually the one of the account holder. However, the account holder may have chosen to give a different name to its bank account.

③ Fill in the IBAN Code (International Bank Account Number) if it exists in the country where your bank is established

④ Only applicable for US (ABA code), for AU/NZ (BSB code) and for CA (Transit code). Does not apply for other countries.

⑤ It is preferable to attach a copy of RECENT bank statement. Please note that the bank statement has to confirm all the information listed above under 'ACCOUNT NAME', 'ACCOUNT NUMBER/IBAN' and 'BANK NAME'. With an attached statement, the stamp of the bank and the signature of the bank's representative are not required. The signature of the account-holder and the date are ALWAYS mandatory.

ANNEX 1.4 - TRUSTCHAIN CONSORTIUM BACKGROUND

Partner	Background description	Specific limitations for the Implementation	Specific limitations for the Exploitation
ED	Outcomes jointly acquired during EU projects such as ONTOCHAIN grant agreement 957338	According to ONTOCHAIN Consortium agreement	According to ONTOCHAIN Consortium agreement
UL	Outcomes jointly acquired during EU projects such as ONTOCHAIN grant agreement 957338	According to ONTOCHAIN Consortium agreement	According to ONTOCHAIN Consortium agreement
AUEB	STEcon 360 BME (Business Model Evaluator) s/w tool	NA	Access to specific versions of the STEcon 360 BME s/w tool that are tailored to the context and needs of TRUSTCHAIN on a fair and reasonable basis
	Outcomes jointly acquired during EU projects such as ONTOCHAIN grant agreement 957338	According to ONTOCHAIN Consortium agreement	According to ONTOCHAIN Consortium agreement
ALA	Data and information necessary to implement the action or exploit the results	No restrictions for other beneficiaries, access on a royalty-free basis, under fair and reasonable conditions	No restrictions for other beneficiaries, access on a royalty-free basis, under fair and reasonable conditions
ICS	NA	NA	NA

CIB	Data and information necessary to implement the action or exploit the results	No restrictions for other beneficiaries, access on a royalty-free basis, under fair and reasonable conditions	No restrictions for other beneficiaries, access on a royalty-free basis, under fair and reasonable conditions
TLX	NA	NA	NA
F6S	NA	NA	NA
NKUA	NA	NA	NA

ANNEX 1.5 - THIRD PARTY(IES) PROPOSAL

[to be integrated]

APPLICANT DECLARATION OF HONOUR

Title of the proposal: _____

On behalf of

_____(Name of the third party) established in _____, (legal address), VAT number_____,[1] represented for the purposes of signing and submitting the proposal and the Declaration of Honor by _____ _____ (Name of the legal representative),

By signing this document, I declare that

1)	I have the power of legally binding the above-mentioned party on submitting this proposal.

2)	The above-mentioned party has not submitted any other proposal under TRUSTCHAIN Open Call 2. In case the above-mentioned party has submitted more than one proposal in this Open Call, all associated proposals will be automatically excluded from the evaluation process.

3)	The party(ies) that I legally represent is(are) fully aware and duly accept all TRUSTCHAIN rules and conditions as expressed in TRUSTCHAIN Open Call documents and all Annexes and will fully respect any evaluation decision and proposal selection under TRUSTCHAIN activities.

4)	If relevant, the information included in the Annex 7: SME Declaration Form is true and legally binding.

5)	All provided information in this declaration is true and legally binding.

Third party(ies) representative Contact Information:

Title (Mr, Mrs, Dr.)	[Complete]
Name	[Complete]
Surname	[Complete]
Position in the organisation (If relevant)	[Complete]
Full Address	[Complete]
Country	[Complete]
Email Address	[Complete]
Telephone	[Complete]
Mobile	[Complete]
Signature of the representative and stamp of the organisation (if relevant)	[Complete]

DECLARATION OF HONOR ON EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST

By signing this declaration of honour, I declare that all provided information below is true and legally binding both for me and for the organisations that I legally represent:

1. I declare that me and/or the organisations that I legally represent (If relevant) is not in one of the following situations:

a) it is bankrupt or being wound up, is having its affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, is the subject of proceedings concerning those matters, or is in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

b) it or persons having powers of representation, decision making or control over it have been convicted of an offence concerning their professional conduct by a judgment which has the force of res judicata;

c) it has been guilty of grave professional misconduct proven by any means which the contracting authority can justify including by decisions of the European Investment Bank and international organizations;

d) it is not in compliance with its obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed, to be proved by the deliverance of official documents issued by the local authorities, according to the local applicable rules;

e) it or persons having powers of representation, decision making or control over it have been the subject of a judgment which has the force of res judicata for fraud, corruption, involvement in a criminal organization or any other illegal activity, where such illegal activity is detrimental to the Union's financial interests;

f) is subject to an administrative penalty for being guilty of misrepresenting the information required by the contracting authority as a condition of participation in a grant award procedure or another procurement procedure or failing to supply this information or having been declared to be in serious breach of its obligations under contracts or grants covered by the Union's budget.

2. I declare that the natural persons with power of representation, decision-making or control over the above-mentioned SME are not in the situations referred to in a) to f) above;

3. I declare that:

a) Neither myself or any person (s)/organisation (s) that I represent is (are) subject to a TRUSTCHAIN conflict of interest;

b) I have not made false declarations in supplying the information required by participation in the Open Call of TRUSTCHAIN Project or does not fail to supply this information;

c) I am not in one of the situations of exclusion, referred to in the abovementioned points a) to f).

d) I am aware and fully accept all TRUSTCHAIN condition and rules as expressed in TRUSTCHAIN Open Call documents.

4. I certify that I or the organisation(s) that I represent:

o Is (are) committed to participate in the abovementioned project;

o   has stable and sufficient sources of funding to maintain its activity throughout its participation in the above-mentioned project and to provide any counterpart funding necessary;

o   has or will have the necessary resources as and when needed to carry out its involvement in the above-mentioned project.

Full name:_____ **On behalf of SME:**_____	**Signature and stamp (if applicable)** **[Complete]**
Done at (place)_____ the (day)_____(month)_____(year)	

[1] VAT is mandatory during the contract preparation for legal entities. Failure of providing a valid VAT of the specific SME will result in automatic rejection of the proposal.

ANNEX 1.7- SME DECLARATION FORM

Declaration of SME Status

Precise identification of the SME:

Name or Business name	[Complete]
Address (of registered office)	[Complete]
Registration / VAT number	[Complete]
Names and titles of the principal director(s)[1]	[Complete]

Type of enterprise:

Tick to indicate which case(s) applies to the applicant enterprise:

☐	**Autonomous enterprise**	My enterprise holds less than 25% (capital or voting rights) in another enterprise and/or another enterprise holds less than 25% in mine. *** Note**: there are exceptions for certain types of investors. See Article 3(2)(D) in the Annex of Commission Recommendation 2003/361/EC.*
☐	**Partner enterprise**	My enterprise holds at least 25%, but no more than 50% in another enterprise and/or another enterprise holds at least 25%, but no more than 50%, in mine.
☐	**Linked enterprise**	My enterprise holds more than 50% of the shareholders' or members' voting rights in another enterprise and/or another enterprise holds more than 50% in mine.

Data used to determine the category of enterprise:

Calculated according to Article 6 of the Annex to the Commission Recommendation 2003/361/EC on the SME definition.

Reference period (*):		
Headcount (AWU[3])	**Annual turnover (€)(**)**	**Balance sheet total (€)(**)**
[Complete]	[Complete]	[Complete]

(*) All data must be relating to the last approved accounting period and calculated on an annual basis. In the case of newly established enterprises whose accounts have not yet been approved, the data to apply shall be derived from a reliable estimate made in the course of the financial year.

(**) EUR 1000

Signature

Name and position of the signatory, being authorised to represent the enterprise:

[Complete]………………………………………………………………………………………………

"I declare on my honour the accuracy of this declaration."

"I declare on my honour that in case of change affecting my SME status, I will immediately inform the Agency."

"I declare having taken knowledge of the Commission Recommendation 2003/361/EC on the SME definition."

Done at (date and place):   [Complete]…………………………………………………………………………

Signature:

[Complete]

---

[1] Chairman (CEO), Director-General or equivalent.
[2] Annual Working Units = number of full-time equivalent employees.