TRUSTCHAIN

OPEN CALL #2 - CALL DOCUMENT

USER PRIVACY AND DATA GOVERNANCE

Closing dates for proposals: 20 September 2023 at 17:00 CEST

Version 1.0 – 20 July 2023

Funded by the European Union

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

Disclaimer

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

Copyright notice

The TrustChain consortium is the following:

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

TABLE OF CONTENTS

1 PREAMBLE 3
2 THE TRUSTCHAIN PROJECT 5
3 OPEN CALL 2: USER PRIVACY AND DATA GOVERNANCE 8
3.1 Introduction 8
3.2 Specific Objectives 9
3.3 Challenges to be addressed 10
3.4 Specific requirements 11
3.4.1 Technical Requirement 11
3.4.2 Sustainability requirements 12
3.4.3 Regulatory and standards requirements 12
3.4.4 User centricity Requirements 12
3.5 Expected outcomes and possible application domains 13
3.6 Mandatory Deliverables 13
4 SUPPORT SERVICES PROVIDED BY TRUSTCHAIN TO THIRD PARTIES 14
5 ANNOUNCEMENT 15
6 SUPPORT TO APPLICANTS 17
7 KIT FOR APPLICATION 18

Funded by the European Union

1 PREAMBLE

This document provides the challenges, expected outcomes and technical details important to be addressed when preparing applications for TrustChain Open Call #2. The guide is complemented by the Open Call #2 Annexes (Section 7. Kit for Application) available at https://trustchain.ngi.eu/.

Today online user platforms and websites face significant security and privacy challenges that make them untrustworthy. With huge amounts of online data collected about users' activity and choices, later to only share them with numerous third parties, the user is left with little to no choice to maintain online privacy if they want to use online services. Online user privacy and data governance face numerous challenges in today's digital landscape. Here are some key challenges:

- **Data Collection and Consent:** Many online platforms and services collect vast amounts of personal data from users, often without their full understanding or explicit informed consent. Users may be unaware of how their data is being used or shared, leading to privacy concerns.
- **Data Breaches and Security:** Data breaches have become increasingly common, with hackers gaining unauthorized access to user data. These breaches expose sensitive information, such as passwords, financial details, and personally identifiable information, compromising user privacy and leading to identity theft or fraud.
- **Lack of Transparency:** Many online companies lack transparency in how they handle user data. Users often have limited visibility into data collection practices, data sharing with third parties, and the overall data governance framework of the platform. This lack of transparency hinders users' ability to make informed decisions about their privacy.
- **Third-Party Data Sharing:** Online platforms frequently share user data with third-party advertisers, marketers, and other service providers. This sharing of data raises concerns about user consent, control over personal information, and potential misuse or mishandling of data by these third parties.
- **Profiling and Targeted Advertising:** User data is often used to create detailed profiles and enable targeted advertising. This can lead to intrusive and personalized marketing strategies that erode user privacy and create a sense of constant surveillance.
- **Cross-Border Data Transfers:** The global nature of the Internet often involves the transfer of user data across borders. Differing data protection laws and regulations among countries can create challenges in ensuring consistent privacy standards and safeguarding user data during international transfers.
- **Surveillance and Government Access:** Government surveillance programs and data requests from law enforcement agencies can infringe upon user privacy. Balancing the need for public safety and law enforcement with individual privacy rights is a complex challenge in the digital age.
- **Lack of Control and Ownership:** Users often have limited control over their own data once it is shared online. This lack of control and ownership can make it difficult for individuals to exercise their rights, including the right to access, correct, or delete their personal information.
- **Technological Advancements:** Rapid technological advancements, such as Artificial Intelligence and Machine Learning, pose additional challenges to user privacy and data

governance. These technologies can process vast amounts of data, leading to potential privacy risks if not appropriately regulated and managed.

Addressing these challenges requires a combination of technological solutions, legal frameworks, and user education. Striking a balance between data-driven innovation and preserving user privacy is essential for a more transparent and secure online environment.

Trustworthy online platforms that preserve user's data privacy and provide strong data governance frameworks are the focus of this TrustChain Open Call #2 on "User Privacy and Data Governance".

Open Call #2 welcomes applications that will clearly define, upgrade/extend the state-of-the-art, and develop the following types of solutions:

- Enhanced Consent profiles to implement transparent and user-friendly consent mechanisms that clearly explain how user data will be collected, used, and shared. A mechanism to provide users the ability to form informed consent and easily manage their privacy preferences in data sharing models,
- Data Minimization and Purpose Limitation techniques built in the web framework so that only necessary data is collected for legitimate purposes. Data owners should have means to share only data necessary to access a particular service,
- Secure data exchange and privacy-aware data processing must be the cornerstone of the new data economy. Privacy of training data, machine-learning models and model parameters should be aimed for[1],
- Developing new privacy preserving data flow techniques in line with international data sharing agreements (e.g., EU Data Spaces) so that the user has choice to tune data parameters for trading/sharing of data,
- Develop new mechanisms in line with the international data flows standards so that the data can move freely within the EU and across international borders including USA, Japan, and China,
- Data identification, data provenance, data tracking mechanisms should be built so that the data that is exchanged can be tracked. Handling of the data according to the user consent provided in a data exchange should be verifiable,
- Data certification/verification methods should be developed to verify the trustworthiness of the data,
- Modern privacy enhancing technologies, such as local differential privacy and other interactive privacy techniques, taking also into account online publicly available datasets that can be linked to the original data,
- Data obfuscation, perturbation and anonymization techniques or their combination that properly address the trade-off between privacy-preservation and data utility.

The above system examples are only indicative, and applicants can propose solutions that integrate one or more of them. Applicants can also submit a proposal under a different example scenario, as long as it serves the overall TrustChain vision and objectives, while also fitting within the scope of human centric decentralised trustworthy Next Generation Internet

[1] https://plg.eu.com/the-cross-border-data-flow-the-oecd-report-for-the-g7-digital-and-technology-pathway/https://plg.eu.com/the-cross-border-data-flow-the-oecd-report-for-the-g7-digital-and-technology-pathway/

protocols. Proposed solutions should utilize existing concepts and technologies already developed for data value sharing and preserving user-privacy and fit within TrustChain's vision and objectives. The solutions should be provided as open-source software desirably at TRL 7, tested and evaluated by an adequate pool of potential end-users that should be identified and mentioned in the application, as well as supported by a self-sustaining business model for exploiting the developed system at the end of the project. Each proposed solution will have to use the latest technologies for full-stack development that are compatible with the current standards.

The call is open for submission from 20 July 2023 to 20 September 2023 at 17:00 CEST.

2 THE TRUSTCHAIN PROJECT

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 the 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 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 the present 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 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 based on local and global data privacy techniques,
- Privacy-preserving usage of Artificial Intelligence, IoT, Cloud or combinations of those environments to provide the decentralised next generation smart digital

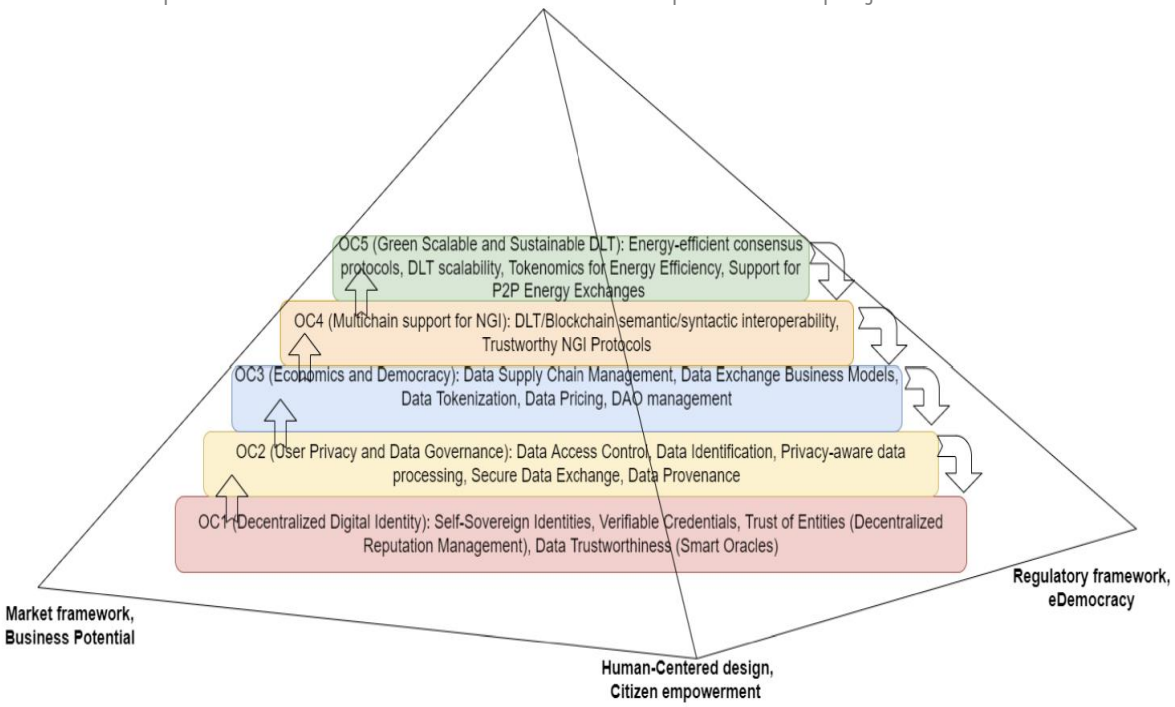
services.

Open Call #3- Economics and democracy
The objective of Open Call #3 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
Open Call #4 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 Open Call #1-4 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 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 to the Open Call #2 and outlines its context and its application modalities.

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:

- Use standard technology for full stack development,
- Be open source,
- 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:

- 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),
- 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,
- Whether the innovation will focus on the development of new solutions for existing areas, or a totally disruptive approach or idea,
- 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,
- Any challenges or opportunities relating to equality, diversity, ethics, and inclusion arising from their project,
- 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:

- Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below,
- Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework,
- Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques,
- Encrypted data analytics based on homomorphic encryption and Trusted Execution environment,
- Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs,

- Protocols to support the digital sovereignty-based data flow and data spaces initiatives.
- Data identification, data provenance, data tracking mechanisms or protocols should be built so that the data that is exchanged can be tracked, so that trustworthy data handling according to the user consent can be verified.

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

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:

- The online data sharing model is flawed as it encourages data duplication, long term data retention and intensive data collection across service providers. There is also lack of data traceability and accountability in online data sharing,
- Privacy is important when user data is employed for training machine learning models 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,
- Data accuracy vs privacy trade-off in privacy-preserving techniques like differential privacy is an open challenge and its solution can be key to solving many open-source data sharing issues,
- Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol,
- Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed,
- A trust layer is missing, and it is often difficult to ensure authenticity of data. Thus, trustworthy data access and data integrity mechanisms based on SSI technologies, including decentralized identifiers and Verifiable Credentials, needs to be designed,
- In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users,
- Users have little to no control over access to their personal data shared online. Therefore, automated user consent/smart user consent for data sharing needs to be implemented,
- Data owners currently do not have 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,
- 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:

- data privacy protection,
- privacy aware data processing,
- data provenance,
- data use policies,
- data retention and data deletion, right to be forgotten, data minimization, and trustworthiness,
- 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).

3.4.4 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.

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:

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

Possible use-cases and application domains include the following:

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

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:

- 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.
- 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.
- 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.

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

4 SUPPORT SERVICES PROVIDED BY TRUSTCHAIN TO THIRD PARTIES

Selected participants will receive support with the following services:

- **Access to Infrastructure:**
  Access to the Alastria blockchain infrastructure (two different networks, T Network based on GoQuorum and B Network based on Hyperledger Besu), compliant with Ethereum, for demonstration purposes, will be provided to the Applicants that request to use it for testing their proposed solution. This will be made available by Alastria through TrustChain, at no cost for the third-party innovators selected, in a BaaS model without requiring that the Applicants install their own blockchain node.

- **Use of token:**
  The TrustChain consortium understands that the ultimate value of a new and innovative application should be shown in business context, for example, by demonstrating that the users (physical persons or companies) are willing to pay for using the service. In this context, the TrustChain core consortium partners are willing to consider the possibility of issuing a crypto-token for the purpose of demonstration of the applications' business value, should such an interest be expressed by the applicants.

- **Business support services:**
  To support the third-party innovators to exploit their use cases and successfully reach the market, different training events and sessions with mentors will be organised. Depending on the team profile, aspects such as Value Proposition, pitching or IPR (among others) will be addressed.

- **Communication support services:**
  Major visibility, promotion and networking opportunities are offered as part of the TrustChain project and the Next Generation Internet initiative. Selected third party innovators will:

  - have access to communication tool kits and co-branding materials,
  - be showcased in the TrustChain project website,
  - be interviewed and promoted on relevant media channels,
  - be invited to participate in top events, and
  - connect with a vibrant ecosystem of innovators, investors, industry players and public authorities.

5 ANNOUNCEMENT

Submission to the TrustChain Open Call #2 will open on 20 July 2023 (13:00 CEST) and close on 20 September 2023 (17:00 CEST). Dates for the different phases are outlined below but may be subject to change if any modifications in the project's schedule occur.

The table below presents the indicative dates during which each phase of TrustChain Open Call #2 will take place.

Call Announcement	20 July 2023 at 13:00 CEST
Call closure and submission deadline*	20 September 2023 at 17:00 CEST
Total EU funding available	1.989.000 €
Evaluation Period*	Up to three months after the call closure
Signature of Sub-grant Agreement*	Up to one month after the announcement of the final list of selected projects
Expected duration of projects	9 months
Task description	Today, 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. In order to achieve TrustChain vision, it is expected that applicants will develop tools, cryptographic mechanisms, and other algorithms for data handling and sharing as well as for the management of data lakes in compliance with GDPR and other regulations that implement techniques such as: • Mechanisms for multi-party data sharing that lies in the scope of the call and addresses the stated challenges below, • Protocols for privacy-preserving data sharing using techniques from technologies such as federated learning both vertical and horizontal framework, • Privacy-preserving data processing, data storage and data computation techniques such as differential privacy, data obfuscation/perturbation, anonymization techniques, • Encrypted data analytics based on homomorphic

	encryption and Trusted Execution environment, • Protocols to verify authenticity and accuracy of data using technologies like zero knowledge proofs, • Protocols to support the digital sovereignty-based data flow and data spaces initiatives. Applications should cover real needs of the end-users in a specific sector such as for example banking, education, healthcare, or e-government. To develop effective user privacy preserving and state-of-the-art consent- based data management, Applicants are requested to addressed current challenges: • The online data sharing model is flawed as it encourages data duplication, long term data retention and intensive data collection across service providers. There is also lack of data traceability and accountability in online data sharing. • Privacy is important when user data is employed for training machine learning models 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. • Data accuracy vs privacy trade-off in privacy-preserving techniques like differential privacy is an open challenge and its solution can be key to solving many open-source data sharing issues. • Privacy-aware data processing needs to be encouraged from the design phase of any data sharing/processing protocol. • Similarly, illegal data copying is a big challenge in user privacy and data governance models today which needs to be addressed. • A trust layer is missing, and it is often difficult to ensure authenticity of data. Thus, trustworthy data access and data integrity mechanisms based on SSI technologies, including decentralized identifiers and Verifiable Credentials, need to be designed. • In line with providing a trust layer supporting user privacy, data provenance ontologies and data transaction logging should be available to users. • Users have little to no control over access to their personal data shared online. Therefore, automated user consent/smart user consent for data sharing needs to be implemented. • Data owners currently do not have 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.

	• Users should be empowered to add the necessary levels of anonymity to share their data with a third party. A user centric design approach should frame the developed solution carefully consider the following: • data privacy protection, • privacy aware data processing, • data provenance, • data use policies, • data retention and data deletion, right to be forgotten, data minimization, and trustworthiness. • data minimization and user informed data deletion
Submission and evaluation process	Proposals are submitted in a single stage and the evaluation process is composed of three phases as presented hereafter: • **Phase 1:** Admissibility & eligibility check • **Phase 2:** Proposals evaluation carried out by the TrustChain Consortium with the assistance of independent experts. • **Phase 3:** Online interviews (10 minutes pitching & 20 minutes of Q&As) and final selection carried out by TrustChain Consortium and TrustChain Advisory Board Members.
Further information	Further details are available at: https://trustchain.ngi.eu/apply

***NOTE:** Dates for the different phases are indicative and may be subject to change if any modifications in the project's schedule occur.

6 SUPPORT TO APPLICANTS

The TrustChain consortium will provide information to the applicants only via trustchain@ngi.eu. No binding information will be provided via any other means (e.g., telephone or email).

More info at: https://trustchain.ngi.eu/apply
Apply via: https://www.f6s.com/trustchain-open-call-2
Support team: trustchain@ngi.eu
Personal Data Protection Policy available at: https://trustchain.ngi.eu/privacy-policy/

The TrustChain consortium will also organise webinars to connect with interested applicants so stay updated and get involved!

7 KIT FOR APPLICATION

TrustChain Open Call #2 supported materials can be found at https://trustchain.ngi.eu/apply and are the following:

- **Open Call #2 – Call document**

  The present document.

- **Annex A - Guide for Applicants**

  This document provides in detail the information to help apply to the TrustChain Open Call #2, such as an abstract of the TrustChain action, a description of the TrustChain Open Call #2, the modalities for application, the evaluation process, the scheme of the funding support, the IPR aspects related to TrustChain and how to prepare and submit a proposal.

The kit also includes the Model Sub-grant Agreement (draft template only), Administrative form (read only), Proposal description and the Additional Applicants templates, as follows:

- **Annex B – Model Sub-grant Agreement – draft template only**
- **Annex C - Administrative Form – read only**
- **Annex D - Proposal Description template – read only**
- **Annex E - Additional Applicants template – read only**

Note: Word templates (Annex D and Annex E) are available at the F6S Submission System.