2nd Open Call NGI_TRUST

NGI_TRUST, co-funded by the European Union's Horizon 2020 research and innovation programme under the grant agreement No 825618, foresees as an eligible activity the provision of financial support to third parties, as a means to achieve its own objectives.

Third-party projects may only receive financial support if they are working on privacy and trust enhancing technologies and their application to the Next Generation Internet (as defined broadly by the Horizon 2020 Work- Programme 2018-20, Information and Communication Technologies Part 5.i - Page 51 of 144), namely: as sensors, objects, devices, AI-based algorithms, etc., are incorporated in our digital environment, develop robust and easy to use technologies to help users increase trust and achieve greater control when sharing their personal data, attributes and information.

1.1. The NGI Trust open calls aim to:

- Engage a variety of players (newcomers to H2020 are encouraged) !
- Explore pre-selected privacy & trust enhancing topics (defined with the support of our advisory board) critical to building a human centric Internet.

1.2. NGI TRUST will support third-party projects working in the following areas:

- Better management of consent, to give more control to the user of their data when accessing and using services.
- Technical innovation in privacy enhancing technologies, such as cryptography, federated identity, security and privacy for IoT, privacy-enhancing data transports and data at rest.
- The application of artificial intelligence/machine learning/neural networks to serve the user's interests.
- Bootstrapping trust at the protocol level, to maintain a trustable Internet Infrastructure.

An indicative list of possible areas of concern/opportunities (specific topics) is provided below:

Topics focused on App implementations to manage the plethora of Information Sharing Agreements and consents that a person would agree to, manage and re-use over time (Type 2 or Type 3 proposals only)

- Solutions enabling users to get trust on privacy terms
- Solutions enabling users to more easily and uniformly set preferences or terms such as machine-readable privacy terms (IEEE - P7012) and technologies that help to reduce the risk that GDPR is misused to further exploit/ complicate the user experience.
- Efficient techniques to anonymize personal data in the era of Big Data.

1. **Technical innovation in privacy enhancing technologies, such as cryptography, federated identity, security and privacy for IoT, privacy-enhancing data transports and data at rest.**

- Simplified multifactor authentication
- Option for encrypted devices/data at rest. i.e. an option for the user to prevent being forced to decrypt their data under, such as physical threat.
- Cybersecurity certification for ICT products, processes and services in the EU (EU Cybersecurity Act).
- Solutions that improve algorithm agility (where deployed algorithms are superseded and must be replaced).
- Improved information for users about the security mechanisms in use by apps (browsers give the user some clues about e.g. TLS; apps give none).
- Pilot implementation of specifications, standards, acceptance criteria and measurement frameworks for new identifiers, for instance: Mobile Driving Licenses; Delegation in the context of ID; eID and authentication services to support, for instance student mobility and access to educational services, thin file individuals, disabled users, refugees, non-digital natives, lost identities due to natural disasters etc.
- projects which bridge the gap between technological enhancements on one side and their actual uptake by non-expert users of the internet on the other side
- With a view to next generation certificates, how can European grid certificate authorities build up user-friendly mechanisms that promote a changed user experience and awareness and addresses forms of identity that comply with EU law and or meet specific European needs.

1. **The application of artificial intelligence/machine learning/neural networks to serve the user's interests.**

- User-centric design, simplicity, usability, edge AI ('artificial intelligence')
- Taking into account the recommendations of the EU High Level Expert Group on AI, a scientific and empirical approach is needed, such as developing guidance on how to approach access and acquisition of data for the development/expansion of AI, operationalize those recommendations in order to strengthen the capacity/ability of the Internet industry in Europe.
- Explainable artificial intelligence (XAI) for improving human trust in artificial intelligence (AI) systems
- Quantum resistant computing

1. **Bootstrapping trust at the protocol level, to maintain a trustable Internet Infrastructure.**

- DNS-based security of the Internet Infrastructure (DNSSEC, DOH approach), given the need to reinforce trust in a world of "deep fake".

1.3. The call is open to individuals or organisations, or groupings thereof.

Specifically, the following may apply, either on an individual basis or as a consortium:

- Researchers and developers (holding a master's degree or higher) employed in third-level education institutes, research infrastructures, not for profit organisations and charitable (scientific) foundations and public research centres.
- Internet technologists and innovators, privacy and trust specialists and action groups
- Organisations/companies with relevant privacy and trust cases or concerns in specific sectors or 'verticals' (fields such as health, etc.).

- Micro, small and medium sized enterprises firms working on internet technologies.

Applicants may be legal entities or natural persons and should be registered (for organisations) or resident (for individuals) in an EU Member State or a Horizon 2020 associated country.

1.4. NGI_TRUST Open Call third-party projects

Three types of third-party projects will be awarded funding:

- Type 1 (viability): up to € 75,000 per project from NGI_Trust, no matching funds required. The objective is to explore and assess the technical feasibility and/or commercial potential of a breakthrough innovation that aims at enhancing privacy and trust for the NGI. Activities can include conceptual development, risk assessment, market study or intellectual property management of a new technology or service, or a new application of existing technologies. Indicative duration: 6 months.
- Type 2 (execution): up to €150,000 per project from NGI_Trust and matching funds of up to €75,000 (2/3 - 1/3 model). The objective is to fund R&D or technology development projects underpinned by a strategic plan and feasibility assessment (which can be, but need not be, developed through a Type 1 project funded by NGI_Trust). Indicative duration: 6-9 months.
- Type 3 (transition to commercialisation): up to €200,000 per project from NGI_Trust and the equivalent in matching funds (50/50). These projects should pursue the commercialisation of a privacy and trust enhancing innovation for the NGI (which can be, but need not be, developed through a Type 2 project funded by NGI_Trust). Indicative duration: up to 12 months.

Interested in applying ?

For the second call, the call text, application form and detailed guidance for applicants are now available (as of 8:30 (CET) 1 October 2019) for download below.

Applications should be received by 1 December 2019 at 18:00 CET

Call text

Guidance for applicants

NGI_Trust_2nd O...ants_190930.pdf

Application form

NGI_Trust_2nd O...ate_190930.docx

1.5. Support and further information:

Please take a look at: NGI Trust Webinar for potential applicants for information about the second call online open day.

Please check for further information published on the NGI_TRUST open call wiki pages & follow our twitter account: https://twitter.com/NgiTrust.

For further information or if you have any question, please contact the NGI_TRUST support team: NGI-Trust-support@lists.geant.org

Email address for further information: NGI-Trust-support@lists.geant.org