ICT-56-2020 "Next Generation Internet of Things"

Grant Agreement number: 957218

IntellioT

Open Call 3

Guide for Applicants

Submission starts August 8th, 2023, 12:00 CET

Submission deadline is October 8th, 12:00 CET

Version 1.0

IntellIoT

Table of Contents

General Overview 3
The IntellIoT framework 3
application Areas for Open Call #3 6
Application 7
Eligibility criteria 7
Proposal / Application preparation 7
Financial support provided 8
Timeline 9
Evaluation and selection process 10
Eligibility check 10
External evaluation 10
Consensus Meeting 12
Collaboration Agreement 12
Pilot Program 12
Additional Information 12
Intellectual Property and Publication Rights 12
Ethics 13
Data protection 15
Coordinator & Contact 16
Complaints 16
Partners 16

General Overview

IntellIoT, a pan-European research and innovation project funded by the European Union as part of the Horizon 2020 program ICT-56-2020 "Next Generation Internet of Things", is organizing a 3rd Open Call with the aim to involve specifically Micro-SMEs to build applications, services, and extensions on the IntellIoT technical framework within a special hackathon ("HackWeek") as well as a 1-month pilot program ("HackMonth").

The Open Call #3 will be used to gain feedback from the participants on the developed framework and technologies as well as to explore different novel business models applied by the Open Call winners with a special focus on the manufacturing domain and the Industrial Metaverse.

Applicants are invited to join the special innovation format – an online HackWeek – to explore the IntellIoT's framework and to redefine a technology and business proposition highlighting how they may be able to integrate the IntellIoT framework. The submissions will be evaluated by independent and external experts based on clearly outlined criteria, resulting in the selection of the four companies in Open Call #3.

The four selected companies will gain access to the IntellIoT project within a 1-month pilot to work with the IntellIoT partners on the framework. In addition, the selected organizations will receive up to 7,000 euros for their efforts in accordance with the selection criterion on economic fairness and as necessary to achieve the objectives of the action.

IntellIoT partner Startup Colors UG is responsible for coordinating the Open Calls.

The IntellIoT framework

The overarching objective of IntellIoT is to develop a reference architecture and framework to enable IoT environments for (semi-)autonomous IoT applications endowed with intelligence that evolves with the human-in-the-loop based on an efficient and reliable IoT/edge-(computation) and network-(communication) framework that dynamically adapts to changes in the environment and with built-in and assured security, privacy, and trust. This reference architecture and framework was applied in the heterogeneous use cases encompassed in the project, covering agriculture, healthcare, and manufacturing smart environments during cycle 1. For cycle 2, results were fed into the demonstration of the 2nd release of the IntellIoT framework and were applied in the domains of construction, energy, and smart city.

Figure 1 showcases how the IntellIoT architecture is organized around the three pillars at the heart of the project's concept; i.e., Collaborative IoT, Human-in-the-loop, and Trustworthiness, and provides a high-level, simplified view of the IntellIoT framework and its building blocks. At this point, only the components colored in green are available for public use, while the gray-colored ones are still being developed.

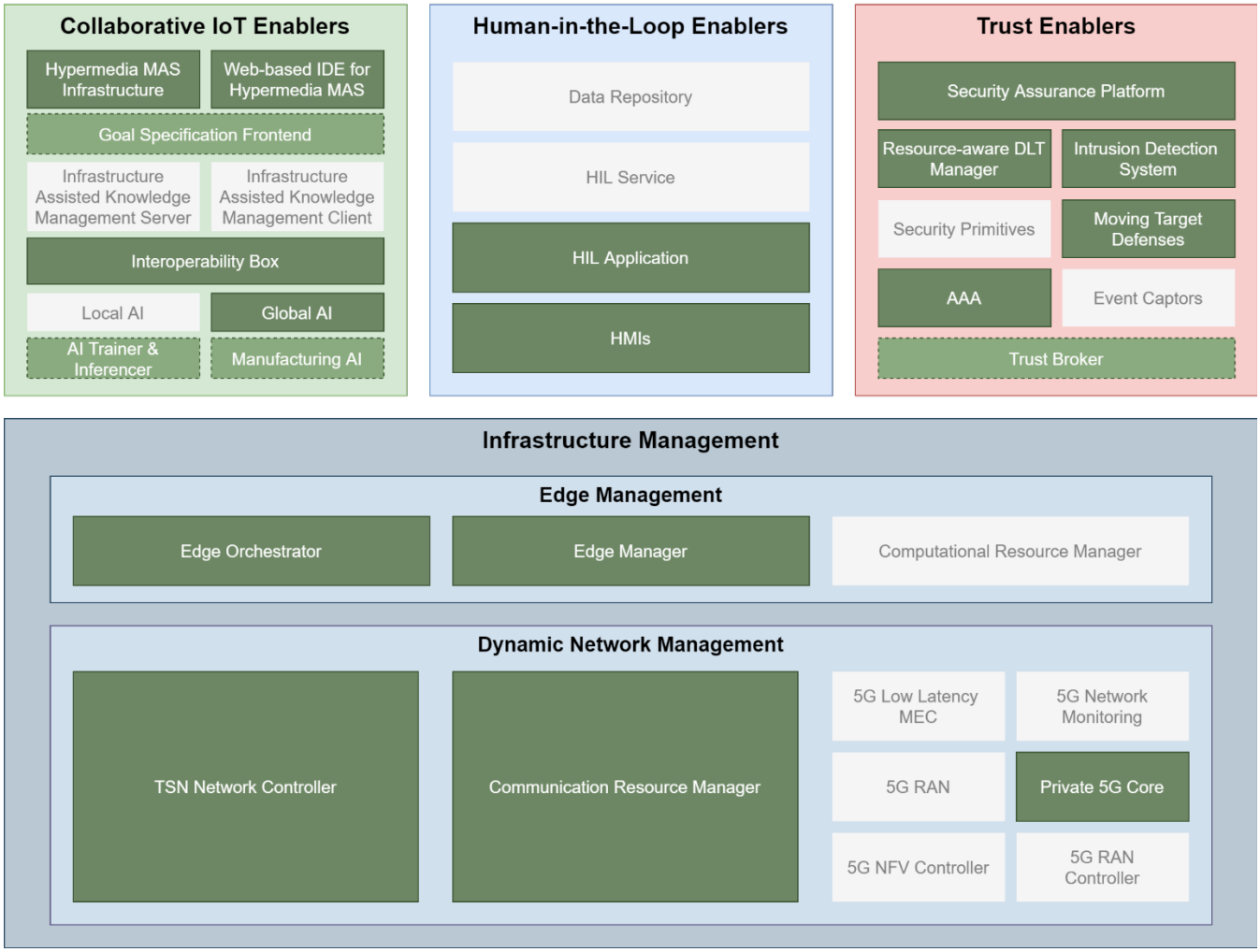

Figure 1: Overview of IntellIoT's components within their respective component areas

- **Collaborative IoT:** Various semi-autonomous entities (e.g., tractors, robots, healthcare devices, etc.) will need to cooperate in order to execute multiple IoT applications. These entities will have to be self-aware and will all have a different amount of knowledge of the task at hand and the environment where they are located. Unfortunately, providing all the necessary knowledge to the entities is not always possible in changing environments. To keep the knowledge of the entities up to date, they need to extend it by applying learning technologies based on Artificial Intelligence and Machine Learning. New knowledge can either be acquired by interacting with the environment (via sensors) or by interacting with the other entities in the environment. By exchanging information via a reliable and secure communication network, the entities in the environment will need to collaborate with each other to update their own knowledge to fulfill their assigned task. At the heart of the Collaborative IoT (system-wide AI) components is the *Hypermedia Multi-Agent System (HyperMAS) Infrastructure*; a multi-agent system that reacts to incoming end-user goal specifications, managing -

including discovery and search facilities - available artifacts and agents (defined in W3C WoT Thing Descriptions or W3C WoT Thing Description Templates) along with available procedural knowledge (i.e., agent plans). Moreover, *Federated Learning* is leveraged to prevent deployed model degradation, address edge cases, and implement data privacy and security.

- **Human-in-the-Loop:** The human within the system will keep on playing a crucial role in the whole process. The aim is not to remove the human from the system, but use his/her/their know-how & input in cases where the system does not have the knowledge (yet) to handle the situation and the collaboration with the other entities in the field also does not provide the required information. The interaction with the human (be it either the machine operator, the farmer, the physician, or any other person) will enable the intelligent system to expand its knowledge about the environment or the application through machine learning technologies and use the experience from the human operator to learn new features or information about the overall process. Therefore, humans will remain a vital element of the system and will interact with the IoT elements in the system to overcome the current limitations of the system. Key elements include the *Goal Specification Front End,* which enables the end user (e.g., farmer, customer, doctor) to specify the goal (e.g., "plant wheat in field 5"), sending it to the back end of the Web-based IDE that does the mapping from user goals to the input for the Hypermedia MAS and enables the systems engineer to monitor the system and to specify the agent organization and the procedural knowledge of individual agents. The IntellIoT features additional innovative Human-Machine Interface (HMI) capabilities, leveraging *Virtual Reality (VR)* and *Augmented Reality (AR)* technologies (based on Oculus Quest 2[1] and HoloLens 2[2], respectively – the latter augmented by a *Stylus Pen*) to provide a user-friendly, feedback-rich and tactile way of interacting with and managing the underlying intelligent infrastructure.
- **Trustworthiness:** Security, Privacy, and, ultimately, trust are considered as indispensable preconditions for reliability and the wider acceptability of distributed, collaborative IoT systems and applications. The trust of the human (e.g., a patient or farmer) in the system is key, as the system's (autonomous) decisions need to be trusted, and the end-user's data need to be handled with the utmost care by providing appropriate levels of security and privacy safeguards. In this context, and in addition to well-understood security and privacy best practices, IntellIoT will adopt advanced security intelligence to protect unsupervised device-to-device interactions based on self-adaptable, security-related operations. Furthermore, the overall trust will be fortified by continuous monitoring, real-time assurance assessment, and primitives enabling transparency of performed actions. Distributed ledger technologies (DLT) and smart contracts will be made accessible by IoT devices and other actors to show transparency of performed actions, create trustworthy supply chains and build trust between parties. Aiming to provide a solution with Trustworthiness by design, a set of trust components are designed, developed, and integrated within IntellIoT. A *Security Assurance* platform acts as the trustworthiness hub within the framework, providing continuous, real-time assessment of the security and privacy posture of the underlying IoT deployment and IntellIoT itself. Moreover, novel, resource-aware *Distributed Ledger Technologies (DLTs)* are developed and integrated, which are based on *HyperLedger Fabric (HLF)*, and are leveraged to provide auditability, reliability, and accountability in all critical operations (transactions) within IntellIoT's deployed application domains. Furthermore, trust components include advanced (trust-based) *Intrusion Detection* systems which are augmented by *Moving Target Defence*

[1] https://www.oculus.com/quest-2
[2] https://www.microsoft.com/en-us/hololens

mechanisms based on agents that administrate the IoT network at runtime to change the system's configuration both proactively and reactively when attacks are detected.

- The above three pillars are supported - and their capabilities are enabled – by IntellIoT's **dynamically managed network and compute infrastructure**. In more detail, IntellIoT features computation resource management and edge management, and orchestration capabilities, along with network choreography and management and xApp management and control features. The underlying network infrastructure supporting tactile communication is built upon *5G* (5G MEC, 5G vRAN, 5G D2D, Private 5G Core), and *Deterministic - Time-Sensitive Networking (TSN)* - technologies.

More details on the framework's components that are available for integration are presented by means of specific one-pagers for each component via their respective component areas:

- Collaborative IoT (key pillar 1)
- Human-in-the-Loop (key pillar 2)
- Trustworthiness (key pillar 3)
- Infrastructure management

In addition to the component one-pagers, there are related publicly-available IntellIoT deliverables (e.g., D2.6, providing the final IntellIoT architecture) that provide information regarding the different technologies, licensing schemes and any other details that the applicants may request.

APPLICATION AREAS FOR OPEN CALL #3

The 3rd Open Call focuses on exploitation activities and highlights the technical impact and sustainability of the developed solution, the IntellIoT framework (see Figure 1). Hence, the consortium would like to attract candidates that can develop technological approaches that apply the IntellIoT framework specifically in the novel space of "**Industrial Metaverse".**

To frame the applicable areas, IntellIoT defined **four specific challenges** that especially MicroSME shall be able to address within the HackWeek that will take place from October 9 – October 13, 2023:

1. **Secure & Transparent Billing on the Blockchain**
2. **Virtual Industrial Revolution using XR Solutions**
3. **AI-Driven Autonomy for Industrial Vehicles**
4. **Remote Robot Control using Multi-Agent-Systems and Web of Things**

In Open Call #3, selected applicants will address these challenges in a special HackWeek (5 days of Co-Creation from October 9–13, 2023) in which concepts and first solutions will be presented. If chosen in the final qualification presentation, a team will be able to join the 1-month pilot period / HackMonth to intensify the work and implement the developed concept.

Applicants are expected to showcase MVPs and Concepts that showcase solution pathways focusing on the four identified Industrial Metaverse challenges. Besides a project description provided on the platform TAIKAI, all eligible HackWeek teams will present their approaches in special 10 min presentations to selected evaluators.

Application

ELIGIBILITY CRITERIA

The IntellIoT Open Call #3 focus on involving startups and SMEs, in particular **Micro-SME**, as per definition from the European Commission (https://ec.europa.eu/growth/smes/sme-definition_en).

Please, be aware that while checking the company's status, if it is a Micro-SME, the linked parties of the company are also taken into consideration. SME status is calculated in accordance with the rules defined in the EU recommendation 2003/361. As a summary, the criteria which define a Micro-SME are:

- Staff headcount in Full Time Equivalents (FTE) less than 10;
- Annual turnover less or equal to €2 million OR annual balance sheet total less or equal to €2 million.

IntellIoT partners and their related entities or entities in which IntellIoT partners have shares or other interests are excluded from participating in the Open Calls. The existence of potential conflicts of interest among applicants and one or more consortium partners will be taken into consideration. Furthermore, the winning SMEs from IntellIoT's OC1 or OC2 are not eligible for OC3.

Each proposal must be submitted by a single applicant, consortia are not allowed.

Organizations must be legally incorporated in the European Union or in one of the Horizon 2020-associated countries to be eligible. For more information, please see the attached links regarding the **European Union member states (EU27)** as well as **countries associated with Horizon 2020**. All applicants must provide a PIC to prove the legal incorporation.

PROPOSAL / APPLICATION PREPARATION

The Open Call proposal, as well as all corresponding documentation must be written or presented in English. Proposals submitted in any other language will not be evaluated. English is also the only official language during the whole duration of the pilot, and accordingly, any requested deliverables will be admitted only if submitted in English.

All applicants will have to submit an outline of their technology proposition describing how their approach is addressing the four defined challenges. They will have to describe how they intend to use the funding provided to realize optimal results during the 1-month pilot.

Applicants are not allowed to submit multiple applications. In case that more than one application from the same applicant is submitted, only the one submitted first will be considered and any other will be rejected.

Applicants can join the Open Call #3 by attending the IntellIoT HackWeek from October 9 – 13, 2023. All interested Micro-SMEs need to register via the hackathon platform TAIKAI. Proposals submitted by any other means will not be considered for funding. All questions need to be adequately answered.

Within the hackathon platform, all applicants must provide information based on a predefined template, including the following sections:

Company Information* • Legal name • PIC • Legal contact • Number of employees / (full-time FTE) • Turnover • Website	**Team Information** • Name of team members • Position of team members • Role of team members • Expertise of team members • Gender
Technology • Description of existing technology / Product • Touch Points with IntellIoT Framework	**Description of your Business** • Current business model • Traction & Achievements
Challenge • Which provided HackWeek challenge do you apply? • Which problem statement do you want to tackle? • Goal for the HackWeek	**Solution Approach**** • Product approach • Applied technologies & Data sets • Novelty of the proposed solution • Technological achievements during the Hackathon
Exploitation / Business Opportunities** • Long-term impact of the proposed challenge solution	**Needs**** • Short work plan for the 1-month • Resources and support needed from IntellIoT

*relevant for eligibility
** to be filled out during the HackWeek

FINANCIAL SUPPORT PROVIDED

The EC funding budget for Third Parties available for all IntellIoT Open Calls is 860,000 Euro. During Open Call #3, the four selected companies will gain access to the IntellIoT project within a 1-month pilot/HackMonth to work with the IntellIoT partners. In addition, the selected organizations will receive financial support of up to **7,000 EUR** for their efforts in accordance with the selection criterion on economic fairness and as necessary to achieve the objectives of the action.

The beneficiaries will receive the funding as a fixed lump sum. The lump sum is a simplified method of settling expenses in projects financed from Horizon 2020 funds. It means that the grantee is not required to present strictly defined accounting documents to prove the cost incurred (e.g., invoices) but is obliged to demonstrate the implementation of the project in line with the milestones set for the project. Simply speaking it means that we will assess your progress and quality of your work during the final review, not your accountancy. The milestones (deliverables and KPIs) will be elaborated at the beginning of the 1-month pilot.

The lump sum does not release you from the obligation to collect documentation to confirm the costs under fiscal regulation.

In order to receive the grant, an individual Collaboration Agreement in accordance with Horizon 2020 funding rules has to be signed between the selected organizations and the IntellIoT consortium. SIEMENS AG, as the overall coordinator of the IntellIoT project, will be responsible for transferring the grants in accordance with the above-mentioned process and the following installments:

- After contract signature, a prepayment of **50% of the requested funding** will be issued.
- One month after the end of the pilot phase and after the final review presentation, plus the submission of a short 2-page Summary Report, the **remaining 50%** of the requested funding will be transferred.

The Collaboration Agreement will include a set of obligations that beneficiaries have towards the European Commission. It is the task of beneficiaries to satisfy these obligations and of the IntellIoT consortium partners to inform beneficiaries about them.

An exemplary set of obligations:

- Obligation to submit to any control measures (checks, reviews, audits, or investigations) in relation to the participation in the IntellIoT project,
- Obligation to keep records,
- Obligation to provide information to the Coordinator or EC or other Consortium Members in order to verify proper implementation of the action and compliance with any other obligation,
- Obligation to adhere to the ethics requirements of the project,
- Liability for damages.

The selected companies shall be responsible for all possible taxes, wire transfer costs, and other possible costs related to the payment of grants.

TIMELINE

The Open Call #3 will apply the following multi-stage process:

HackWeek

- August 8th, 2023, 12:00 CET: Registration for HackWeek via Online Hackathon Platform TAIKAI
- October 8th, 2023, 12:00 CET: End of Registration for HackWeek /Eligibility Check
- October 9th, 2023, 12:00 CET: Invitation of eligible Micro-SME to join the HackWeek
- October 9th , 2023, 17:00 CET: Kick off of HackWeek
- October 10th – October 12th, 2023: Attendance of a minimum of 3 check-ins / workshops via MS Teams
- October 13th, 2023, 12:00 CET: Final submission of information/MVP/Slide Deck developed during HackWeek
- October 13th, 2023, 15:00 CET: 10 min-presentation of Submission/HackWeek achievements (Demo Day)
- October 13th, 2023, 18:00 CET: Announcement of Winners

HackMonth

- October 23th, 2023: Start of HackMonth / 1-month pilot program

- November 29th, 2023: Final 30 min-Presentation & Q&A of Pilot Results

The Organizers might change the submission timeline at their discretion, the change in application timeline will be duly communicated. The applicants are strongly recommended not to wait until the last minute to register for the HackWeek.

After the closing of the registration phase, all registered Micro-SME will first be checked for eligibility on October 8th. All eligible Micro-SME will be invited to join the HackWeek. During the HackWeek, eligible SMEs can decide if they want to enter the final presentation/ DemoDay taking place on October 13th, 2023, 15:00 CET. Applicants that have not uploaded their final information/MVPs/Slide Decks by October 13th, 2023, 12:00 CET onto the hackathon platform are disqualified automatically. Applicants that do not check in with the IntellIoT team (via Email, message, Slack) during the HackWeek at least 3 times will also be disqualified.

Evaluation and selection process

The evaluation and selection process of the Open Call is designed to create an open, accountable, multi-step selection process based solely on the merit of the submitted application. All submissions shall receive the same opportunity.

ELIGIBILITY CHECK

Registered Micro-SME will first be checked according to the "Eligibility criteria" described in the earlier "Application" section. Proposals that do not comply with these criteria will be excluded. This eligibility check will take the following information into account:

- Legal name
- PIC
- Legal contact
- Number of employees / (full time FTE)
- Turnover
- Website

Applicants that are providing incomplete data will be disqualified. Please ensure to add a PIC which can be obtained from the EU Commission within 48h free of costs.

EXTERNAL EVALUATION

Each eligible application shall be evaluated by a minimum of two independent and external experts. The experts will be individuals with experience in the fields of innovation linked to this Open Call and with the highest level of knowledge. In the Open Call #3, the evaluators will take over the role of HackWeek jurors. They will attend the final presentation / DemoDay on October 13th, 2023, and will also receive access to the submitted information on the Hackathon Platform TAIKAI on October 13th, 2023, between 12:00 and 15:00 CET.

All involved experts will sign a declaration of confidentiality concerning the evaluation process and the content of the proposals they evaluate. They will also declare their absence of any conflict of interest for the assigned tasks.

The experts will apply the criteria outlined below to the concepts presented at the final day of the HackWeek:

- **Problem-Solution-Fit based on the chosen challenge** (desirability): Will the proposed solution solve the identified challenge?
- **Level of Innovation / Technical Excellence:** How innovative is the proposed technical solution? How applicable is the solution to the IntellIoT framework? Which provided technologies & data sets have been applied? Assessment of soundness of concept, quality of objectives and innovative elements of the proposal.
- **Feasibility of Idea & Implementation:** To what extent has the application already been implemented within the HackWeek? What is the quality, functionality, and stability of the developed "hacks"? Has the team the technical ability to finalize the implementation of the solution within the HackMonth? Are there enough resources to finalize the solution within the HackMonth? What working packages are defined for the HackMonth / 1-month pilot.
- **Impact and Business Approach:** What is the long-term impact of the proposed challenge solution? (viability) Demonstrate impact through examples showing specific future exploitation potential. Contributions should showcase ways to create added value to an existing IoT solution and enable next-generation IoT technologies across Europe.
- **Team Set-up / Diversity:** What technical expertise does the team bring in? Assessment of the quality and relevant experience of the individual participants, quality of the team as a whole, including complementarity, balance and diversity.
- **Economic Fairness:** The provided budget of 7,000 euros should be adequate with the proposed work plan and should allow significant improvements of the first MVP during the HackWeek / 1-month pilot.
- **Presentation / Pitch**: Is the applicant able to present their achievements in an understandable and convincing way?

Each criterion will be scored between 1 and 6 points and only entire points are allowed:

- **1 (Fail):** Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
- **2 (Poor):** The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.
- **3 (Fair):** While the proposal broadly addresses the criterion, there are significant weaknesses.
- **4 (Good):** The proposal addresses the criterion well, although improvements would be necessary.
- **5 (Very Good):** The proposal addresses the criterion very well, although certain improvements are still possible.
- **6 (Excellent):** The proposal successfully addresses all relevant aspects of the criterion in question.

Each evaluator will receive an equal amount of token provided by the platform TAIKAI. Each score will be translated into tokens which will be calculated into a joined score per applicant. This score will be used to create a ranking.

The comments and scores of each external evaluator will be recorded via TAIKAI and will be published in the form of a Leadership Board after October 16th, 2023.

Per HackWeek challenge one (1) Micro-SME with the highest score - altogether four (4) Micro-SME in Open Call #3 - will be selected and invited to join the HackMonth. In case there is no eligible applicant in one challenge/category, a 4th SME will be selected besides the top SME per category based on the next highest score applying the overall ranking.

Consensus Meeting

After the external evaluator selection based on the score, a selection committee formed by selected members of the consortium partners and potentially external evaluators, will decide by consensus the list of winning Micro-SME selected for the funding, as well as the "reserve list". The discussion will be based on the ranking obtained as a result of the external evaluation via Taikai.

The results of the consensus meeting will be recorded. The 4 highest ranking applicants per challenge will be contacted on October 16th, 2023 and the ranking will be published via the Leadership board on Taikai. With these results in mind, a due diligence with the selected applicants will be carried out between October 16th and October 23rd, 2023. Whilst normally the highest ranked proposals will be selected for funding, there might be a fair reason for objecting to a specific third party, e.g. if significant ethical concerns or a potential conflict of interest can be identified. In this case, the choice may pass to another applicant on the shortlist.

Collaboration Agreement

Before the 1-month pilot phase starts, we will ask the Micro-SME to sign the Collaboration Agreement with the IntellIoT consortium. To do so, we will ask the winning SME to provide documents regarding your formal status. Please provide all requested documents within the deadlines that will be communicated to you. If you fail to deliver the requested documents on time, without clear and reasonable justification, the SME will be excluded from the further formal assessment and will be replaced with a company from the reserve list.

Pilot Program

The four selected Micro-SME will be invited to join a 1-month pilot programme – so called HackMonth. The HackMonth will take place between October 23rd and November 29th, 2023, in a virtual environment. During this 4-weeks pilot, experts from IntellIoT will support the Micro-SME in developing the MVP from the HackWeek further, in applying additional data and open source resources as well as existing IntellIoT framework components provided by IntellIoT partners. During this pilot programme, the selected Micro-SME will have weekly check-ins with IntellIoT experts. On November 28th, the four SME will present their achievements in a final review session.

Additional Information

Intellectual Property and Publication Rights

Participants retain full and exclusive ownership of their prior information and intellectual property rights. By submitting their application participants warrant that they hold ownership or have legally secured the right to use all elements of the technology. Participants shall indemnify and hold harmless the IntellIoT project partners, or any

assignee or affiliate for any allegations or claims by third parties of infringement of intellectual property rights by the technology of participants.

Participants shall have the right to further develop, use and license their intellectual property rights for creating, making, marketing, and distributing products, services and technology.

By submitting their application forms, the selected companies agree to the possible inclusion of their technology in any media coverage by IntellIoT and its partners, such as press releases or publications. The content of such publications will be checked with the companies and only published after approval. Also, all winners agree that their personal data, such as their names and affiliations, pictures, videos and sounds may be used and processed for such purposes by IntellIoT and its partners.

The ownership of the IP rights arising from the development of a project, within the scope of this program, shall belong to the corresponding SME/consortium, as referred in the signed consortium agreement.

The following aspects will be considered in the agreement:

- **Knowledge management (IPR, data, and open access):** The *IntellIoT* consortium pays particular attention to the knowledge protection (background and foreground). The knowledge management and IPR protection strategy aims to be as open as possible to achieve maximum impact of the project results, so the default rule is for results to be public.
- **Background knowledge** remains the property of the participant that brings it into the project. It is offered by the corresponding partner royalty free for the implementation of the project only.
- **Foreground knowledge** is owned by the participant(s) creating it. This can be used by any of the partners for scientific/research purposes without any other obligation. It can also be used for commercial purposes by any of the partners according to the IPR agreement, which will be signed by all partners. Further, it cannot be used by others without the permission of the corresponding partner even if this is related to scientific/research purposes.
- **Deliverables and prototypes** will be offered to the wider public through the website of the project. All other deliverables and prototypes will be protected by the IPR agreement.
- **Publication of journal and conference papers** will be uploaded to the project website.
- **Open source and standards** will be influenced by the *IntellIoT* consortium in order to provide benefits for the European community.
- **Data** generated or collected as part of the project will be carefully managed regarding privacy concerns of user related data.

ETHICS

Ethics is currently a topic in Artificial Intelligence standardization (e.g. ISO IEC JTC1 SC42), where there is a general consensus that they will not standardize ethics or ethical values. Ethical values are defined by the societal and cultural environment and may change over time. Therefore, it hardly makes sense to standardize these values and they are not a technology specific issue. What is important is that technologies may enable and provide new applications that may impact the ethical values of a society. A negative impact on these values will decrease the trust people have in the technology and hamper its acceptance by the society. Trustworthiness, the degree to which users and all stakeholders have confidence that a product or system will behave as intended, is therefore an issue for each technology. IoT

trustworthiness aspects are mainly related to privacy, security and safety. *IntellIoT* therefore proposes to focus on IoT Trustworthiness.

As the use and impact of IoT and autonomous and intelligent systems become pervasive, we need to establish societal and policy guidelines for such systems to remain human-centric, serving humanity's values and ethical principles. These IoT systems must be developed and should operate in a way that is beneficial to the users and their environment, beyond simply reaching functional goals and addressing technical problems. This approach will foster the heightened level of trust between people and use IoT technology that is needed for its fruitful use in our daily lives. Typically, IoT systems are specifically designed to reduce the necessity for human intervention in our day-to-day lives. In doing so, these new systems are also raising concerns about their impact on individuals and societies. IoT systems/Machines do not, in terms of classical autonomy, comprehend the moral or legal rules they follow. They move according to their programming, following rules that are designed by humans. This requires ethical and values-based design, development, and implementation of IoT systems, that should be guided by the following general principles:

- Human Rights: IoT shall be created and operated to respect, promote, and protect internationally recognized human rights.
- Well-being: IoT creators shall adopt increased human well-being as a primary success
- Data Privacy: IoT creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity.
- Effectiveness: IoT shall provide evidence of the effectiveness and fitness for purpose.
- Transparency: The basis of a particular IoT decision should always be discoverable.
- Accountability: IoT needs to provide an unambiguous rationale for all decisions made.
- Awareness of Misuse: IoT creators shall guard against all potential misuses and risks of IoT in operation.
- Competence: IoT creators shall specify and IoT operators shall adhere to the knowledge and skill required for safe and effective operation.

IoT systems solve many real-life problems, but they create serious ethical concerns and legal challenges related to:

- Protection of privacy
- Data security
- Data usability
- Data user experience
- Trust
- Safety, etc.

Trustworthiness is the degree to which users and all stakeholders of an IoT system have confidence that a product or system will behave as intended. Trustworthiness is a major issue for the acceptance of a technology by the society, especially if applications enabled by a new technology may have a negative impact on ethical values of the society. Standards can support adherence to ethical principles, while supporting a wide range of ethical value systems.

From an IoT point of view the following areas are of major importance when considering trustworthiness:

Privacy: due to the vast amount of personal and related data that might be gathered by IoT applications.

Information security: due to the possibility to have access IoT devices from basically everywhere in the world in case they are connected to the Internet.

Safety: in case physical equipment and processes, which can lead to harm to humans, property and the environment, are controlled via IoT.

It should be noted that these topics must be evaluated in a holistic view for a system taking its specific functionality, the environment and all deployed technologies into account. IoT may introduce specific issues, vulnerabilities and threats related to a specific topic. ISO/IEC JTC SC41 has work items on a Trustworthiness Framework and Methodology for trustworthiness of IoT system/service.

Based on above general principles, concerns and legal challenges about Ethics, to reach the aims of the *IntelliIoT* project, user and/IoT device data needs to be collected and stored, e.g., to develop distributed AI algorithms and applications.

Following paragraphs describe further details where data needs to be extracted from existing infrastructures at the clinical site, de-identified, and processed for algorithm development and validation. Additionally, patients are enabled to access, communicate and process their health-related data. These (and related) actions can raise ethical and privacy implications. Therefore, the consortium will ensure that the proposed research activities comply with all legal and ethical requirements and that all necessary measures are taken to protect the rights of any data subject that could be involved. In no case, and under no circumstances, will the consortium do research activities that involve sensitive issues without considering EU legislation and proper authorisation from the Ethics Committee of the clinical partner, PAGNI, and of the other partners involved in the data processing tasks.

To further enhance our efforts concerning the implementation of the applicable EU and national regulations and the compliance with all legal and ethical requirements, our External Advisory Board includes Prof. Dr. Nikolaus Forgó who is a prominent expert on the topics of IT law, European data protection (EU regulations and their implementation in the member states), and related ethics aspects. Prof. Forgó will regularly provide feedback and recommendations on the relevant activities of the project.

DATA PROTECTION

The sole purpose of the collection of data is to verify the eligibility of the submitted applications and to identify the best proposals. Only for the purposes of the execution of the Open Call participants will provide name and email address ("personal data"). Startup Colors UG will process the submitted material according to the European General Data Protection Regulation (GDPR).

The evaluation of the submitted applications will be done via TAIKAI (https://taikai.network) an online hackathon and idea submission management tool by LayerX Labs.

YOUR CONSENT TO THE USE OF Taikai AS SUBMISSION AND EVALUATION TOOL: By submitting your application within this Open Call you implicitly state your consent to the TAIKAI Terms and Conditions as well as the Privacy policy of TAIKAI, available under https://www.f6s.com/terms and https://taikai.network/terms

YOUR CONSENT TO THE USE OF PERSONAL DATA: By submitting your application within this competition you consent that Startup Colors UG will collect, transfer, process, store and delete your data under above-mentioned conditions.

COORDINATOR & CONTACT

The IntellIoT Open Calls are organized by the IntellIoT project consortium. Startup Colors UG is responsible for the central coordination of the Open Calls, coordinating the dissemination, application, and evaluation process.

Open Call Coordinator is:

Startup Colors UG
Pettenkoferstr. 4c, 10247 Berlin, Germany
Email: intelliot@startupcolors.com

For any enquiries regarding the IntellIoT Open Call topics and process, submission procedure, or any other general issues, please contact the coordinator.

COMPLAINTS

If, after receiving the results of one of the evaluation phases (when foreseen), you consider that a mistake has been made, you can send us your complaint. To do so please send us your complaint in English by email to: intelliot@startupcolors.com, including the following information:

- your contact details (including email address),
- the subject of the complaint,
- information and evidence regarding the alleged breach.

You have **5 calendar days** to submit your complaint starting from the day of becoming aware of the grounds for the rejection. We will review your complaint within no more than seven calendar days from its reception. If we need more time to assess your complaint, we will inform you by email about the extension.

We will not review anonymous complaints as well as complaints with incomplete information.

Please take into account that the external evaluation is run by experts in the IoT field, and we do not interfere with their assessment, therefore we will not evaluate complaints related to the results of the evaluation.

The Eligibility Check is carried out by the partners of the IntellIoT project. Should you have any concerns related to this evaluation phase, submit your complaints as described above.

PARTNERS

SIEMENS	Siemens AG (headquartered in Berlin and Munich) is a global powerhouse in electronics and electrical engineering. Operating in the fields of automation, electrification and mainly also digitalization, Siemens holds leading market positions in all its business areas. For more than 171 years, Siemens has stood for technological excellence, innovation, quality, reliability, and internationality. By discussing, sharing, and implementing ideas with scientists from outside the company, especially with 25 preferred universities and numerous research centers, Siemens researchers keep abreast of the latest findings resulting from

	fundamental and applied research all over the world. Concerning the IntellIoT Projects, three research groups will be involved: Industrial Networks, Wireless Networks and Mechatronic Systems. They combine research on communication technologies with applications such as (indoor) localization, as well as a holistic view on architectures and systems for the Internet of Things and mechatronics, such as robotic systems. This research finds its use in all Siemens business domains, e.g., in the definition and evaluation of the emerging 5G technology for the manufacturing shop floor, asset tracking for smart hospital management, the advanced engineering of intelligent office environments, or AI-based robot control.
EURECOM Sophia Antipolis	EURECOM is a graduate-level engineering school and research center that offers master and postmaster programs in the area of Digital Sciences and C-ITS. EURECOM is composed of three departments: Digital Security, Big Data and Communication Systems. The Communications Systems department (participating in this project) has a long expertise in cellular networks both from access stratum to cellular networking and management. EURECOM belongs to the Institut Mine Telecom and has 6 academics and 7 industrial members within its Economical Interest Group and is a founding member and strategy contributor to the Open5G Platform 'OpenAirInterface'. Thanks to its strong ties set up with the industry, EURECOM was awarded the "Institut Carnot" label jointly with the Institut Mines Telecom right from 2006.
AALBORG UNIVERSITET	Aalborg University (AAU) is a dynamic and innovative university of more than 20,000 students and 3,000 staff, with very strong engineering background and close ties with industry. AAU is engaged in more than 2600 externally funded research projects and has been continuously ranked among top institutions worldwide, e.g., according to US News World Ranking, as well as to the 2018 MIT report. The Department of Electronic Systems is one of the largest departments at AAU and is internationally recognized for its contributions in information and communication technology. Research activities are carried out in cooperation with industry and national and international research institutions. The project will be carried out by Connectivity (CNT) section at the Department of Electronic Systems at AAU. CNT conducts research connectivity enablers, dominantly wireless, both in fundamental and practical aspects. CNT is well-known for its pioneering results in the field of Internet-of-Things, publishing innovative and original works on short-packet communications, advanced wireless access networking schemes for massive IoT and ultra-reliable low-latency communications (URLLC). CNT staff took part in the flagship EU research projects on 5G and IoT technology.

UNIVERSITY OF OULU	The University of Oulu is an international science university that creates innovation for the future, well-being, and knowledge through multidisciplinary research and education. The involved Centre for Wireless Communications (CWC) is a large university-based research unit operating within the Faculty of Information Technology and Electrical Engineering at the University. The objective of CWC is to provide a widely recognized, high-quality international research and learning environment for its 150 research staff members thus enabling the production of cutting-edge research results and novel innovations in cooperation with its research partners. The scope of CWC spans a comprehensive range of wireless telecommunications topics. The research builds on radio channel competence, expanding through communications signal processing and radio access technologies, finally addressing the wireless internet working domain. CWC also applies basic knowledge to the application of wireless technology in several fields, including 5G, medical ICT as well as energy and environment. The 5GTN developments serve as a major validation platform for the 5G FRINGE project. Previously, CWC has been one of the few academic partners from Europe to participate in the development process of 3G and IMT-A (4G) cellular standards.
TTControl HYDAC INTERNATIONAL	TTControl GmbH is a leading supplier in the field of safety controls, displays and connectivity solutions for mobile machinery. TTControl boasts a broad experience regarding commercial production projects in the domain of electronic control systems for mobile machinery that rely on their equipment to function under the most difficult environmental conditions. TTControl is a joint venture of the TTTech Group and HYDAC International, uniting two leading technology partners for the mobile machinery market. The TTTech Group is globally oriented and formed of high-tech companies providing leading real-time networking platforms and safety controls, while HYDAC International works with well-known global customers on projects requiring fluid technology in connection with hydraulics, electronics and engineering. TTControl is headquartered in Vienna, Austria and in Bressanone/Brixen, Italy and has access to a global sales network thanks to the HYDAC and TTTech Group offices worldwide. Including contractors and freelancers, more than 130 employees are working for TTControl.
TSI	The Telecommunication Systems Institute (TSI) is a National Research Institute founded by the Greek Ministry of Education in 1995. TSI operates within the framework of the Technical University of Crete as an administratively independent entity. Its mission is to spearhead basic and applied research in telecommunications and allied areas, contribute to graduate education, service, and outreach activities, and promote technological development at the regional and national level. TSI is entirely funded from external research and development grants and contracts in telecommunications and allied areas: telecommunication systems/networks and network services, networking hardware, sensors, RF, and high-performance computing systems, machine learning, information systems, big data analytics, signal processing for telecommunications, speech, language and image processing, and biomedical

	applications. TSI has had significant experience in FP6, FP7 and H2020 projects, including FET, acting on many occasions as coordinator. It has also adopted a strategy of promoting the commercial exploitation of R&D results, by providing services and contracting with industrial partners for specific products.
	Philips is a diversified health and well-being company, focused on improving people's lives through meaningful innovation in the areas of Healthcare and Consumer Lifestyle. The company is a leader in cardiac care, acute care, digital pathology, and home healthcare. In an increasingly connected world, the convergence of Philips' consumer technologies that facilitate healthy living, medical technologies that help clinicians to deliver better diagnosis and treatment, and cloud-based technologies that enable data sharing and analysis, will be a key enabler of more effective, lower-cost integrated health solutions. This fits very well with the core strengths of Philips in professional healthcare and in consumer health and well-being. The company brings expertise in applying IoT in healthcare, integrating consumer and clinical data to create smarter and more meaningful connected consumer and care solutions, enabling seamless patient care. Specifically, to healthcare, stringent requirements for data security, privacy, and regulatory compliance, make such integration a very challenging task as well as embedded software, supporting tailor-made solutions that maximize the performance of devices. This requires a combined expertise in the cloud, IoT security, regulatory and connectivity technologies.
	Sphynx Analytics Ltd is a subsidiary company of Sphynx Technology Solutions AG, which offers solutions and consulting services, in the areas of big data analytics with a focus on analytics for cybersecurity, and for healthcare systems and services. The solutions offered are based on two core underlying technologies of its mother company Sphynx Technology Solutions, namely a model-driven big data analytics engine, and a complex event processing engine based in event calculus. Key innovative features of the analytics platform of the company include the realization of a model-driven data analytics approach in which analytics are embedded in the context of and driven by models that describe the decision-making based on the evidence arising from it, and the execution of trustworthy analytics (e.g., seamlessly embedded checks within the core computations of the SPARK platform services). Sphynx Analytics also offers consulting services and has expertise in providing customized big data analytics and cybersecurity solutions tailored to client needs as well as more general training on analytics, security assessment and cyber intelligence.
	The University of St. Gallen (HSG) was founded as a business academy in 1898, and is nowadays a School of Management, Economics, Law, Social Sciences, and International Affairs. While extending HSG's study programs towards Computer Science MSc and BSc degrees, it established its Institute of Computer Science in August 2018 with the creation of four initial chaired professorships. From HSG, the participating entity in the proposed project is the Chair of Interaction- and Communication-based Systems that is led by Prof. Dr. Simon Mayer. Within its research agenda, the team, which currently consists

	of eight individuals, explores interactions among devices and people in ubiquitous environments. Our focus is on the integration of physical things into the Web, on increasing the autonomy of Web-enabled devices and on making interactions of connected devices intelligible for people.
HOLO-LIGHT	Holo-Light is a tech company based in Munich, Germany, recognized as a pioneer in developing Augmented and Mixed Reality solutions for Enterprises, many of which are already implemented by global market leaders in several verticals and use cases. They are also pioneering in tackling the biggest issues in fully actualizing the potential of AR and MR. Through the development of deep tech, for example, they render 3D content remotely on edge computing systems and 5G infrastructures with low-latency data transmission. Their revolutionary input device Holo-Stylus (Winner in 2018 of the "German Innovation Award" and the "Auggie Award" for the best input device at Augmented World Expo in Santa Clara) allows users to naturally and precisely interact with 3D content.
AVL	AVL List GmbH is the world's largest privately-owned company for the development, simulation, and testing technology of powertrains (hybrid, combustion engines, transmission, electric drive, batteries and software) for passenger cars, trucks and large engines. AVL has about 4150 employees in Graz (Austria), and a global network of 45 representations and affiliates resulting in more than 10,000 employees worldwide. AVL's Powertrain Engineering division activities are focused on the research, design and development of various powertrains in the view of low fuel consumption, low emission, low noise and improved drivability. The Agricultural market is one of the most demanding but also exciting markets. Highest requirements and customer expectations regarding functionality, efficiency and comfort are the driving factors in this branch. One of the major challenges for the off-highway OEMs is to manage the application diversity in a cost-effective manner. Sophisticated tools and methodologies from AVL keep the development time and cost to a minimum. Based on the latest technologies, air to air communication, various sensor inputs and signal processing enable developments to optimize the complete process and increase production and quality.
Startup Colors	Startup Colors is a Berlin-based innovation and communications agency specialized in startup consulting, innovation strategy as well as ecosystem building. Founded in 2018, the agile agency is run like a startup with a team of 6 full-time and additional part-time and freelance experts. In the previous 10 years, working in the startup ecosystem in Europe, the Startup Colors team has worked with over 2000 startups. The company is a vivid supporter of international startup programs such as Startupbootcamp Digital Health Berlin, Startupbootcamp Mobility in Dubai, Techstar Retail in Berlin, Barcelona Health Hub, or enpact. Startup Colors will bring a broad, international network to technology startups into IntellIoT as well as experience in Open Call management and support. Together with very strong communication expertise, Startup Colors will be able to efficiently lead communication and coordinate the Open Calls as well as dissemination and ecosystem building activities. Further, Startup Colors will contribute to the exploitation and the definition of novel and

	disruptive business models through their experience with startups and design thinking.
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΗΡΑΚΛΕΙΟΥ	The University General Hospital of Heraklion was founded in 1989 and is the major hospital in Crete, Greece. As a University Hospital, it shares a long-standing affiliation with the University of Crete. It covers a population of approximately 650,000 and has more than 750 beds and over 1,700 staff members. It is the referral hospital for the island of Crete and all the Aegean Islands. Cardiovascular services include heart care, heart surgery, and treatment for all types of heart disease. The Department of Cardiology at the University Hospital provides comprehensive evaluation, consultation, and medical and surgical management of diseases of the heart and circulatory system. With the latest technology, skilled physicians and compassionate staff, the department provides care for abnormalities of cardiac rhythm and conduction, coronary artery disease, cardiomyopathies, heart failure and valvular heart disease. The Hospital is also at the forefront of implementing Management Information Systems technology. Further, it is working actively in the development and advance of research in the sector of medicine and other relevant sciences. In this direction, it applies and develops research projects, scientific researches and collaborates with other relevant institutions as well as with international organizations on scientific and research projects.
vidavo Healthcare Anytime Anywhere	VIDAVO, is a digital health company established in 2002. All these years it has consistently invested in scientifically proved, market focused products. Our solutions cover a wide range of connected health and self-management (mobile apps; web platforms) for supporting chronic disease (medical), nutrition and weight management (wellness). The has an impressive track record in terms of capitalizing on research outcomes and turning research results into successful commercial products. The Vida24© connected care suite is a secure modular online platform, where citizens can log and keep health records and healthcare professionals manage and process patient data, enjoy personalization tools, effective time management, and flexible UXs. Also, Vida24© provides mindfulness-based interventions and coaching using the transtheoretical model of behavior change to promote self-management and prevent chronic conditions by a healthy and active lifestyle. Vida24© is CE0653 Class IIa certified according to EU Medical Devices Regulation (MDR 2017/745).