**Request for Information (RFI): National Strategy for the Internet of Things (IoT)**

The Ministry of Digital Governance and the General Secretariat of Telecommunications and Post is focusing on developing a comprehensive national strategy for the use of Internet of Things (IoT) technology - and establishing a clear and coherent framework for their secure, responsible and regulated integration in Greece. The strategy aims to create a favorable environment for the development and use of this technology in the country, to support the development of a competitive and innovative IoT industry and to maximize the benefits for society and the economy.

In order to achieve this objective, the Greek government seeks information from stakeholders on various aspects of a national IoT strategy, inviting them to answer key questions such as:

* What are the major technological challenges facing the development of IoT devices and applications, both in terms of networking protocols and connectivity, storage capacity, data rate, security and interoperability?
* What are the specifications and requirements of IoT devices in terms of frequency spectrum and the corresponding challenges?
* What are the technological shortcomings hindering the development of IoT?
* Similarly, what are the shortcomings in the regulatory framework that hinder the development of IoT?
* What measures should the Ministry and other relevant stakeholders take to facilitate public and private investment in the field of Internet of Things?
* What opportunities are presented by the latest technological developments in the field of IoT space and which market segments benefit from the development of IoT?

This Request for Information (RFI) invites responses from companies, research organizations and other interested parties with expertise in the following areas:

**Infrastructure development:**

* Ensuring the deployment and expansion of 5G networks to provide high-speed connectivity for IoT applications, its advantages and disadvantages.
* Presentation of the main challenges for implementing high-speed connectivity for IoT applications in Greece.
* Deployment of other low power wide area networking protocols such as LoRaWAN, Sigfox, Narrowband IoT (NB-IoT), LTE-M for IoT applications that require long range communication, low data rate and low power consumption and what are the main challenges in deploying these protocols.
* Development of short-range wireless communication protocols such as Zigbee, Bluetooth Low Energy (BLE) for indoor IoT and smart home applications.
* Development of data storage, management and analysis capabilities to support the large amount of data generated by IoT solutions.
* Construction of IoT testbeds to support the development and testing of new technologies and applications.
* Listing best practices for the above technologies.
* Upgrading existing telecommunications infrastructure.

**Policy and Regulations:**

* Existing organizational and administrative structures.
* Development of policies and regulations to create a favorable environment for the development and use of IoT technology.
* Identification and addressing existing legal gaps for IoT.
* Compliance with international standards and regulations (e.g. NIS2).
* Evaluation, elaboration and adoption of regulations and legislation from other countries (e.g. Product Security and Telecommunications Infrastructure Bill-UK).
* Harmonization of regulations between different sectors to enable the development and use of IoT solutions.
* Promotion of data protection and security.
* Data protection and security, including measures such as encryption and secure communication protocols.
* Encouragement of standardization to ensure interoperability and security of IoT solutions.
* Support open data policies, where feasible, to promote transparency and innovation.
* Best practices to facilitate the development and use of IoT.

**Research and Development:**

• How to best support IoT research and development.

• How to Increase funding for academic research to develop new technologies and applications.

• How to Increase funding for companies working on IoT projects to support the commercialization of new products and services.

• How to Encourage collaboration between industry and academia to drive innovation.

• Identifying the main challenges faced by research organizations and businesses.

• Creating a conducive ecosystem for IoT innovation and development.

• Supporting the development of testbeds and experimental facilities to research and test new IoT solutions.

**Human Capital Development:**

* + Developing education and training programs to help citizens develop the skills they need to work with IoT technologies.
  + Encouraging citizen participation in IoT-related projects and initiatives in order to develop practical experience.
  + Supporting the development of specialized curricula and training programs in cooperation with academic institutions and professional bodies.
  + Implementation of educational initiatives to familiarize students with IoT technologies.
  + Rewarding and recognizing initiatives that contribute to lifelong learning and the development of IoT-related skills.

**Innovation and Entrepreneurship**:

* + Encouragement of innovation and entrepreneurship by providing tax incentives or other forms of financial assistance to companies working on IoT projects.
  + Encouragement of the creation of incubators and accelerators for IoT-related start-ups.
  + Providing successful IoT use cases and analysis of challenges.
  + Supporting IoT projects aimed at commercializing new products and services.
  + Developing a strong innovation ecosystem involving collaboration between industry and academia.
  + Providing support and incentives for the development of IoT pilot projects and initiatives.
  + Encouragement of young entrepreneurs to enter the IoT sector.
  + Strengthening the participation of Small and Medium-sized Enterprises (SMEs) in IoT projects through specific support programs.
  + Best practices and successful examples of innovation and entrepreneurship in other countries.

**Privacy and Security**:

* + Developing strong data protection and security measures for the storage, management and use of IoT-generated data.
  + Encouraging the use of best practices in data security, such as encryption and secure communication protocols.
  + Raising public awareness of the risks and benefits of the IoT and providing resources for citizens to understand and manage their personal data.
  + Working with international organizations to set standards for privacy protection.
  + Ensuring compliance with international standards and regulations for the protection of personal data on IoT devices and applications (e.g. GDPR).
  + Promoting transparency and citizen participation in privacy and security issues in the IoT sector.