United Arab Emirates

هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

REGULATORY POLICY

INTERNET OF THINGS (IoT)

Issue Date: 22 March 2018

Telecommunications Regulatory Authority (TRA)
P O Box 26662, Abu Dhabi, United Arab Emirates (UAE)
www.tra.gov.ae

CONTENTS

1. Definitions

The terms, words and phrases used in this Policy shall have the same meaning as are ascribed to them in the Telecommunications Law, unless this Policy expressly provides for otherwise, or the context in which those terms, words, and phrases are used in this Policy requires otherwise. For the purposes of this Policy, the following terms and words shall have the meanings ascribed to them below:

1.1. **"Class Authorization"** means the frequency spectrum Authorization which permits the operation of Wireless Equipment by any Person within designated frequency bands subject to the terms and conditions stipulated by the TRA.

1.2. **"Consent[1]"** means any freely given, specific, informed and unambiguous indication of the **Data Subject**'s wishes by which the **Data Subject**, by a statement or by a clear affirmative action, signifies agreement to Data Processing for data relating to them.

1.3. **"Data Classification"** means classification of data in four (4) categories[2] based on the potential adverse impact caused in case of a confidentiality breach or uncontrolled disclosure of the data:

- 'Open': Data provided by individuals, businesses or the government, to be freely or subject to a minimum limit, used or exchanged with third parties
- 'Confidential': Data, the unrestricted disclosure or exchange of which may cause limited damage to individuals, businesses or the government

[1] Adapted from 'EU General Data Protection Regulation 2016/679'. Reference to EU General Data Protection Regulation in this document are meant for information purposes only. They cannot be interpreted as incorporation of the EU General Data Protection Regulation or any other related instruments or decisions of any of the EU bodies or authorities into the UAE law. For avoidance of doubts, the UAE law shall always take precedence.

[2] Adopted from the 'Dubai Data Manual (Version 2.0)' published by Smart Dubai (June 2016)

- 'Sensitive': Data, the unrestricted disclosure or exchange of which may cause significant damage to individuals, businesses or the government
- 'Secret': Data, the unrestricted disclosure or exchange of which may cause significant damage to supreme interests of the country and very high damage to individuals, businesses and the government.

1.4. **"Data Controller[3]"** means any **Person** that, alone or jointly with other **Person**s, determines the purposes and means of **Processing** of data.

1.5. **"Data Processing[4]"** means any operation or set of operations that is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6. **"Data Processor[5]"** means any **Person** that processes data on behalf of the Controller.

1.7. **"Data Subject[6]"** means an identified or identifiable **Person** to which the data relates to.

1.8. **"Embedded SIM ('eSIM')[7]"** (also called embedded Universal Integrated Circuit Card, eUICC) means a Subscriber Identity Module (SIM) that is physically integrated into the device and cannot be removed and replaced with another SIM.

[3] Adopted from the 'EU General Data Protection Regulation 2016/679'
[4] Adopted from the 'EU General Data Protection Regulation 2016/679'
[5] Adopted from the 'EU General Data Protection Regulation 2016/679'
[6] Adopted from the 'EU General Data Protection Regulation 2016/679'
[7] As set out in GSMA 'Understanding SIM evolution, March 2015'

1.9. **"Internet of Things ('IoT')[8]"** means a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) Things based on existing and evolving interoperable information and communication technologies. The scope of this definition in context of this **Policy** is to regulate IoT within the UAE.

1.10. **"IoT Advisory Committee"** means the high-level Advisory Committee chaired by the TRA, established for IoT related matters within the UAE with representatives from various identified ministries, regulators, public sector entities and experts in IoT.

1.11. **"IoT Service"** means a set of functions and facilities offered to a user by an IoT Service Provider and it does not encompass IoT-specific Connectivity.

1.12. **"IoT Service Provider"** means any **Person** that provides an **IoT Service** to users (including individuals, businesses and the government), that will comprise the provision of IoT-related service/ solutions.

1.13. **"IoT Service Registration Certificate"** means a certificate that the TRA issues for authorizing an **IoT Service Provider** to offer **IoT Service** in the UAE.

1.14. "**IoT Service Registration Procedure[9]"** means the procedure published by the TRA for **IoT Service Provider**(s) to register their **IoT Service**(s).

1.15. **"IoT-specific Connectivity"** means connectivity that is, transmitting, broadcasting, switching or receiving IoT related data by means of a Telecommunications Network[10] covering a wide area.

---

[8] As adapted from ITU's standard ITU-T Y.2060
[9] Provided as Annexure in the IoT Regulatory Procedures document
[10] As defined in the UAE Telecommunications Law. To extend that such Network falls under the definition of a "Regulated Activity" as per the UAE Telecommunications Law such can only be provided by a licensed operator or an exemption according to Article 31 of the Telecommunications Law.

1.16. **"Licensee[11]"** means an entity which has been issued a Telecommunication license under Federal Law by Decree 3/2003, including any modifications or amendments.

1.17. **"Machine to Machine (M2M) Service[12]"** means service represented by the automated data transmission between devices using any communication channel such as wireline and wireless communication that may be carried out without any human interaction.

1.18. **"Mission Critical"** service means an **IoT Service** that if fails, may result in an adverse impact on health of individual(s), public convenience/ safety and/ or national security.

1.19. **"Over The Air (OTA)/ Remote Provisioning[13]"** means the ability to remotely change the SIM profile on a deployed SIM without having to physically access the SIM itself.

1.20. **"Person"** means a natural human being, company, public authority or any other legal entity.

1.21. **"Personal Data[14]"** means any information relating to an identified or identifiable Natural Person; an identifiable Natural Person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Natural Person.

[11] As set out in UAE Telecommunications Law
[12] Adapted from TRA's "National Numbering Plan Version 5.4"
[13] As set out in GSMA 'Understanding SIM evolution, March 2015'
[14] As set out in 'EU General Data Protection Regulation 2016/679'

1.22. **"Private Telecommunication Network"** means Telecommunication Networks operated exclusively to serve the requirements and to benefit one person or a group of persons who have a common ownership.

1.23. **"Regulated Activities"** means either the operation, supply or provisioning of a Public Telecommunications Network and/or Service to subscribers and all other types of activities specified by the Board in accordance with the provisions of the UAE Telecommunications Law.

1.24. **"Soft SIM[15]"** means a collection of software applications and data that perform all of the functionality of a SIM card but does not reside in any kind of secure storage. Instead, it would be stored in the memory and processor of the communications device.

1.25. **"Telecommunications Law"** means the Federal Law by Decree No 3 of 2003 Regarding the Organization of the Telecommunications Sector as Amended.

1.26. **"Telecommunications Regulatory Authority (TRA)"** means the General Authority for regulating the telecommunications sector in the UAE.

1.27. **"Thing(s)[16]"** means objects of the physical world (Physical Things) or of the information world (Virtual Things) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic. Physical Thing refers to a thing that exists in the physical world and is capable of being sensed, actuated and connected. Virtual Thing refers to a thing that exists in the information world and is capable of being stored, processed and accessed.

1.28. **"UAE"** means the United Arab Emirates.

[15] As set out in GSMA 'Understanding SIM evolution, March 2015'
[16] As adapted from ITU's standard ITU-T Y.2060

2. Legal Reference

This Policy has been issued by the TRA based on the powers granted to it within the articles cited below.

2.1. Article 13(2) of Federal Law by Decree No. (3) of 2003, as amended, stipulates that the TRA shall exercise its functions and powers in order to, "enhance the level of service provided by the telecommunications sector in order to promote the interests of subscribers".

2.2. Article 13(4) of Federal Law by Decree No. (3) of 2003, as amended, stipulates that the TRA shall exercise its functions and powers in order to, "encourage, promote, and develop the telecommunications and information technology industries in the State".

2.3. Article 14(7) of Federal Law by Decree No. (3) of 2003, as amended, stipulates that the TRA shall have the competence to issue regulations, instructions, decisions regulating "importing, manufacturing, using and managing Telecommunications Apparatus and issuing their respective approvals".

2.4. Article 14(8) of Federal Law by Decree No. (3) of 2003, as amended, stipulates that the TRA shall have the competence to issue regulations, instructions, decisions regulating, "the allocation of telephone numbers, numbering plans and number portability".

2.5. Article 14(9) of Federal Law by Decree No. (3) of 2003, as amended, stipulates that the TRA shall have the competence to issue regulations, instructions, decisions on, "regulating the usage of radio spectrum pursuant to the Law, including the allocation, re-allocation, usage of these frequencies and granting their authorizations".

3. Scope

3.1. The TRA intends to allow the IoT service to develop in a coordinated, coherent, safe and secure manner.

3.2. This Policy specifies the TRA's stance on regulatory aspects that underlie **IoT Service** across industries. Ministries and regulators for specific industries if required, may develop their own additional IoT-specific guidelines in coordination and consultation with the **IoT Advisory Committee** and/ or the TRA, as applicable.

3.3. This Policy shall be applicable to all Persons concerned with IoT within the UAE, including but not limited to:

- **Licensees**;
- **IoT Service Providers**; and
- **IoT Service** users including individuals, businesses and the government.

4. UAE IoT Vision and Objectives

4.1. The TRA envisions the UAE to be a leading country in development of IoT service.

4.2. The TRA has developed this IoT Regulatory Policy based on specific considerations enlisted below, in alignment with UAE's Telecommunications sector objectives:

- Providing secure IoT service
- Meeting all reasonable demands for IoT Service
- Supporting ongoing innovation
- Managing scarce resources efficiently
- Protecting the rights and interests of user of IoT
- Providing clarity for IoT market development

4.3. The TRA may issue additional regulatory instrument(s) including regulations, directives and/or guidelines, as deemed necessary that provide incentives and support for development of IoT ecosystem within the UAE.

5. Approach and Methodology

5.1. To develop this Policy in alignment with the UAE's Telecommunications sector objectives, the TRA has considered the current situation of IoT within the UAE, IoT technology trends, as well as inputs from multiple stakeholders across the IoT ecosystem and regulatory best practices.

5.2. With advances in IoT development both globally and within the UAE, the TRA may update this Policy and its associated Regulatory **Procedure** on an as-needed basis.

5.3. While this Policy covers the key requirements for IoT implementation, the TRA provides specific requirements for **Mission Critical IoT Service**. These Services require a higher level of safety and security as they may have significant adverse impact for users and the nation as a whole, in case of malfunctioning.

6. Requirements for Radio and Telecommunications Terminal Equipment (RTTE)[17] providing IoT Service

6.1. In line with the prevailing Type Approval Regulations[18] requirements, all RTTEs to be sold, offered for sale, or connected to any Telecommunication Apparatus[19] within the UAE shall require a type approval from the TRA. In case the RTTE (i) collects data/ information, and/ or (ii) is capable of

[17] As defined in the TRA's 'Telecommunications Apparatus Type Approval Policy'
[18] Telecommunications Apparatus Type Approval Regulation dated 05 April 2007
[19] As defined in the UAE Telecommunications Law

providing **IoT Service**, the RTTE shall be required to fulfil additional requirements as indicated below:

6.1.1. All key features and functionalities of the device especially involved in collecting data and/ or sensory inputs such as a camera or microphone, location identifiers, shall be indicated on the device and/ or its packaging and/ or in the user documentation.

6.1.2. The impact on the device's features and functionalities in case of unavailability of connectivity shall be indicated on the device and/ or its packaging and in the user documentation.

6.1.3. The device shall have the capability for users to reset it to factory settings.

6.1.4. Security by Design[20] shall be incorporated in the device to provide protection against unauthorized usage.

6.2. In addition to any licensing requirements for the provision of **Regulated Activities** and connectivity services, the use of RTTE equipment for the purpose of providing IoT Service in **Private Telecommunication Network** shall continue to be regulated by the Telecommunications Law, its Executive Order and decisions issued by the Board.

6.3. The TRA shall continue to follow its existing approach on Short Range Devices under **Class Authorization**. The Short Range Devices shall continue to adhere to the Authorized parameters as stipulated in the **Class Authorization**. For details on the spectrum requirements, relevant regulations and other relevant regulatory instruments must be referred to.

[20] An approach to software and hardware development that attempts to make systems free of vulnerabilities and robust to attacks to the best possible extent through continuous testing, authentication safeguards and adherence to best practices

6.4. In the context of IoT, the holder of a **Class Authorization** does not in itself entitle the holder to conduct a **Regulated Activity** in the UAE. In the context of IoT, a **Class Authorization** can only be used for the operation of wireless equipment for provision of registered IoT Service as per the **IoT Service Registration Certificate** issued by the TRA and not for any further unspecified operation of wireless equipment.

6.5. Any **Person** that intends to provide **IoT-specific connectivity** shall directly approach the TRA. The TRA shall conduct a case-by-case assessment to consider whether awarding a license for deployment and operation of an **IoT-specific connectivity** network within the UAE is necessary subject to the Telecommunications Law and the licensing regime in place at the time.

6.6. For the purposes of IoT, the TRA shall permit use of both physical SIMs and **eSIMs**[21]. Use of Soft SIMs shall require a prior approval from the TRA.

6.7. The TRA encourages wider adoption of **OTA/ remote provisioning** for devices that are used for provisioning of **IoT Service**. The TRA has the right to stipulate mandatory **OTA/ remote provisioning** requirements for specific[22] **Mission Critical IoT Service**.

6.8. The TRA encourages all entities to transition to IPv6.

7. Requirements for IoT Service Providers

7.1. Ability to offer IoT Service does not allow the IoT Service Provider to perform any Regulated Activity which is defined in the UAE Telecommunications Law.

[21] The detailed procedure for usage of eSIMs has been indicated in the IoT Regulatory Procedures
[22] Potentially IoT Service that require mass deployment of devices with SIMs

7.2. Any **Person** offering **IoT Service** to the UAE market irrespective of its place of establishment, management or operations, shall be subject to the UAE Telecommunications Law and any regulatory framework related to **IoT** including this present Policy.

7.3. **IoT Service Provider** shall register at TRA to provide **IoT Service** and obtain **IoT Service Provider Registration Certificate.** As a prerequisite, the **IoT Service Provider** shall have a local presence or it can appoint an official representative that shall be responsible for communication with the TRA and other law enforcement agencies in the UAE and must be physically present within the UAE.

7.4. All **IoT Service Providers** shall register their **IoT Service** with the TRA by following the procedure prescribed in the **IoT Regulatory Procedures document** to obtain the **IoT Service Registration Certificate**.

7.5. Ensure that the **IoT Service** provided are adequate, reliable and meet the expected quality standards of performance for the users of such service.

7.6. In case of **Mission Critical IoT Service, IoT Service Providers** shall be required to:

7.6.1. Fulfil additional requirements stipulated by TRA including maintenance of subscriber information such as enlisted below. These requirements and information shall be provided by the **IoT Service Provider** upon TRA request.

- Subscriber's name, address and ID
- Device's model and registration number
- Any other information that the TRA may stipulate from time to time

- In addition to adherence to the requirements as stipulated in this Policy, the **IoT Service Providers** shall also comply with respective policies and stipulations from concerned authorities within the UAE

7.7. Subject to competent UAE authorities developing further regulations concerning data management and protection, the TRA has herein proposed specific stipulations for management of data in order to protect user privacy and national security within the UAE. Public authorities in UAE will retain the right of processing data within the purview of the legislative powers provided to them.

7.8. For storage of data, the **IoT Service Providers** shall follow the specific principles and stipulations as defined below.

7.8.1. The **IoT Service Providers** shall follow specific principles for storage of data:

7.8.1.1. *'Purpose limitation'*: Data shall be collected for specified, explicit and legitimate purposes only and shall not be further processed in a manner that is incompatible with those purposes

7.8.1.2. *'Data minimization'*: Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

7.8.1.3. *'Storage limitation'*: Data shall be kept in a form that permits identification of **Data Subjects** for no longer than is necessary for the purposes for which the data is processed

7.8.2. The **IoT Service Providers** shall implement the following stipulations for storage of data.

7.8.2.1. '**Secret**', '**Sensitive**' and '**Confidential**' data for individuals and businesses shall primarily be stored within the UAE. However, such data may be stored outside of the UAE provided that the destination country for data storage meets or exceeds any data security and user protection policies/regulations followed within the UAE. These stipulations shall also apply to Personal Data as the TRA deems Personal Data to be Secret data for individuals.

7.8.2.2. '**Secret**', '**Sensitive**' and '**Confidential**' data for the government shall remain within the UAE under all circumstances.

7.8.2.3. '**Open**' data for individuals, businesses and the government may be stored, within the UAE and/ or outside of the UAE.

7.9. The **Data Processors** shall establish technical measures towards enabling inspection of the data stored and/ or transported, by relevant public authorities in the UAE within purview of their legislative powers.

7.10. The existing legal and regulatory requirements for interception and monitoring of data by the law enforcement agencies in the UAE shall be applicable to all **IoT Service Providers**.

7.11. The **IoT Service Providers** shall use an encryption standard that fulfills requirements of the competent UAE authorities. In instances where an **IoT**

Service Provider uses or intends to use an encryption standard higher than the approved one, the **IoT Service Provider** shall seek an explicit case-by-case approval from the TRA.

7.12. The **IoT Service Provider** shall comply with any directions as the TRA or other competent authority may issue from time to time on matters relating to public interest, safety and/or national security.

8. Requirements for Licensees

8.1. **Licensees** who intend to provide **IoT Service** shall follow the procedure indicated in the **IoT Regulatory Procedures** document to obtain the **IoT Service Registration Certificate.**

8.2. **Licensees** within the UAE can provide **IoT Service** using their assigned frequency spectrum as well as the frequency spectrum available under **Class Authorization**.

8.3. The TRA has implemented a numbering plan[23] for **M2M** Services. The **M2M** numbering can be used for **IoT Service** where applicable. For details on numbering, please refer to the TRA's National Numbering Policy.

8.4. The **Licensees** shall be able to differentiate numbers assigned for **Mission Critical IoT Service** at all times. In case **Licensees** are unable to maintain a clear distinction of such numbers, the TRA may support the **Licensees** with assignment of block(s) within the **M2M** numbering range, if required.

8.5. The TRA exercises forbearance on roaming of **IoT** devices. However, it may subsequently issue necessary regulations as needed.

[23] National Numbering Plan Regulatory Policy issued 07th December 2016

8.6. Licensees are required to enable **OTA/ remote provisioning** for **IoT Service Providers** when such capabilities are requested.

9. Governance for IoT Regulation

9.1. The **IoT Advisory Committee**, chaired by the TRA, shall be responsible for evaluation of **IoT Mission Critical Service** that require a cross-industry assessment within the UAE, with the following responsibilities:

9.1.1. Provision of inputs for Mission Criticality assessment of services and recommendations on the conditions to be stipulated for **IoT Service Registration**.

9.1.2. Identification and revision of violations/ disputes with regards to **IoT Mission Critical Service** that require a cross-industry assessment and issue related recommendations.

9.1.3. Recommendations for formulation/ update of policies/ guidelines for regulation of IoT on an ongoing basis in line with advances in technologies and services and issue related recommendations.

9.2. The **IoT Advisory Committee** members shall decide the frequency and agenda of their meetings. The proceedings from each such meeting shall be duly documented and shared with the **IoT Advisory Committee** members.

9.3. A transition period of one year from the Effective Date of this Regulatory Policy, as specified in Article 11, shall be provided for existing **IoT Service** to be registered with the TRA.

9.4. Any **Person** that is associated with provisioning or usage of **IoT Service** within the UAE and does not comply with this Policy and/ or UAE's Telecommunications regulations, may be penalized by the TRA as per penalties defined within the UAE Telecommunications Law and/ or other relevant regulations, including temporary or permanent suspension of their services.

9.5. Non-compliance with any of the provisions of this Policy shall be considered as a breach of the UAE Telecommunications Law, and this Regulatory Policy. The TRA shall report such breach to the concerned authorities.

9.6. Notwithstanding the generality of article 9.5, this Policy defines the following actions as violations/breach of this Policy:

- providing **IoT-specific connectivity** without being licensed to do so by the TRA;
- providing an **IoT Service** for public use, that is, beyond Personal use to other **Persons**, without registering it with the TRA;
- providing **Mission Critical IoT Service** by **IoT Service Provider** and not having the up-to-date required information about their subscribers
- not implementing the defined **consent** administration for **Data Processing**;
- not adhering to the stipulated data storage requirements;
- providing and activating Soft SIMs in the UAE without approval from the TRA; and
- not providing **OTA/ remote provisioning** in services where the TRA stipulates mandatory provisioning of **OTA/ remote provisioning**.

10. Compliance with Concurrent Obligations

10.1. It is the responsibility of the relevant **Licensee** and **IoT Service Providers** to ensure that before any **IoT Service** is introduced, it is in compliance with

the TRA's entire Regulatory Framework as well as any conditions imposed by any other competent authority.

10.2. Under no circumstances shall an approval with respect to this Regulatory Policy be construed as a waiver or excusal of any other relevant conditions or obligations.

11. Effective Date and Publication

This Regulatory Policy shall take effect on the date of issue and shall be published in the official gazette.