AFRIDI & ANGELL
LEGAL CONSULTANTS

Since 1975

inBrief

New UAE Regulatory Policy for the Internet of Things

By James Bowden and Deniz Ghazal | 4 July 2019

Along with the prediction that the continued growth of the Internet of Things (**IoT**) will transform our everyday lives and how we do business, we can also anticipate that the increased number of connected devices will bring about additional challenges, including greater security and privacy-related risks. In light of these challenges, the UAE Telecommunications Regulatory Authority (the **TRA**) has recently laid the groundwork for regulating IoT by introducing a regulatory policy (the **IoT Policy**) and a set of regulatory procedures (**IoT Procedures**) that give the TRA control and oversight over IoT services in the UAE while also setting forth some data protection-related principles. It is important that those that provide IoT services to the UAE market understand their obligations under the TRA's IoT Policy going forward.

What is IoT?

When we speak of IoT, we generally refer to the network of everyday physical objects or devices connected to the Internet, which are able to communicate with other devices and collect and exchange data through software, embedded electronics, sensors and other forms of hardware. These devices can be consumer-based, such as wearables, cars, speakers, and smart home devices and appliances, as well as industry-based objects, such as intelligent medical devices, security systems, and machinery and robots used in factories.

In the IoT Policy, IoT is broadly defined as "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".

Who is Subject to the IoT Policy?

The IoT Policy is applicable to all individuals, companies, public authorities, and other legal entities concerned with IoT within the UAE. This includes IoT Service Providers that are located in the UAE as well as foreign-based IoT Service Providers providing services remotely to the UAE market.

The Authors

James Bowden
Partner
jbowden@afridi-angell.com
Tel: +971 4 330 3900

James heads the data privacy and cyber security practice at Afridi & Angell. He advises companies in the TMT sector on industry specific regulatory compliance as well as on general corporate and commercial matters. Prior to joining Afridi & Angell, James gained in-depth technology outsourcing experience while working as in-house counsel with one of Canada's leading technology companies. He is a member of the Ontario Bar.

Deniz Ghazal
Knowledge Manager
dghazal@afridi-angell.com
Tel: +971 4 330 3900

Deniz is responsible for the delivery of all aspects of legal knowledge management for Afridi & Angell, including the monitoring of legal, regulatory, and market developments in the UAE. She has been a practicing corporate lawyer since 2001 and has experience in the US as well as in Turkey advising on cross-border acquisitions, capital markets transactions, and financing. Deniz is admitted to practice law in the US in New York, California and New Jersey.

The TRA defines an IoT Service Provider as any individual, company or public authority that "provides an IoT Service to users (including individuals, businesses and the government) that will comprise the provision of IoT-related service/solutions". In addition, an IoT Service is considered to be any "set of functions and facilities offered to a user by an IoT Service Provider", other than IoT-specific Connectivity (which is generally the type of activity that is provided by a network service provider). The TRA's wide-reaching definition of IoT Service Provider and IoT Service would likely capture traditional IT providers offering IoT related services or solutions to businesses located in the UAE as well as foreign companies bringing IoT related products to the market, such as cars and smart home devices and appliances.

Requirements under the IoT Policy

The following are some of the principal requirements under the IoT Policy:

Registration and Local Presence. All IoT Service Providers must register with the TRA and obtain a registration certificate. To obtain a registration certificate, the IoT Service Provider is required to have a local presence or an appointed representative physically present in the UAE to be responsible for communicating with the TRA and law enforcement agencies. It also must have registered its IoT Service with the TRA pursuant to the IoT Procedures.

Mission Critical IoT Service. If an IoT Service is characterised as Mission Critical (*i.e.*, any service that if it fails, may result in an adverse impact on the health of individuals, public convenience or safety or national security), then the IoT Service Provider is required to meet additional requirements stipulated by the TRA, including maintenance of subscriber information.

Soft SIMS. The TRA requires prior approval for the use of Soft SIMs. A Soft SIM refers to 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. Rather, the Soft SIM is stored in the memory and processor of the communication device.

Type Approval. Any Radio and Telecommunications Terminal Equipment (**RTTE**) as defined in the TRA's type approval policy that is to be sold, offered for sale or connected to any Telecommunication Apparatus within the UAE, requires a type approval from the TRA. In addition, if the RTTE collects any data or information or is capable of providing IoT Service, then it must also meet additional requirements set forth in the IoT Policy.

IoT-specific Connectivity. Any person that intends to provide IoT-specific Connectivity must contact the TRA to obtain a license, and the TRA will conduct a case-by-case assessment to consider whether awarding such a license is necessary subject to the Telecommunications Law (Federal Decree Law 3 of 2003) and the licensing regime in place at the time.

Data Protection

In addressing data protection, the IoT Policy focuses on data storage and the location of stored data. It should be noted that while drafting these provisions on data protection, we can see that the TRA has looked to existing international standards as well as Dubai's own policies as many of the data protection-related terms and principles contained in the policy have been adopted from the General Data Protection Regulation (EU) 2016/679 (the **GDPR**) and the Dubai Data Manual published by Smart Dubai in 2016.

Data Storage. IoT Service Providers must adhere to the following principles:

- Purpose Limitation – Data must be collected for specified, explicit and legitimate purposes only and cannot be further processed in a manner that is incompatible with these purposes.
- Data Minimisation – Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Storage Limitation – Data must 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.

Data Localisation. Essentially, data must be classified based on the potential impact that will be caused in the event of a confidentiality breach or uncontrolled disclosure, and where data is to be stored depends on its classification. The TRA has set out four categories of classification, Open, Confidential, Sensitive, and Secret. Each of these classifications is defined in the IoT Policy and has been adopted from the Dubai Data Manual.

Data that is considered Secret, Sensitive or Confidential for individuals and businesses must be primarily stored within the UAE. However, this type of data may be stored outside of the UAE provided that the destination country meets or exceeds the UAE's data security and user protection policies and regulations. Personal Data (as defined in the GDPR) will be classified as Secret Data for individuals. If any data is classified as Secret, Sensitive or Confidential Data for the government, then it must always be stored in the UAE. Finally, data that is classified as Open Data for individuals, businesses or the government may be stored in the UAE or abroad.

Compliance with the IoT Policy

Although the IoT Policy and IoT Procedures have only recently been made available to the public, they have been in effect since 22 March 2018 and 6 March 2019, respectively. In addition, the one-year transition period set out in the IoT Policy has elapsed. Therefore, unless an additional grace period is given, IoT Service Providers must immediately begin compliance with this new regulatory framework. Otherwise, noncompliance may result in the temporary or permanent suspension of services and may be considered as a breach of the Telecommunications Law, which could result in the imposition of fines and/or imprisonment.

Further Thoughts

The practical implications of the IoT Policy and IoT Procedures that are immediately obvious are the requirements that relate to data protection noted above. While the UAE (outside of the DIFC and ADGM) has not yet adopted a data protection law, the IoT Policy and Procedures have the effect of adopting certain key elements of a modern data protection regime and making them applicable to IoT Service Providers. This could be construed to apply to anyone who collects data remotely, if a liberal view is taken, as it could be difficult to draw a line between devices that collect and transmit data which do qualify as IoT devices, versus that which still collect and transmit data (like a mobile phone) which do not qualify as IoT devices. It may be that all such devices effectively are treated as IoT devices, and the result will be that different data protection regimes apply in the UAE depending on whether the data was transmitted by a device as opposed to collected directly or with pen and paper. We anticipate that this inequality of treatment under the law will be a transient phase as the UAE moves uniformly towards a consistent data protection regime, but businesses and advisors will need to be aware of this dichotomy in the meantime. It is easy to speculate that there may also be TRA approval required for importation of IoT devices too, to enable them to maintain a record or registry of IoT devices operating in the UAE.

We will provide further updates as this important area of regulation evolves. ■

Afridi & Angell

Founded in 1975, Afridi & Angell is a full-service UAE law firm in its fifth decade at the forefront of the legal community. From the beginning, our hallmarks have been a commitment to quality, unsurpassed knowledge of the law and the legal environment, and crafting of innovative business solutions. Licensed in the three largest Emirates of Abu Dhabi, Dubai and Sharjah as well as the Dubai International Financial Centre, our practice areas include banking and finance; corporate and commercial law; arbitration and litigation; construction; real estate; infrastructure projects; energy; project finance; maritime (wet and dry); and employment. We advise local, regional and global clients ranging in size and sophistication from start-ups, sole proprietorships, family-owned businesses, entrepreneurs and investors to some of the world's largest public and private companies, governments and quasi-government institutions. We attract and retain clients with our dedication to practical guidance focused on their business needs supported by decades of experience here in our home jurisdiction, the UAE.

Afridi & Angell is the exclusive member firm in the UAE of top legal networks and associations, most notably Lex Mundi, the world's leading network of independent law firms, and World Services Group.

www.afridi-angell.com

Afridi & Angell's inBrief provides a brief overview and commentary on recent legal announcements and developments. Comments and opinions contained herein are general information only. They should not be regarded or relied upon as legal advice.