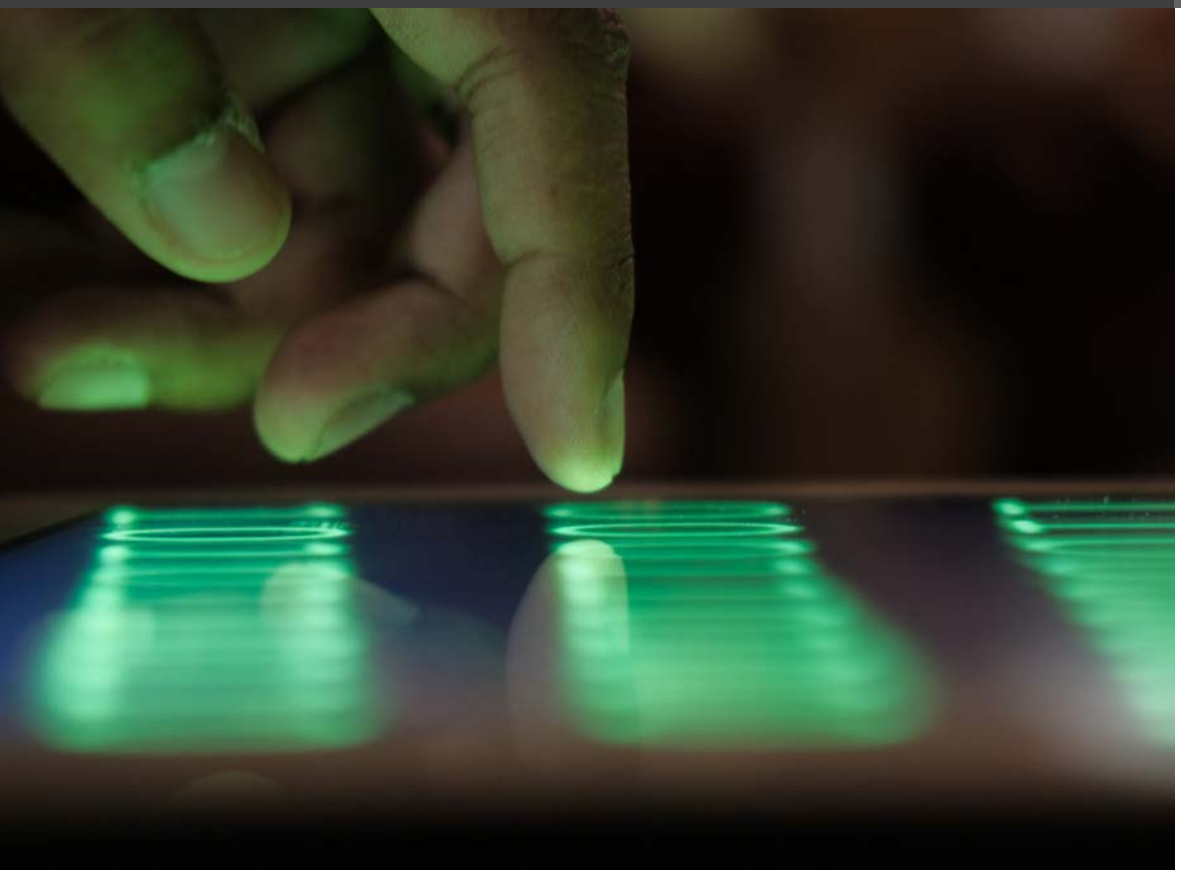
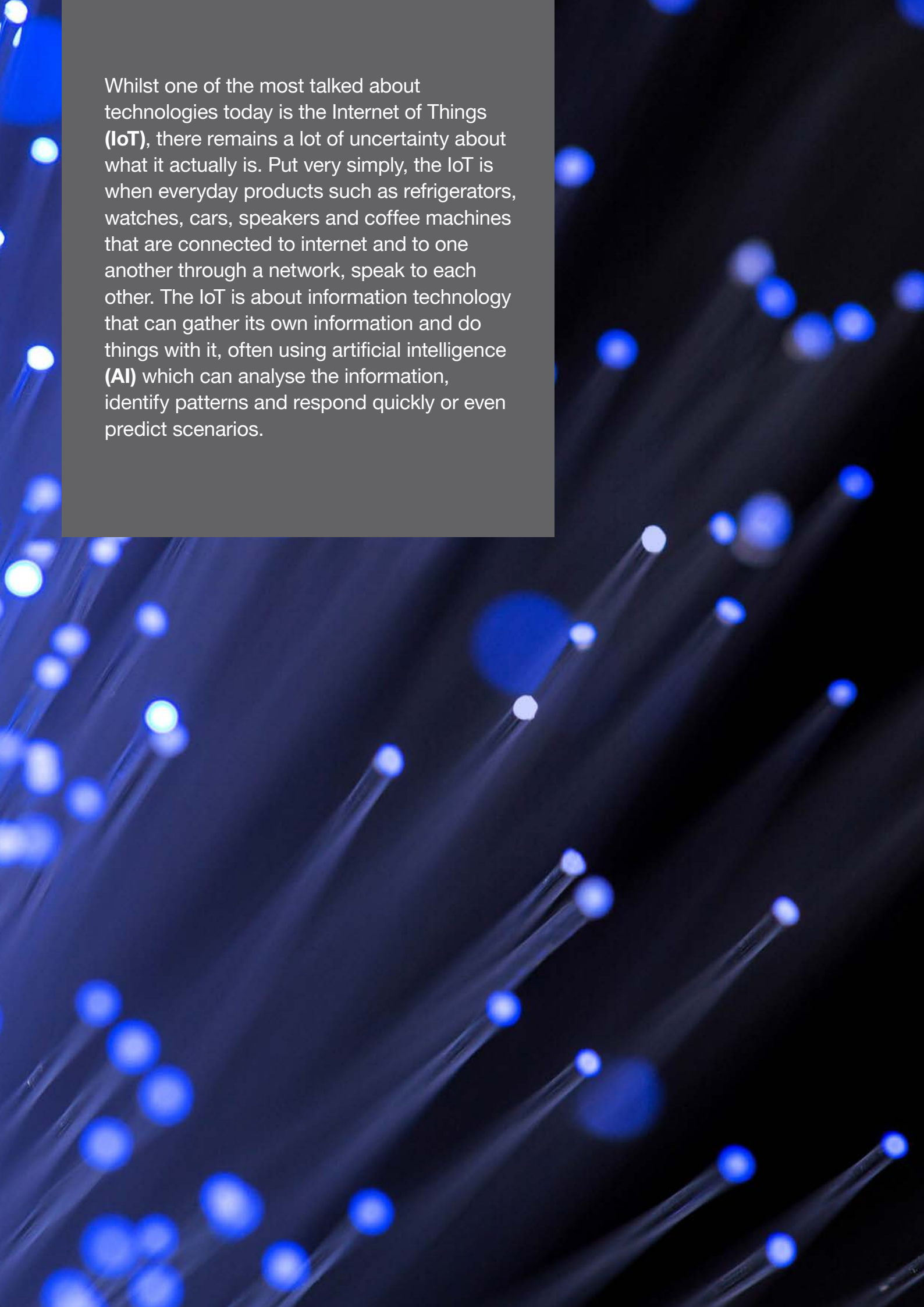
Regulating the Internet of Things in the UAE



pwc

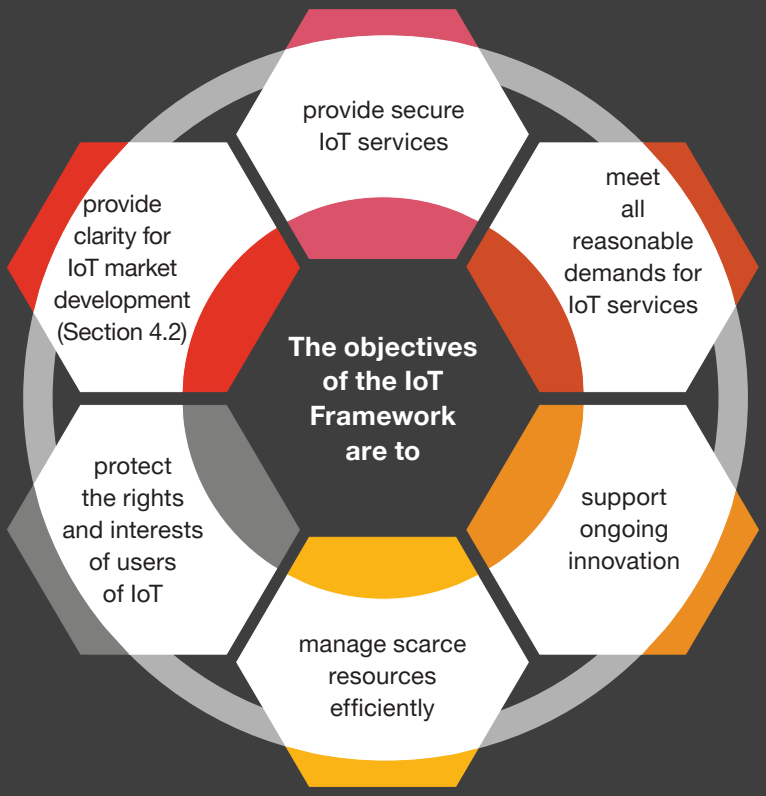


Whilst one of the most talked about technologies today is the Internet of Things **(IoT)**, there remains a lot of uncertainty about what it actually is. Put very simply, the IoT is when everyday products such as refrigerators, watches, cars, speakers and coffee machines that are connected to internet and to one another through a network, speak to each other. The IoT is about information technology that can gather its own information and do things with it, often using artificial intelligence **(AI)** which can analyse the information, identify patterns and respond quickly or even predict scenarios.

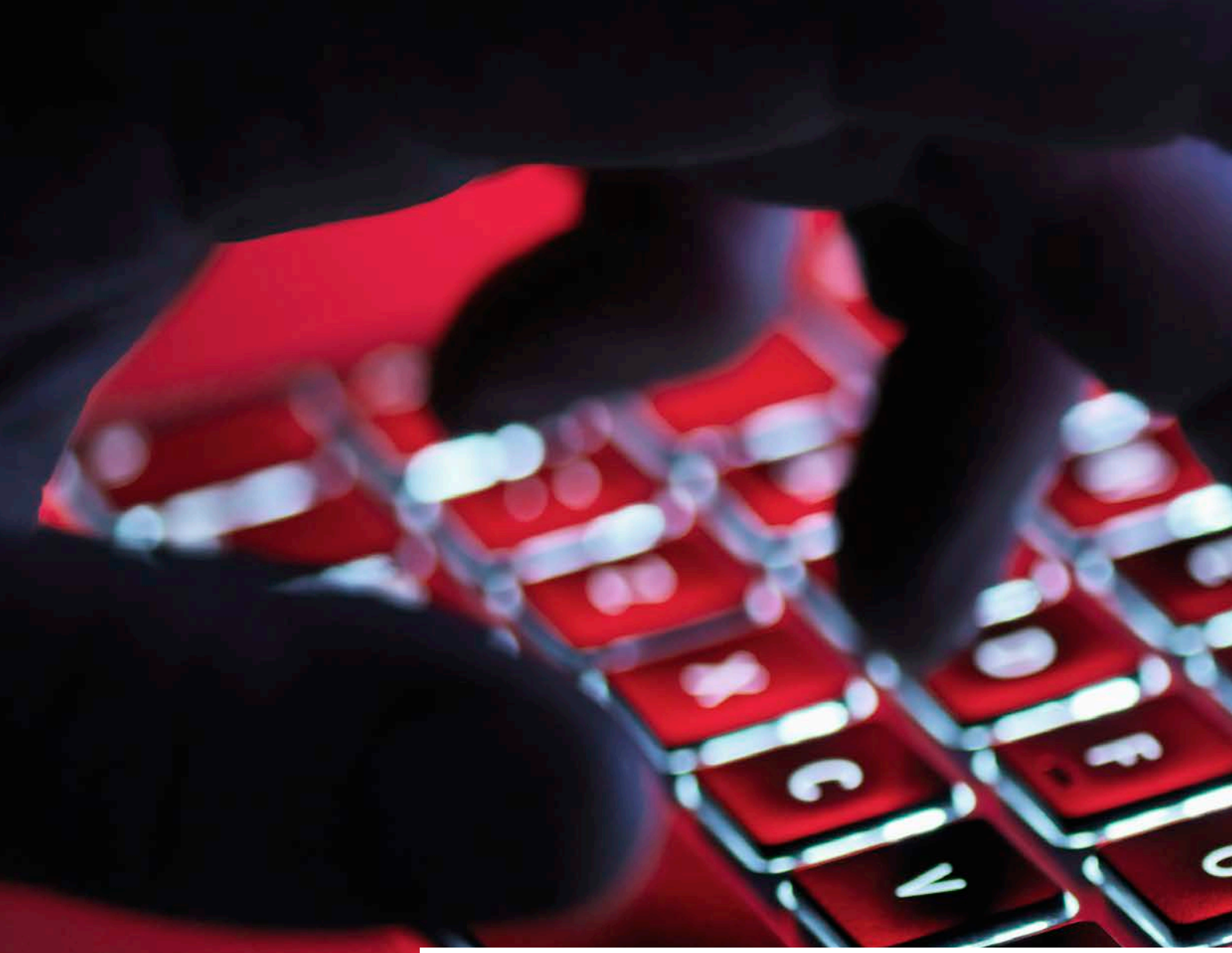
So what does this practically mean in the real world? Well, how would you like your car to send a text or email to a contact in your phone to notify them that you are stuck in traffic and will be late for a meeting? Even go back a step – how about your car having access to your daily calendar and being able to plan the best route to take in light of traffic, weather etc. before you even wake up? We can go back even further – how about your alarm clock telling your coffee machine that your alarm is set for 6.30am and to start brewing your morning coffee at 6.25am? In the office, what about your computer and your chair telling your air conditioning that at certain times of the day and at certain temperatures, you work most effectively? The possibilities are endless.

Research from TechRadar indicates that investment in IoT over the next 12 months in the UAE alone will increase from $574.89m to $672.75m. It is with this mind that the UAE's Telecommunications Regulatory Authority **(TRA)** recently published a new IoT regulatory policy **(IoT Policy)** and IoT regulatory procedures **(IoT Procedures** and together the **IoT Framework**). The IoT Framework aims to develop and regulate, **'in a coordinated, coherent, safe and secure manner'**, IoT in the UAE and secure UAE's position as a global leader in the IoT sphere. Keen eyes will note that although both documents were only made available very recently, they are dated 22 March 2018 and 6 March 2019 respectively meaning that the 12-month transition period provided for in the IoT Policy (from the date it was issued) has now ended. Compliance starts now.

Purpose of the IoT Framework



To meet these objectives and in recognition of the dynamic nature of IoT technologies, the IoT Policy states that the TRA may issue further regulatory guidance, directives and/or regulations to provide incentives and support the UAE IoT ecosystem (Section 4.3). Alongside the TRA, UAE ministries and industry regulators may also develop their own additional IoT-specific guidelines through co-ordination and consultation with the IoT Advisory Committee and/or the TRA (Section 3.2). The IoT Advisory Committee was established for IoT-related matters in the UAE and is comprised of representatives from various identified ministries, regulators, public sector entities and IoT experts (Section 1.1). It is chaired by the TRA.



What does the IoT Framework apply to?

The IoT Policy provides a more detailed technical definition of IoT, calling it **'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'** (Section 1.9). With that in mind, the IoT Framework regulates the provision of 'IoT Services', which are any functions or facilities consisting of IoT-related services and/or solutions to users located in the UAE. Notably, the IoT Framework specifically states that it does not apply to 'IoT-specific Connectivity', which is the transmission, receiving, broadcasting or switching of IoT-related data over a telecommunications network.

Who does the IoT Framework apply to?

The scope of the IoT Framework is broad and applies to **'all persons concerned with IoT within the UAE'**, including but not limited to:

- telecommunications service providers
- 'IoT Service Providers'
- users of IoT Services (i.e. individuals, businesses and government).

An IoT Service Provider is any person/business that provides IoT Services in the UAE and includes, but is not limited to IoT network provider platforms (e.g. Salesforce IoT Cloud) and machine-to-machine connectivity providers.

An interesting aspect of the IoT Framework is that has extraterritorial application meaning that any person or organisation established, located, managed or operated from outside of the UAE that remotely offers IoT Services to UAE-based customers will be caught (Section 7.2).

The IoT Framework also states that those entities considered to be IoT Service Providers that are not established in the UAE must either:

- establish a presence in the UAE (which can be either onshore or in one of the free zones); or
- appoint an official representative based in the UAE who will be responsible for all communications with TRA and UAE law enforcement agencies.

What does the IoT Framework require IoT Service Providers to do?

The IoT Framework sets out a number of compliance considerations for IoT Service Providers that include:

Registration

All IoT Service Providers must register with the TRA to obtain and IoT Service Registration Certificate prior to providing any IoT Services. For IoT Service Providers providing 'Mission Critical IoT Services', there are additional registration requirements including:

- maintaining records of subscriber information (e.g. subscriber's name, address and ID, the device's model and registration number)
- adhering to policies and/or stipulations from other UAE authorities.

Mission Critical IoT Services are IoT Services that **'may result in an adverse impact on the health of individual(s), public convenience/ safety and/or national security'** if they were to fail.

Data Privacy and Protection

The IoT Framework contains terms and concepts drawn from established and accepted international best data protection practices and principles including from the EU General Data Protection Regulation (**GDPR**). These include that IoT Service Providers must:

- only collect data for specified and lawful purposes and not use that information for any reason that would be incompatible with those purposes **(purpose limitation)**
- only collect as much data from users as is actually needed in order to achieve the above purposes and no more **(data minimisation)**
- retain this data only for so long as it is actually needed in order to achieve the above purposes and no longer unless the law requires otherwise **(storage limitation)**
- use data encryption standards that fulfil the requirements of the competent UAE authorities.
- when developing software and hardware, 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' are made **(privacy by design)**
- classify data collected on the basis of the anticipated harm that could result should such information be disclosed without consent **(data classification)**
- based on how the data is classified, comply with the data localisation requirements prescribed for each category of data.

The categories of data are:

i. **Open data** – data freely provided by individuals, businesses or government that can be freely, or subject to only minimum limitations, shared with third parties
ii. **Confidential data** – data that if disclosed without restriction may cause limited harm to the individual, business or government
iii. **Sensitive data** – data that if disclosed without restriction may cause significant harm to the individual, business or government

iv. **Secret data** – data that if disclosed without restriction may cause significant damage to the supreme interests of the UAE and very high damage to the individual, business or government.

On the basis of the above, the data localisation requirements are:

i. Open Data – may be stored either in the UAE or abroad

ii. 'Confidential', 'Sensitive' or 'Secret' – where it relates to individuals and businesses, it shall primarily be stored in the UAE (unless certain adequacy requirements* are satisfied)

iii. 'Confidential', 'Sensitive' or 'Secret' – where it relates to the UAE government, must be stored in the UAE without exception.

It must be noted that whilst none of the above obligations actually refer to personal data, the TRA considers this to be Secret Data and therefore should be treated as such.

*Adequacy requirements mean that these categories of data may be stored, for example on a server, outside the UAE where the country in question meets or exceeds the data security and user protection policies/ regulations in the UAE.

SIMs

The use of both physical SIM cards and embedded/eSIMs are allowed for IoT Services but the use of any software that performs all the operations of a SIM card but is located in the memory and processor of the communications device (e.g. mobile phone) rather than any kind of secure physical storage (i.e. Soft SIMs) requires prior approval from the TRA.

Type approval

All radio and telecommunication equipment capable of collecting data and/or capable of providing IoT Services must, in addition to complying with the UAE Type Approval Regulations, comply with the following:

- indicate the features and functions of the device that collects data including sensory inputs such as cameras, location identifiers, and microphones;
- indicate the impact on the device's features or use in case of unavailability of connection;
- the device shall be capable of being reset to its original settings; and
- that 'Security by Design' be an incorporated feature to combat unauthorised usage.

IoT Device roaming

The IoT Framework states that the TRA will **'exercise forbearance'** on the roaming of IoT devices for now, but may implement future regulations on this subject at its discretion.

IoT Specific connectivity

Persons or organisations that want to provide the underlying connectivity for IoT Services will require a separate licence from the TRA to do so. Applicants for this licence will be considered by the TRA on a case-by-case basis.

What if you fail to comply with the IoT Framework?

The IoT Framework refers to the UAE Telecommunications Law (Federal Law by Decree No. 3/2003) for the range of penalties that may be imposed by the TRA for a breach of the IoT Framework. These include:

- temporarily or permanently suspending a business's right to provide IoT Services
- potential imprisonment for not less than 1 year; and/or
- fines between AED50,000 – AED200,000.

In addition, any breach of the IoT Framework will constitute a breach of the Telecommunications Law. The IoT Framework helpfully lists a number of actions that will be considered to violations of its provisions. These include, but are not limited to:

- providing services without a licence
- not having up-to date information of subscribers in regard to Mission Critical IoT Services
- non-adherence to defined consent requirements for data processing
- non-adherence to data localisation requirements
- provision or activation of Soft SIMS without TRA approval.

What do organisations needs to do next?

The introduction of the IoT Framework by UAE reflects a growing trend across the Gulf region to regulate specific sectors of the market and technologies in response the proliferation of market actors and the perceived consumer risks they present.

Providers of IoT Services in the UAE are recommended to take the following actions:

- assess your current operations and ensure that they are in compliance with the IoT Framework
- fully inform yourself of the registration requirements set out in the IoT Procedures and assess whether or not any current or proposed activities will give rise to any registration or licensing obligations
- consider creating a register of the types of data collected, categorise these based on the categories set out above (open, confidential, sensitive and secret) and ensure that each category of data is held in accordance with the relevant data localisation requirements (i.e. inside or outside the UAE)
- be mindful that the IoT Framework is likely to be just one of a number of similar policies that will emerge across the Middle East as the region becomes a 'smarter' and more connected.

Contacts

Legal Services

Richard Chudzynski
Legal Data Protection and Privacy Leader

M: +971 56 417 6591
E: richard.chudzynski@pwc.com

Gordon Wade
Senior Data Protection and Privacy Lawyer

M: +971 50 143 5619
E: gordon.wade@pwc.com

Digital Trust

Matt White
Partner, Head of Digital Trust

M: +971 56 113 4205
E: matt.white@pwc.com

Phil Mennie
Partner

M: +971 56 369 7736
E: phil.mennie@pwc.com

190710-101211-HO-OS