Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

TMT

UAE
Eversheds Sutherland

chambers.com

2019

Law and Practice

Contributed by Eversheds Sutherland

Contents

1. Cloud Computing p.4
- 1.1 Laws and Regulations p.4
- 1.2 Regulations in Specific Industries p.4
- 1.3 Processing of Personal Data p.4

2. Blockchain p.4
- 2.1 Risk and Liability p.4
- 2.2 Intellectual Property p.5
- 2.3 Data Privacy p.5
- 2.4 Service Levels p.5
- 2.5 Jurisdictional Issues p.5

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence p.5
- 3.1 Big Data p.5
- 3.2 Machine Learning p.6
- 3.3 Artificial Intelligence p.6

4. Legal Considerations for Internet of Things Projects p.6
- 4.1 Restrictions Affecting a Projects' Scope p.6

5. Challenges with IT Service Agreements p.7
- 5.1 Specific Features p.7
- 5.2 Rules and Restrictions p.8

6. Key Data Protection Principles p.8
- 6.1 Core Rules Regarding Data Protection p.8
- 6.2 Distinction Between Companies/Individuals p.8
- 6.3 General Processing of Data p.8
- 6.4 Processing of Personal Data p.8

7. Monitoring & Limiting of Employee Use of Computer Resources p.9
- 7.1 Employees' Restrictions on Computer Use p.9

8. Scope of Telecommunications Regime p.9
- 8.1 Technologies within Local Telecommunications Rules p.9

9. Audiovisual Services and Video channels p.10
- 9.1 Main Requirements p.10
- 9.2 Online Video Channels p.11

10. Encryption Requirements p.11
- 10.1 Legal Requirements Governing the Use of Encryption p.11

Eversheds Sutherland has a team of 15 TMT lawyers, including seven partners, covering all of the UAE and the wider region. In the UAE it has offices in Abu Dhabi and Dubai, with additional regional offices in Amman, Baghdad, Erbil, Doha and Riyadh, and a team of over 100 lawyers in total. The firm's lawyers are qualified and experienced in common and civil law jurisdictions, and have combined linguistic skills in over ten languages, including Arabic, English and French. It is an integrated regional and international practice, combining international standards with a uniquely embedded knowledge of local custom, practice and culture. The TMT team in the Middle East and North Africa region is supported by lawyers across the firm's international network, particularly in the UK and USA. The key areas of practice in relation to the TMT sector are dispute resolution, IP, IT, data protection, commercial and contract law, corporate (including M&A), media law, technology and telecommunications regulatory/policy, and real estate (including data centres).

Authors

Nasser Ali Khasawneh is co-global head of the TMT practice, chairman of the Middle East practice and managing partner of the firm's UAE practice. Nasser has expertise in dispute resolution, IP, and technology and media law in the United Arab Emirates and regionally. He has been a domain name panellist with the World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre in Geneva since 2003 and was co-chair of the Arab Regional Forum, one of the committees within the International Bar Association (IBA), under the Legal Practice Division umbrella from 2016-18. He was appointed as the chair of the Courts of the Future Forum's 'the future of the legal profession' discussion. Nasser has spoken at several IBA conferences and been a guest lecturer at over 100 conferences organised by the Business Software Alliance, the WIPO and various other organisations in the Middle East and Europe.

Geraldine Ahern is head of commercial for the Middle East and the senior office partner in Abu Dhabi, who specialises in commercial and employment, including in relation to TMT. She has experience of advising on a range of commercial matters, including commercial structuring arrangements, agency, distribution and franchising and competition law issues, and drafting bespoke, complex and high-value commercial contracts including for a range of leading clients in the TMT sector. Geraldine is a regular contributor to events, including presenting at a major conference in Dubai with two other leading industry experts on cyber and data security issues. She also regularly provides training to clients and their in-house legal teams.

Andrew Garbett is a senior associate with many years' experience advising on the structure and drafting of contracts in the TMT sector, including high-value, strategic IT acquisitions by major clients. He has also advised on the IP aspects of many contentious and non-contentious matters, including acting for a technology manufacturer in a successful claim relating to electronic circuit design and software against one of its former designers and a competitor company, and acting for a US-based international software company in the difficult and long-running negotiation of a trade mark co-existence agreement with a UK-headquartered software company. Andrew has presented at many events and provided training to clients, most recently to a major regional bank on IT contracting issues.

Erica Crosland is a senior associate who is particularly interested in the emerging technology sector and the legal issues related to blockchain, artificial intelligence, algorithmic accountability, data audits, cloud computing, data protection and cryptocurrencies. She also works with organisations and in-house legal teams on digital transformation journeys and is a big supporter of technology for the legal sector. Her practice areas extend to commercial dispute resolution concerning technological, commercial, IP issues and financial disputes. She is a member of the International Association of Privacy Professionals as Certified Information Privacy Professional/Europe and Manager. Erica completed the Oxford FinTech Programme at the Saïd Business School, University of Oxford, in 2018 and is studying towards an MSc in data science, technology and innovation at the University of Edinburgh.

1. Cloud Computing

1.1 Laws and Regulations

The use of cloud computing is steadily increasing across the UAE and organisations of all sizes are moving to the cloud in order to facilitate digital transformation objectives.

At present, there are no comprehensive laws or regulations that govern the use of cloud computing and the legal framework consists of a patchwork of overarching legal requirements in respect of data protection and more stringent sector-specific requirements (where applicable).

1.2 Regulations in Specific Industries

Key sectors that operate under restrictions that could impact a move to the cloud include: the public sector and related private entities that form part of the critical infrastructure of the UAE; the banking sector; and the healthcare sector.

Taking each briefly in turn, the public sector is regulated at both a federal and emirate level. The National Electronic Security Authority (NESA) is a federal authority responsible for the national advancement of cybersecurity. To support this, NESA developed the UAE Information Assurance Standards (the IAS) which includes technical controls and information security requirements for cloud computing environments. All UAE government entities and other entities deemed critical to the national infrastructure are required to implement the IAS and private sector entities are encouraged to do the same. The IAS takes a risk-based approach and public entities are required to establish sound data security requirements for cloud environments, including appropriate due diligence, risk assessments, governance policies, incident response policies and, where possible, audits of security arrangements by cloud service providers.

At an emirate level, Abu Dhabi's Smart Solutions and Services Authority (ADSSSA) is responsible for the governance and use of government data, securing the government's IT systems, communications network and government data technology, as well as providing recommendation of standardised systems and implementation across all Abu Dhabi government entities. The ADSSSA (at the time known as 'ADSIC') Information Security Standards 2009 (as amended) includes specific requirements that any government information classified as 'Restricted' or above must not be hosted outside Abu Dhabi government data centres without approval from ADSSSA.

In Dubai, the comparable oversight function is fulfilled by the Dubai Electronic Security Center (DESC) and DESC has also issued information security rules that apply to emirate level public sector entities. DESC is currently working on a new framework and this will likely include a cloud certification standard. If launched, this should provide a much greater degree of certainty for regulated entities.

As previously mentioned, the banking industry is also subject to sector-specific requirements. These are not contained in a single comprehensive regime but relevant restrictions can be found in regulations dealing with outsourcing and the management of customer financial information. Similarly, the health sector has strict data localisation requirements for patient data.

1.3 Processing of Personal Data

At a more general level, the UAE does not have a comprehensive data protection regime and there are several laws that could be relevant to the use and transfer of personal data, including the general privacy safeguards contained in: the UAE Constitution; the Penal Code; the Civil Code; and the Cybercrime Law. Additionally, certain fee zones have developed their own data protection frameworks (notably the Dubai International Financial Centre, the Abu Dhabi Global Market and the Dubai Healthcare City).

In view of the above, a move to the cloud in the UAE is generally permitted but may require consideration of a number of regulatory regimes depending on the relevant entity's operations within the jurisdiction.

2. Blockchain

2.1 Risk and Liability

The UAE has set ambitious targets to develop blockchain technology for practical use. The Dubai Blockchain Strategy launched in October 2016 and its aim is to become the first city fully powered by blockchain by 2020. To support this, the Dubai Future Foundation launched a global blockchain council (made up of 46 key players in the blockchain industry) to explore and discuss current and future applications of blockchain technology.

The public sector, often in collaboration with Smart Dubai (the technology arm that supervises the implementation of electronic and smart transformation in the Dubai government), has already announced several blockchain-driven initiatives. For example, the Department of Economic Development announced plans to develop a business registry platform using blockchain technology in mid-2018. The platform would be aimed at streamlining the process of establishing and operating a business in Dubai, as well as to ensure regulatory compliance and facilitate direct foreign investment. Similarly, the Dubai Land Department has already deployed blockchain technology in three initiatives (ownership verification, properly sales by developers and smart leasing process).

The judiciary are also taking steps to enable blockchain transformation and the Dubai International Financial Centre (DIFC) Courts have announced plans to develop the world's first Court of the Blockchain. The preliminary work

will explore cross-border enforcement of legal judgments through the blockchain and building dispute resolution mechanisms into the blockchain in order to facilitate commercial use.

Despite the impressive number of blockchain-enabled projects, there are few specific laws or regulations that deal with blockchain or distributed ledger technology as a distinct technology. But this is likely to change soon. Currently, the Abu Dhabi Global Market (the ADGM – a financial free zone in Abu Dhabi) has issued specific regulation but only in the context of cryptocurrencies. The ADGM is an active member of R3, a leading financial innovation and technology firm that focuses on designing and applying distributed ledger technology solutions for the financial services industry and has also launched the first cross-border FinTech sandbox between Abu Dhabi and Singapore. Since 2017, the ADGM has actively published guidance on initial coin offerings and virtual currencies under the Financial Services and Markets Regulation and, in 2018, it published further guidance on the regulation of crypto asset activities in the ADGM.

We are aware that both emirate-specific and federal regulations are in the process of being developed to cover both blockchain (as a general technology) and specific regulations for cryptocurrency and other FinTech applications. For now, the general laws will apply.

Risk and Liability

It is generally advisable for clients to carefully consider whether their business falls within the scope of regulated activities (free zone or federal), especially if the blockchain technology is used for FinTech ventures. There is no specific regulated activity covering blockchain in general so the particular features and use of the technology would have to be considered on a case-by-case basis. Even if the use of the blockchain technology does not fall within any regulated activities (for instance, because it is not yet recognised) it could still raise questions of KYC, AML and, separately, data protection concerns.

The general principles of contractual liability and 'acts causing harm' will apply and companies should, as always, be mindful of the UAE law position in relation to limitation of liability and indemnity provisions.

2.2 Intellectual Property

There are no specific IP provisions dealing with blockchain per se, but the various general IP laws will apply.

2.3 Data Privacy

The UAE does not have a comprehensive data protection regime (with the exception of certain free zones that operate under separate frameworks). As such, general privacy safeguards under the UAE Constitution, Civil Code, Penal Code and Cybercrime Law will apply. In addition, sectorial laws may impact the ability to utilise blockchain technology if data localisation requirements apply to certain categories of data thereby preventing international transfers.

2.4 Service Levels

General laws apply which will be more relevant when dealing with the public sector.

2.5 Jurisdictional Issues

General laws apply. However, the DIFC Courts currently have a taskforce working on jurisdictional issues, so further guidance may be available soon.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Big Data

In October 2017, the government of the UAE launched the 'UAE Strategy for Artificial Intelligence (AI)' with the goal of increasing government performance and promote innovation through investment in AI.

Since then, the government has taken several steps to facilitate the safe testing of new technologies including the announcement in late 2018 that laws are being developed to regulate self-driving cars and AI more generally. In order to keep up with the technological developments, a new RegLab was reportedly set to launch in January 2019 in order to provide a safe testing environment for new technologies and help establish future laws governing their use. In the meantime, the UAE Cabinet has been authorised to grant temporary licences for testing of innovative solutions that utilise future technology such as AI.

Until specific regulations have been developed, companies in the UAE would be well advised to consider and apply 'Smart Dubai's AI Ethics Principles & Guidelines', which sets out best practice when dealing with emerging technologies. It also sets out four broad principles, guidelines and practical examples. The Smart Dubai website also hosts a toolkit that can be used by AI developers or operators to self-evaluate the ethics level of an AI system using Dubai's AI Ethics Guidelines. These are also reflected in the 'Data Policy in the Fourth Industrial Revolution: Insights on personal data' (a paper by the world Economic Forum published in collaboration with the UAE Ministry of Cabinet Affairs and the Future). Another helpful resource may be the recently published European Commission's draft ethics guidelines for trustworthy AI (published December 2018 and set to be finalised in March 2019), which provides an informative assessment list that could be used to complement the Smart Dubai guidelines until mandatory regulation is introduced in the UAE. The above-cited resources are not mandatory but they offer useful guidance on the likely direction of

future regulation and, in the meantime, they offer some protection against civil liability in the event that an action was brought by in an individual, or group of individuals, under the general legal principles of UAE law.

In legal terms, 'big data' remains a rather fuzzy concept but it is commonly accepted that it includes (at least) the following characteristics: considerable volume (referring to the scale and size of data); variety of format (ie, it can be text, image, video, sound); mixed structure (the data can be both unstructured and structured); and velocity (the speed at which new data is generated).

On its own, big data has little intrinsic value and it is the operations performed on it – namely, quantitative analysis – that generates important insights. This can be done using AI, algorithmic computing, machine learning or other methods (discussed below).

When working with big data, it is important that entities consider the extent to which they could be dealing with personal data which is protected under local data privacy laws or categories of data subject to sectorial restrictions (such as banking/transactional data or government data).

3.2 Machine Learning

There is no single definition of machine learning but, in simple terms, it is a process of getting computers to learn from data without relying on explicit programming (ie, it learns over time in an autonomous fashion). This raises a number of interesting legal considerations.

For example, in machine learning the quality of data used to train the algorithm is incredibly important as any biases present in the data will quickly be 'learned' and implemented by the algorithm. It is therefore quite possible to (inadvertently) produce algorithms with biases in respect of ethnicity, gender or religion (all of which are protected under UAE law) simply by virtue of poor quality checks on the 'training data'. Quality checks and proper documentation are therefore essential when dealing with training data sets.

Another legal consideration is the autonomous nature of the learning process. When faced with consumer complaints or lawsuits, a company may be unable to justify how a decision was reached. Proper documentation policies and algorithmic audits may guard against excessive exposure in this regard until formal industry standards have been established.

3.3 Artificial Intelligence

In addition to the above there are numerous legal considerations in relation to AI ranging from liability issues, IP, control and accountability and transparency. Fundamentally, with the exception of AI in the healthcare industry, there are currently no laws, regulations or policies that govern the use of AI in the UAE and any existing compliance or other obligations to clients will remain unaltered and responsibility will lie with the implementing entity.

In the UAE, general AI regulations and regulation in respect of autonomous vehicles have been announced and are expected to be published in the near to medium future.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions Affecting a Projects' Scope

Pursuant to the Telecommunication Regulatory Authority Decision 17 of 2018, an Internet of Things (IoT) Policy was formally approved in the UAE and the Telecommunications Regulatory Authority (TRA) was mandated with the implementation of the policy (the 'Policy').

The purpose of the Policy is to enable the development of IoT services in a safe manner and it is intended to cover all industries (while acknowledging that ministries and regulators for specific industries may develop their own additional IoT specific guidance in co-ordination with the TRA). Therefore, the Policy can be considered as a first step rather than a comprehensive framework.

The Policy covers key requirements for IoT implementation, including the following.

General Requirements for RTTE Devices Providing IoT Services

Any Radio and Telecommunications Terminal Equipment (RTTE) device that provides IoT Services (as defined in the Policy) must meet prevailing Type Approval Regulations (see Telecommunications Apparatus Type Approval Regulation dated 5 April 2007). In addition, the Policy specifies additional requirements specific to IoT Service-enabled devices which include:

- labelling/packaging/documentation requirements in respect of key features and functionalities involved in data collection or sensory inputs;
- the impact of any connectivity issues must be clearly indicated and documented;
- Security by Design must be implemented to guard against unauthorised access;
- consideration of whether the IoT Service is a regulated activity which requires a licence; and
- spectrum requirements for short-range devices under the general Class Authorisation.

Registration Requirements

IoT Service Providers (as defined in the Policy) must register with the TRA in order to obtain an IoT Service Provider Registration Certificate. Any applicants are required to have a local presence or official representative within the UAE.

The process for applying is set out in the IoT regulatory procedures document. There is currently no set procedure for providing IoT connectivity networks and any entity that is considering such services should approach the TRA directly for a case-by-case assessment.

Failure to comply with the Policy (including the registration requirements) may be penalised by the TRA in accordance with the penalties set out in the Telecommunications Law and/or other relevant regulation, including temporary or permanent suspension of the services.

Data Management and Protection
Within the context of IoT services, the TRA has developed specific data management and privacy requirements. These requirements are adopted from the EU General Data Protection Regulation 2016/679 (GDPR), albeit the Policy notes that these references are for guidance only and that UAE law shall prevail in any area of conflict. Furthermore, public authorities will retain the right to process data within the purview of the legislative powers provided to them and appear exempt from the stricter requirements set out in the Policy.

The Policy contains the following principles of data storage:

- purpose limitation;
- data minimisation;
- storage limitation; and
- data classification and localisation requirements.

In addition, the Policy includes requirements to establish technical measures towards enabling inspection of the data by relevant public authorities in the UAE and compliance with interception/monitoring of data by law enforcement agencies. Encryption standards must meet requirements of the UAE authorities and, if higher levels of encryption are to be utilised, approval must be sought from the TRA.

5. Challenges with IT Service Agreements

5.1 Specific Features

Even when they are stated to be subject to local law, contracts for the provision of IT services in the UAE often reflect the standard terms of one of the parties or the terms of corresponding UK or US IT contracts. However, there are several points to be borne in mind in relation to IT contracts in the UAE.

Storage/Hosting of Data Outside the UAE
There is no specific legislation in the UAE for either cloud services or data protection (other than as described below). There are, however, provisions under the Penal Code and Cybercrime Law which protect the privacy of individuals. There are also regulations that apply to specific industries such as the banking sector regarding the hosting of data. In order to minimise the risk of committing a breach of such laws and regulations, before private data of an individual is disclosed (including to a provider of cloud services) or transferred outside the UAE, the consent of that individual should be obtained and it should be confirmed that such data can be hosted outside the UAE. Any privacy policy should reflect such consent.

The DIFC, Dubai Healthcare City and ADGM free zones have data protection regimes which closely follow the pre-GDPR EU model. As such, they include a prohibition on the transfer of data except to jurisdictions which offer equivalent protection.

In some sectors, additional requirements apply. For example, the banking sector in the UAE is regulated by the Central Bank, and customers of such regulated industries may not have their data stored in the cloud without the regulated company obtaining the necessary consents from the applicable authority first.

Intellectual Property
The transfer by an author (including an author of software) of all future copyright works, or more than five such works, is null and void under UAE law. If the parties intend that the customer will own all the rights in the software produced by the supplier under the agreement, the parties will therefore need to draft a clause which is more sophisticated than the relatively simple transfer of all future copyright which may be adequate in a UK IT contract.

Exclusion of Liability
Exclusion and limitation of liability feature prominently in IT contracts. Liability for personal injury, death and for tort cannot be excluded under UAE law. Moreover, liability in contract cannot be excluded if the liability arises from 'harmful acts'. The meaning of this term is not settled but would include gross negligence, wilful default and unlawful acts. In practice, it is possible that an exclusion of liability for faults, inaccuracy of data etc would be unenforceable. A cap on liability may therefore be better from the supplier's point of view than an exclusion. However, UAE courts tend in general to limit compensation to direct losses. If exclusions of indirect and consequential loss are included in a contract it is possible in practice that such losses would not be awarded against a party in breach.

Limitation of Liability
UAE law permits limitation of liability (as opposed to exclusion of liability) in business-to-business contracts. However, the UAE courts reserve the right to adjust any contractual liability cap if the amount agreed in the contract is less than the actual damages suffered by the injured party. The courts may therefore order that any cap is increased to be equal to

the amount of damages suffered. Any such cap is, however, a starting point; if the claimant seeks to increase it he or she must show loss which shows that that is justified.

Indemnities
Indemnities are commonly used in UAE contracts. However, they do not have a fixed meaning and are generally interpreted against the party seeking to rely on them. Accordingly, indemnities should be drafted as clearly as possible. There is still a risk that broad indemnities will not be upheld. An indemnity for a matter which is of a criminal nature or strict liability, or a liability which cannot be excluded, may of course not be enforceable as a matter of public policy in any event.

5.2 Rules and Restrictions
The UAE does not operate under a comprehensive European-style data protection regime and there is no national data protection regulator.

Instead, there are overreaching privacy safeguards set out in various laws (including the UAE Constitution and the UAE Penal Code, among others). These laws provide a basic foundation for data protection that have then been developed further by either sectorial laws or, in some instances, completely separate regimes such as the data protection framework's operated free zones, such as the Dubai International Financial Centre (the DIFC), the Abu Dhabi Global Market (the ADGM) and Dubai Healthcare City (DHCC).

6. Key Data Protection Principles

6.1 Core Rules Regarding Data Protection
In view of the above, companies should give careful consideration to the applicable regime and ensure that they understand the data protection rules that they will be subject to. Common features include a desire to protect the private information of individuals by requiring consent to process or transfer personal data but the scope of data protected, as well as the steps required to achieve compliance, vary across the different laws.

Concepts such as 'data controller' and 'data processor' only exist in some laws and are not universally applicable across the UAE.

Core Rules include:

- General:
  (a) UAE Constitution;
  (b) UAE Penal Code; and
  (c) UAE Cybercrime Law;

- Sectorial laws:
  (a) telecommunication Regulatory Authority Policies (such as the IoT Policy);
  (b) financial sector regulations by the UAE Central Bank, Insurance Authority and the Securities and Commodities Authority (such as the Stored Values and Electronic Payment Regulations);
  (c) public sector regulations (such as the Dubai Electronic Security Centre (DESC) policies, the Abu Dhabi Smart Solutions and Services Authority (ADSSSA) or the National Electronic Security Authority (NESA); and
  (d) healthcare Regulations (such as the Federal Ministry of Health and Prevention (MOHAP) and the emirate-level health authorities);

- Free zone laws:
  (a) the Data Protection Law, DIFC Law No 1 of 2007 (as amended) and the Data Protection Regulation Consolidated Version No 3 of 2018;
  (b) the Dubai Healthcare City Regulation No 7 of 2013; and
  (c) the ADGM Data Protection Regulations 2015 (as amended);

- Expected laws:
  (a) the UAE has already announced plans to publish laws and regulations in relation to emerging technology. This may include specific data protection provisions in the context of big data, machine learning and AI.

6.2 Distinction Between Companies/Individuals
Most data protection obligations only apply in respect of individuals. However, there are certain sectorial laws that apply to classes of data (such as transactional data which can belong to either an individual or a company or to categories of data produced by the public sector). The relevant legal framework should be considered and the specific laws consulted prior to adopting a blanket approach to data processing in respect of individuals or companies.

6.3 General Processing of Data
The general processing of data is not ordinarily subject to legal/regulatory oversight or specific requirements. However, there are several notable exceptions to this and certain sectorial laws apply to classes of data (such as transactional data or to categories of data produced by the public sector). In addition, any statistical data that relates to the emirate of Dubai is also subject to separate regulations.

The relevant legal framework should be considered and the specific laws consulted prior to adopting a blanket approach to data processing in respect of individuals or companies.

6.4 Processing of Personal Data
The general rule is that processing of personal data requires consent. The nature of extent of the consent is subject to different criteria depending on the applicable legal framework.

Furthermore, some laws contain data residency requirement restricting transfers outside the UAE for certain categories of data (which may or may not be personal data); other laws require assurances as to the adequacy of data protection standards if data is to be transferred out of the jurisdiction.

7. Monitoring & Limiting of Employee Use of Computer Resources

7.1 Employees' Restrictions on Computer Use

Company computer resources provided by an employer for the use of their employees remain the property of the employer. The starting point is that the employer can control use (eg by blocking websites and not permitting personal use) and monitor activity on its systems.

Where the employee has not expressly consented to the monitoring of their use of the computer resources, there are mixed views among lawyers regarding the extent of monitoring that can be undertaken by the employer.

For this reason it is sensible to adopt an IT Usage policy which details the rights of the employer to limit and/or withdraw use of the computer resources and to monitor usage including the websites that have been visited and the contents of e-mails sent via the computer e-mail system.

Ideally, an employee would expressly consent to the policy but in the absence of this, so long as the company can demonstrate the employee has been made aware of the policy and received a copy of it, then it should be upheld. If such a policy is in place, it should be carefully drafted since the company must abide by its terms.

If the company does not have such an IT Usage policy, then monitoring and investigation of web traffic and e-mails is subject to compliance with UAE Labour Law and individuals' privacy right under the UAE constitution.

In all cases it is recommended that the following is kept in mind:

- communications that are clearly of a private nature, even if sent or received on a company device, should be considered private. If a company accesses such private communications without justification this may be deemed to be a breach of the employee's privacy;
- if e-mails are of a private nature and are pertinent to an investigation then while the company can disclose these to the authorities any broader disclosure should only be undertaken following legal advice;
- the company is permitted to block access to private e-mail accounts and social media websites etc on company computer resources. However, if employees are permitted to access these sites then they should be considered private and should not be accessed by the company.

When reviewing e-mails and IT equipment in the course of an investigation, employers should additionally bear in mind that:

- the Labour Law sets out a specific procedure to be followed (including timeframes and notice requirements) before a disciplinary penalty can be imposed - failure to comply with such requirements may result in the penalty being deemed illegal;
- the UAE Penal Code imposes an obligation on all individuals to report crimes that they become aware of (failure to report is in itself a criminal offence) - therefore, the company may need to consider disclosure of its investigation to the UAE authorities.

DIFC, ADGM and Dubai Healthcare City Free Zones have their own data protection laws that must also be complied with where applicable and if the company is based in any of these locations separate advice should be obtained.

8. Scope of Telecommunications Regime

8.1 Technologies within Local Telecommunications Rules

A licence is required from the Telecommunications Regulatory Authority (TRA or Authority) to provide a telecommunications network (wired or wireless) and the connectivity services required for related products to be used by end users. The TRA determines the form and substance of each licence granted and may include in such licences any conditions that it requires.

In addition, the technologies that fall within the scope of UAE telecommunications rules require licensing and/or type approval from the TRA. The TRA website provides a summary of those technologies.

The TRA has exclusive competence in issuing all authorisations in relation to Telecommunications Apparatus (apparatus made or adapted for use in transmitting, receiving or conveying any of the Telecommunications Services through a Telecommunications Network) comprised in or intended for use in connection with a Telecommunications Network (a system comprising one or more items of apparatus or means of communication medium for broadcasting, transmission, switching or receiving of Telecommunications Services, by means of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy and any other means of communication medium) or in the provision of a Telecommunications Service (the service of transmitting, broadcasting, switching or receiving by means of a Telecommunications Network of any of the following:

- wired and wireless telecommunications;
- voice, music and other sounds;
- visual images;
- signals used in radio and TV broadcasting;
- signals used to operate or control any machinery or apparatus; and
- the installation, maintenance, adjustment, repair, replacement, moving or removal of apparatus which is or will be connected to a Public Telecommunications Network).

No person is permitted to use, sell, offer for sale or connect to any Telecommunications Network any Telecommunications Apparatus that has not been approved by the Authority. The Authority has enacted specific Type Approval Regulations (Telecommunications Apparatus Type Approval, version 1, dated 5 April 2007), which set out in more detail the process for obtaining Type Approval in the UAE.

Telecoms equipment employing wireless transmission in the frequency range 9 kHz to 3,000 GHz and/or Telecommunications Apparatus directly connected to or intended to be directly connected to a Public Telecommunications Network is required to be registered with the Authority prior to use, sale, offer for sale or connection in the UAE (except for equipment purchased outside the UAE and imported personally for an entity's own use). Only a dealer, importer or manufacturer of such telecoms equipment registered with the TRAis permitted to apply for the registration of such telecoms equipment with the Authority and the registered dealer is required to have a valid trade licence for the equipment concerned.

The registered dealer is responsible for ensuring that Telecommunications Apparatus is suitable for the purpose for which it is supplied and that it operates in accordance with the claims made in relation to it, and for registering the equipment with the TRA unless the equipment has previously been registered. Governmental entities are exempt from obtaining the approval of the TRA in respect of Telecommunications Apparatus used or to be used by governmental entities.

A Frequency Authorisation is required to use radio frequencies in the UAE and all authorised users are required to comply with the Radiocommunications Policy, which is available on the TRA website.

The establishment and use of wireless transmission stations and the installation and use of any wireless transmission is prohibited unless permitted by a radio spectrum authorisation issued by the TRA.

In addition, the TRA has issued ancillary regulations, such as the Consumer Protection Regulations, which provide for a consumer dispute resolution procedure and a resolution dealing with spam e-mails.

In practice, early engagement with the TRA is advisable to understand the specific steps required in relation to the launch of any product or technology in the telecoms sector. It is prudent to assume that every product which falls within the telecoms rules will require some form of prior consent or approval from the TRA.

9. Audiovisual Services and Video channels

9.1 Main Requirements

Despite the fact that the UAE Cabinet issued Resolution No (23) of 2017 Concerning Media Content (the '2017 Regulations'), which came into force at the end of August 2017 and provides that the vast array of digital media offered by OTT providers in the UAE (such as e-books, music streaming services, and on-demand film and TV) are now within scope of national content laws and subject to censorship and pre-approval by the National Media Council (NMC), the current applicable legislations do not address the issue of enforcement against offshore OTT/media providers who deliver digital content to UAE-based customers via the Internet (ie Netflix).

There might be some discussions to regulate the services delivered by offshore OTT platforms in the UAE in the future; however, at this stage OTT platforms are not fully regulated in the UAE, so the main requirements for providing audiovisual services for OTT platforms are not applicable.

Audiovisual Regulations

Traditional media content and digital media content, including television shows and film, are regulated in the UAE by the following:

- the Electronic Media Regulations, released by the NMC in 2018 under the umbrella of the 2017 Regulations, are intended to apply to 'all electronic Media activities' apply to all media activities carried out in the UAE, both onshore and free zone-based entities, including but not limited to advertisement and promotion, publishing, new sites and sites selling or otherwise dealing in print, video and audio materials. They include a list of four activity types which the NMC considers to be 'Electronic Media Activities' and in respect of which an Electronic Media Licence will be needed to be obtained. This is in addition to the licence to be obtained by the relevant companies registrar.

The four types are:

- websites for trading, offering and selling of audiovisual and print material;
- on-demand electronic publishing and printing;

- specialised websites (e-advertising, new sites etc); and
- any electronic activity that the NMC may determine to add.

It also addresses personal websites, blogs and social media platforms and exempts school and government websites.

The 2017 Regulations

- the national media council's resolution no 20 of 2010 on the criteria for media content ('nmc content guidelines'), which applies to all media, audiovisual and print institutions in the uae, require all media companies to comply with specific criteria including respect for the principles of islamic beliefs and the cultural heritage of the uae;
- federal law no 15 for 1980 concerning publications and publishing ('Publications Law'), which regulates publishing activities in the UAE, covers all forms of content, whether published digitally or via traditional media, and is arguably broad enough to cover art and films.

9.2 Online Video Channels

Issues To Be Considered under the Electronic Media Regulations

- application Requirements (an application must be filled by the applicant and submitted to the nmc along with the supporting documents and necessary payments);
- appointment of a responsible manager (every website that is subject to an electronic media licence must appoint an responsible manager/administrator to oversee such website's content);
- electronic media activities via social media accounts (according to the electronic media regulations each website owner is responsible for the content published from such account).

Objectives of Regulating the Electronic Media Activities

The media regulation that is organised in accordance with the provisions of the Electronic Media Regulations is aimed at the following:

- support the electronic and digital media industry and regulate the activities of the same as an effective industry that could contribute to supporting the publishing industry;
- keep au courant of the rapid development in the electronic media spheres to enrich digital content;
- Reinforce the respect of the religious, cultural and social values prevailing in the country and respect the freedom of opinion and expression and constructive interaction in the field of the electronic media;
- provide a balanced, responsible and impartial media content that could respect the individual privacy and protect the various community members against any possible negative effects.

NMC Feedback

According to information received following a recent meeting held by Eversheds Sutherland UAE and the NMC management, the Electronic Media Regulations will not be imposed on companies based outside the UAE irrespective of whether such companies are targeting the UAE market-audience or not (namely, OTT platforms). Having said that the authorities in the UAE have full discretion to block any websites or accounts they deem illegal.

10. Encryption Requirements

10.1 Legal Requirements Governing the Use of Encryption

Unless explicitly authorised by the TRA, it is not permitted to use encryption techniques for the purpose of obscuring the meaning in relation to content of radio communications or the transmission, emission or reception of electromagnetic energy by Radio Frequency spectrum. ('Radio Frequency' means radiated electromagnetic energy measured in Hz or cycles/sec).

As a result, a Frequency Spectrum Authorisation granted by the TRA does not accord any privacy rights to end users (except in relation to diplomatic official correspondence as defined in Article 27 of the Vienna Convention on Diplomatic Relations (1961)). A supplier of wireless or telecoms products which use Radio Frequency therefore needs to ensure that, if any elements of the products include encryption, there is an explicit authorisation from the TRA for the use of that encryption. If there is no such authorisation, the products should not contain any form of encryption. Encryption may be of particular concern to the authorities if, for example, relevant information or data is hosted outside the UAE. It is unclear whether the TRA would in practice pursue a manufacturer or supplier which merely provides such products to an importer or service provider in the UAE if there were a contravention of this requirement, but this could be possible under the broad language used in the Radiocommunication Policy.

Eversheds Sutherland (International) LLP
Dubai
Unit 803, 8th Floor,
Building 6, Emaar Square,
Burj Khalifa, P.O. Box 74980
Dubai
UAE

EVERSHEDS SUTHERLAND

Tel: +971 0 4389 7000
Fax: +971 0 4389 7001
Email: nasseralikhasawneh@eversheds-sutherland.com
Web: www.eversheds-sutherland.com