DATA PROTECTION LAWS OF THE WORLD

UAE - General

UAE - GENERAL

Last modified 21 January 2021

LAW

Note: Please also see UAE – Dubai (DIFC), UAE – ADGM, UAE – DHCC.

Generally

The United Arab Emirates ("**UAE**") does not have a comprehensive data protection law at its federal level, however there are a number laws in place that govern privacy law in the UAE, as well as laws that also relate to data security. There are also sector specific data protection provisions in certain laws. The UAE also has a number of special economic or sector free zones, three of which have specific data protection laws (please see the links above). These are the Dubai International Financial Centre, the Abu Dhabi Global Market and the Dubai Health Care City.

The most relevant privacy law of general application in the UAE is Article 379 of the UAE Penal Code. This law prohibits a person who, by reason of their profession, craft, situation or art, is entrusted with a "secret," from using or disclosing that "secret," without the consent of the person to whom the secret pertains, or otherwise in accordance with the law.

A breach of this provision is punishable by criminal penalty of imprisonment of a minimum of one year, or a fine of a minimum of Twenty Thousand Dirhams, or both.

The term "secret" is undefined, however it is generally broadly construed to cover the concepts of personal data, as defined in many data protection laws (for example, name, date of birth, sex, religion etc.).

The terms "use" or "disclose" are also undefined, however the terms are again generally broadly construed to cover the concepts of "processing" and "transfer" respectively. Transfer can be to a third party or to another entity within the UAE or overseas.

Article 379 of the UAE Penal Code allows for the use or disclosure with the consent of the person to whom the secret pertains. Therefore, to mitigate against the risk of a breach of Article 379 of the Penal Code it is generally advised to obtain such consent prior to the use or disclosure of personal data. This can be done in a number of ways, depending upon the specific context of how the data is collected and used, for example by signature against a paper consent form, or by electronic signature or tick box against an electronic consent form.

In addition, there are several UAE federal level laws that contain various provisions in relation to privacy and the protection of personal data:

- Constitution of the UAE (Federal Law 1 of 1971)
- Penal Code (Federal Law 3 of 1987 as amended)
- Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control) (as amended by Federal Law

No. 12 of 2016 and Federal Decree Law No. 2 of 2018), and

- Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended), which includes several implementing regulations/policies enacted by the Telecoms Regulatory Authority ('TRA') in respect of data protection of telecoms consumers in the UAE.

Stored Value Facilities Regulation

On 30 September 2020 the UAE Central Bank issued a new Stored Value Facilities Regulation ("**SVF Regulation**"), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems it has issued in September 2016. While the SVF Regulation makes amendments to the licensing and enforcement regime for SVF (on onshore UAE only; it does not apply in, or affect, the DIFC and ADGM free zones), from a data protection perspective little has changed. The SVF Regulation applies to those providing Stored Value Facilities, which is now defined as *"a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the "Relevant Undertaking". SVF includes Device-based Stored Value Facility and Non-device based Stored Value Facility".*

Article 10 of the SVF Regulation requires that licensees providing SVF services ("**SVFLicensee**") must have in place adequate policies, measures and procedures to protect its information and accounting systems, databases, books and accounts, and other records and documents from unauthorized access, unauthorized retrieval, tampering and misuse.

An SVF Licensee must also adequately protect customer data (including customer identification and transaction records) which are required to be stored and maintained in the UAE. Such data can only be made available to the corresponding customer, the Central Bank, other regulatory authorities following prior approval of the Central Bank, or by a UAE court order. An SVF Licensee must store and retain all customer and transaction data for a period of five years from the date of the creation of the customer data, or longer if required by other laws.

Article 8 of the SVF Regulation requires that outsourcing arrangements must also contain adequate data protection and data handling controls.

ICT Health Law

On 6 February 2018 Federal Law No. 2 of 2018 on the Use of the Information and Communication Technology ("**ICT**") in Health Fields ("**ICT Health Law**") was issued. The primary purpose of the ICT Health Law is to establish a central electronic system of medical records for use within the health industry within the UAE.

Article 13 of the UAE ICT Health Law states that the Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health.

The UAE ICT Health Law applies to all Competent Entities.

"Competent Entity" is defined as *"any entity in the State providing medical services, health insurance or national health insurance services, brokerage services, claims management services or electronic services in the medical field of any entity related, whether directly or indirectly, to the implementation of the provisions hereof."*

"Health Information" is defined as *"the health information that were processed and were given a visual, audible or readable indication, and that may be attributed to the health sector, whether related to the health or insurance facilities or entities or to the health services beneficiaries."*

At the date of writing this, there has been no decision issued under article 13 of the ICT Health Law by any UAE Health Authorities in coordination with the Ministry. We have been verbally informed by staff at the Ministry that patient consent for the transfer of data out of the UAE should be sufficient. However, this is not binding legal advice.

On 22 April 2020 the Federal Cabinet issued Cabinet Resolution No. 32 of 2020 concerning the Regulations Concerning the Use

of the Information and Communications Technology in the Areas of Health ("**ICT Health Law Regulations**"). The regulations provide further details, including on permission controls to access and use the central system, and on the storage and exchange of information on the central system.

Dubai Data Law

In December 2015 the Dubai Government published the Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("**Dubai Data Law**"). The purpose of the Dubai Data Law to collate and manage data that relates to the emirate of Dubai and, where appropriate, to publish it as "Open Data" or at least ensure that it is shared it between authorised persons. This law is considered unique as it is the only one in the world we are aware of that provides a government with the power to require designated private sector entities to provide to a government with information held by the company in relation to a city, for the purposes of making that information Open Data.

DEFINITIONS

The concept of 'Personal Data', as understood in the EU, is not reflected under UAE federal law as yet. The corresponding concept within UAE law encompasses notions such as 'secrets', 'photographs', 'the privacy of the individual or family life' and 'private life or family life secrets of individuals'. As such, while no UAE federal law explicitly states that the collection of personal data requires express consent, if any such data pertains to private or family life then, in certain circumstances, the consent of the individual(s) concerned may be required. References to the term 'Personal Data' below refers to the UAE understanding of the concept as described in the paragraph above.

Central Bank regulations, including the SVF Regulations but also more generally AML and CFT rules, require, for example, that when licensees take on customers that they conduct customer due diligence to identify customers, including verifying the customer's identify, or that when opening an account they obtain documentation to include the full name of the account holder, the current address and place of work as well as copies of the account holders passport.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in the UAE. In respect of telecommunications services, the TRA is responsible for overseeing the relevant telecoms laws and policies.

The UAE Central Bank is responsible for the SVF Regulation.

The Ministry of Health and Prevention is responsible for the ICT Health Law.

The Telecommunications Regulatory Authority is responsible for the regulation of its Consumer Protection Regulation.

REGISTRATION

There are no data protection registration requirements in the UAE.

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organizations to appoint a data protection officer.

COLLECTION & PROCESSING

If the collection and processing of any personal data pertains to an individual's private or family life then the consent of the individual may be required in certain circumstances. A failure to obtain such consent would constitute a breach of the Penal Code (Article 378 and 379) and could also be a breach of the:

- Cyber Crime Law if the personal data is obtained or processed through the internet or electronic devices in general (Articles 21 and 22); and
- Telecoms Law to the extent that data is obtained through any means of telecommunication, including through a

telecommunications service provider, or any other electronic means. In addition, the facility should be made available for such consent to be withdrawn at a later stage (TRA Consumer Protection Regulations v1.5, Article 20.5).

The Cyber Crime Law criminalises obtaining, possessing, modifying, destroying or disclosing (without authorisation) electronic documents or electronic information relating to medical records (Article 7). Additionally, unlawful access via the internet or electronic devices of financial information (eg Credit Cards and Bank Accounts) without permission is an offence under Articles 12 and 13.

TRANSFER

Subject to the sector specific restrictions or requirements referred to below, generally, pursuant to the Penal Code (Article 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer, or otherwise where allowed by law.

However, the requirement to obtain written consent may be waived, pursuant to the Penal Code (Article 377), where the personal data pertains to a crime to which the data subject is answerable and it is disclosed in good faith to the relevant authorities.

Article 10 of the SVF Regulation requires that customer data (including customer identification and transaction records) are required to be stored and maintained in the UAE.

Article 13 of the ICT Health Law requires that Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health. We have been verbally informed that until such decisions are issued that individuals' consent to such transfers should be sufficient.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the telecommunications services ordered by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber's information (TRA Consumer Protection Regulations v1.5, Article 20.8).

SECURITY

There are no specific provisions under UAE Federal Law relating to the type of measures to be taken or level of security to have in place against the unauthorised disclosure of personal data, however UAE's Federal Cabinet has issued Resolution No. 21 of 2013, concerning the Regulation of Information Security in Federal Authorities. The requirements of this resolution might be passed on to contractors providing services to Federal government bodies when they are entering into service supply agreements with such bodies.

Article 20.1 of the TRA Consumer Protection Regulations v1.5 requires telecommunications service providers to *"take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information"*. Article 20.3 further stipulates that telecommunications service providers must take *"all reasonable measures to protect the privacy of Subscriber Information that it maintains in its files, whether electronic or paper for"*, and that *"reliable security measures"* should be employed.

The UAE Cyber Crime Law focuses on offences related to accessing data without permission and/or illegally (Articles 2 and 3), including financial information (eg credit card information or bank account information) (Articles 12 and 13).

Based on the above, best practice from a UAE law perspective would be to take appropriate technical security measures against unauthorised or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security adequate enough to minimise the risk of liability arising out of a claim for breach of privacy made by a data subject.

BREACH NOTIFICATION

In principle, there is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data, liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

In relation to telecommunication services, the Telecoms Law and most policies do not include an explicit requirement on service providers to take the initiative in notifying the TRA of a breach or alleged breach, unless a subscriber complains to a service provider about the unauthorised disclosure of his or her personal data. Such a notification would be included in the monthly reporting which is submitted to the TRA (Article 22.10.2 of the TRA Consumer Protection Regulations v1.5).

Subscribers are also able to complain directly to the TRA about the unauthorised disclosure of their personal data. However, the TRA will generally only handle subscriber complaints after the complaint has been submitted to the service provider and if the matter has not been satisfactorily resolved by the service provider's own customer complaints procedure (Article 20.11.1 of the TRA Consumer Protection Regulations v1.5).

ENFORCEMENT

There are four possible methods of enforcement from a UAE law perspective:

1. Where the unauthorized disclosure of personal data results in a breach of the Penal Code

The Public Prosecutor in the Emirate where:

- the party suspected of the breach ('Offender') resides; or
- the disclosure occurred,

will have jurisdiction over a data subject's complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The data subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to the Penal Code (Article 379), if the Courts find a suspect guilty of disclosing secrets that were entrusted to him *"by reason of his profession, craft, situation or art"* the penalties to be imposed under the Penal Code may include a fine of at least UAE Dirhams 20,000 (the fine is determined by the Courts) and/or an imprisonment for at least one year. More generally, pursuant to the Penal Code (Article 378), *"a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals"* private or family life by committing any of the acts described under Article 378 "*other than the legally permitted cases or without the victim's consent".*

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the data subject to the Civil Courts of First Instance for further consideration. The data subject would need to prove the losses her or she has suffered as a direct result of the disclosure of his/her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorized disclosure of personal data results in a breach of the Cyber Crime Law

The police in each Emirate have developed specialized cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, the cybercrime unit in the Emirate where:

- the Offender resides; or
- where the disclosure occurred,

will have jurisdiction over a data subject's complaint.

The cybercrime unit would investigate the case and decide whether or not to refer it to the Public Prosecutor in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect. The same procedure identified above is then followed before the Courts.

If found guilty of an offense under the Cyber Crime Law, the punishment an Offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and / or a fine between AED 150,000 and AED 1,000,000 (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). If found guilty of an attempt to commit any of the relevant offenses under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

3. Where the unauthorized disclosure of personal data results in a breach of the Telecoms Law and Policies

The TRA is responsible for overseeing the enforcement of the Telecoms Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either:

- the breach has occurred; or
- where the suspect resides.

Where a licensed telecommunications service provider has breached the law, the subscriber/data subject generally needs to complain first to the service provider about the breach, though a direct approach to the TRA may be accepted by the them at their discretion (Article 15.11.1 of the TRA Consumer Protection Regulations v1.5).

The subscriber's complaint needs to be submitted to the TRA within three months of the date when the service provider last took action. This three months requirement may be waived subject to the discretion of the TRA (Article 15.11.1 of the TRA Consumer Protection Regulations v1.5).

After examining the complaint the TRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 15.11.5 of the TRA Consumer Protection Regulations v1.5).

4. Where the unauthorised disclosure or transfer of personal data results in a breach of the SVF Regulation

The Central Bank will issue administrative penalties against SVF Licensees. Currently the SVF Regulation does not specify the administrative penalties.

ELECTRONIC MARKETING

There are no general laws in the UAE law covering electronic marketing, however the TRA has issued a regulation governing telecommunications licensees' electronic communications with subscribers, as well as how they should monitor spam passing through their networks. Articles 21 and 22 of the Cyber Crime Law and Article 20.5 of the TRA's Consumer Protection Regulation v1.5, as described in the 'Collection and Processing' section above, are also worded widely enough to potentially apply to electronic marketing. Article 22 of the Cyber Crime Law, for example, prohibits the use of various electronic devices in order to disclose, without permission, confidential information that has been obtained through the course of a person's duties.

The TRA's Unsolicited Electronic Communications Regulation states that telecommunications licensees are under a general obligation to put all practical measures in place to minimise the transmission of Spam having a UAE Link across their Telecommunications Networks, and where they are aware of Spam having a UAE Link sent to or from a particular Electronic Address, they must take all practical means to end the transmission of that Spam and to prevent the future transmission of such Spam. Spam is defined as Marketing Electronic Communications sent to a Recipient without obtaining the Recipient's Consent. Although the Unsolicited Electronic Communications Regulation is targeted and enforced against telecommunications licensees, it effectively puts an obligation upon the licensees to minimise and prevent Spam from being transmitted through their networks.

ONLINE PRIVACY

Although the UAE Penal Code does not contain provisions directly relating to the internet, its provisions related to privacy are broadly drafted and therefore could apply to online matters (such as Article 378 as described above).

Additionally, as described in the 'Collection and Processing' section above, under certain circumstances, online privacy is protected through Articles 21 and 22 of the Cyber Crime Law and the TRA's Consumer Protection Regulation. Unlawful access via the internet, by electronic devices, of financial information (eg Credit Cards and Bank Accounts) without permission is also an offence under the Cyber Crime Law (Articles 12 and 13).

KEY CONTACTS

Eamon Holley
Partner
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.