

DATA PROTECTION LAWS OF THE WORLD

UAE - General



Downloaded: 11 July 2017

UAE - GENERAL



Last modified 26 January 2017

LAW

Note: Please also see [UAE – Dubai \(DIFC\)](#).

On 1 January 2017 the UAE's Central Bank published the Regulatory Framework for Stored Values and Electronic Payment Systems ("**Digital Payment Regulation**"). This regulation governs digital payment service providers ("**PSPs**") in the UAE, providing services such as cash-in services, cash out services, retail credit and debit digital payment transactions, government credit and debit digital payment transactions, peer-to-peer digital payment transactions and money remittances. PSPs are required to store all User identification data and transaction records. This data can only be made available to the corresponding User, the Central Bank, to other regulatory authorities following prior approval of the Central Bank, or by UAE court order. PSPs must not process or share the personal data provided by Users, unless necessary as per anti-money laundering ("**AML**") and combatting of financing terrorism ("**CFT**") laws. PSPs must store and retain all User and transaction data exclusively within the borders of the UAE, excluding UAE financial Free Zones (the DIFC and ADGM), for a period of five (5) years from the date the original transaction. No User or transaction data can be stored outside of the UAE. Details of Users' personal information must be stored for a minimum of five (5) years from the date the User relationship is terminated.

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.

In addition, there are several UAE Federal 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), 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.

DEFINITIONS

The concept of 'Personal Data', as understood in the EU, is not reflected under UAE Federal Law. 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.

The term 'Personal Data' as used below refers to the UAE understanding of the concept as described above.

The Digital Payment Regulation does not define User identification data, however other Central Bank regulations, such as AML and CFT rules, require, for example, that when banks open 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 Digital Payment Regulation.

REGISTRATION

There are no data protection registration requirements in the UAE.

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organisations 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 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, Article 12.5).

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

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.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the services requested by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the 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, Article 13.8).

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.

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. Instead, the 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).

Article 13.1 of the TRA Consumer Protection Regulations requires telecommunications service providers to 'take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information'. Article 13.3 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 form', and that 'reliable security measures' should be employed.

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 15.10.2 of the TRA Consumer Protection Regulations).

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 15.11.1 of the TRA Consumer Protection Regulations and Article 1.1 to 1.3 of the TRA Consumer Dispute Procedure).

ENFORCEMENT

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

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

The Public Prosecutor in either the Emirate:

- where the party suspected of the breach ('Offender') resides
- where 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 he/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 unauthorised disclosure of personal data results in a breach of the Cyber Crime Law:

The police in each Emirate have developed specialised 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 offence 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 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 offences under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

3. Where the unauthorised 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 them at their discretion (Article 14.11.1 of the TRA Consumer Protection Regulations).

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 14.11.1 of the TRA Consumer Protection Regulations).

After examining the complaint the TRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 14.11.5 of the TRA Consumer Protection Regulations).

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

The Central Bank will issue administrative penalties against PSPs. Currently the Digital Payment 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 13.5 of the TRA's Consumer Protection Regulation, 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



Paul Allen

Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com



Eamon Holley

Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com



Jamie Ryder

Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com



Robert Flaws

Senior Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.