General Data Protection Rules

Type	Gulf Legal Advisor
Document type	Practice Note
Date	7 Jul 2021
Jurisdiction	United Arab Emirates
Copyright	LexisNexis

Table of contents

Overview

- The United Arab Emirates does not have a comprehensive Federal data protection law specifically designed to regulate the collection, processing, transfer and/or use of personal data, nor does the UAE have a dedicated data protection supervisory authority.
- Personal information relating to an individual is protected under laws of general application with relevant provisions not specifically focused on modern principles of data protection but which are relevant to the collection and processing of data (including personal data) in the UAE. The key legal provisions can be found in the following UAE laws /regulations: Federal Law No. 3/1987 (Penal Code) and Federal Decree-Law No. 5/2012 (Cybercrimes Law).
- There are some sector-specific laws (including health, insurance, patient confidentiality, and credit worthiness areas that contain specific data protection and privacy related provisions such as:
    1. the Federal Law No. 2/2019 (ICT Health Law) and its implementing regulations Cabinet Decision No. 32/2020 (ICT Health Regulations), that regulate the uses of information and communications technology in the areas of health in the UAE, and
    2. the Central Bank of the UAE issued Consumer Protection Regulations (Circular No. 8/2020), which apply to all Licensed Financial Institutions (LFIs) regulated by the Central Bank. Additionally, the Credit Information Law (Federal Law No. 6/2010), Insurance Authority Board of Directors' Decision No. 18/2020 Concerning the Electronic Insurance Regulations, the Medical Liability Law (Federal Law No. 10/2008) and the Telecommunications Law (Federal Decree-Law No. 3/2003), are examples of laws that also have data protection or personal privacy implications.
- Certain financial and healthcare freezones, being the Dubai International Financial Centre (DIFC), the Abu Dhabi Global Markets (ADGM) and Dubai Healthcare City (DHCC) have enacted specific data protection laws and regulations that are generally heavily modelled on their European counterparts and influenced by international standards and practices.
- UAE-based companies offering goods or services to European Union (EU) consumers, and/or monitoring the behaviour within the EU, also need to determine whether they need to comply with the EU 2016/679 General Data Protection Regulation[1 p.10] (GDPR).

Definitions

- *Data Subject:* A natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
- *GDPR*: General Data Protection Regulation (EU 2016/679).
- *IoT*: Internet of Things
- *Personal Data*: Any information relating to an identified or identifiable Data Subject.
- *Processing*: Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, altering, retrieving, consulting, using, disclosing, disseminating, aligning or combining, restricting, erasing or destroying.
- *TDRA*: The UAE Telecommunications and Digital Government Regulatory Authority.

Practical Guidance

Data protection authorities

There is no single federal authority responsible for the regulation of data protection in the UAE.

Certain sectors have specific authorities that are responsible for overseeing matters related to data protection, including:

- the Central Bank of the UAE in respect of issued Consumer Protection Regulations (Circular No. 8/2020);
- the Insurance Authority Board of Directors' Decision No. 18/2020 Concerning the Electronic Insurance Regulations;
- the TDRA under:
    - Federal Decree-Law No. 3/2003 regarding the Organization of the Telecommunications Sector, as amended;
    - Information Assurance Regulations (the IAR)[2 p.10];
    - Internet of things (IoT) Regulatory Policy and Procedures[3 p.10];
    - Consumer Protection Regulations Version 1[4 p.10];
- Signals Intelligence Agency (SIA) under Federal Decree-Law No. 3/2012;

- Dubai Electronic Security Center (DESC) Dubai Law No. 11/2014.
- The Ministry of Health and Prevention under:
    - Federal Law No. 5/2019 (Concerning the Practice of Human Medicine Profession);
    - The Ministry of Health (MOH) Code of Conduct 1988 governing medical practitioners, pharmacists and other healthcare professionals licensed in the UAE; and
    - Federal Decree-Law No. 4/2016 on Medical Liability.
- The Dubai Healthcare City (DHCC), Department of Health (DOH), and Dubai Health Authority (DHA) have further standards regarding confidential health information applicable to healthcare establishments and professionals in their respective jurisdiction.
- The DIFC Commissioner of Data Protection under DIFC Data Protection Law (DIFC Law No. 5/2020).
- The ADGM office of data protection under the ADGM Data Protection Regulations.

Registration

- There are currently no data protection registration requirements for organisations in the UAE outside of the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Markets (ADGM).
- Data Protection Registration requirements for the Dubai International Financial Centre (DIFC): The information to be set out within the notification is available on the DIFC's public register https://portal.difc.ae/clientportal/s/login/
- Data Protection Registration requirements for the Abu Dhabi Global Markets (ADGM): The information to be set out within the notification is available on the ADGM's public register https://access.adgm.com/accessadgmlogin

Under the TDRA's Internet of Things Regulatory Policy ("IoT Policy") and Internet of Things Regulatory Procedures (together the "IoT Framework"), all providers of IoT services must register with the TRA to obtain an IoT service registration certificate prior to providing any IoT services.

Rights of individuals

Under the TDRA's Consumer Protection Regulations Version 1.4 Issued: 20 March (TDRA CPR), customers have the right to request the Licensee i.e. a telco provider to disclose his or her own Subscriber Information to that Subscriber, the Licensee shall disclose it free of charge and without delay after an adequate verification process. Service Provider shall disclose to the customer their own information free of charge and without delay only after an adequate verification process.

The TDRA CPR further states that there is a consumer right to privacy of information. Additionally, the private consumer information collected by the service provider should only be used for the purposes related to the provision of the service for which the information was provided.

Additionally, the Central Bank of the UAE (CB) has issued the Consumer Protection Regulations (Circular No. 8/2020) (CB Regulations), which apply to all Licensed Financial Institutions (LFIs) regulated by the CB whilst carrying out licensed financial activities. Specifically, the Regulations introduce requirements for LFIs relating to the protection of a client's personal data, which reflect those in the GDPR and other privacy legislations around the world.

LFIs must have the consumer's express consent before using and sharing a consumer's personal data for direct marketing or prior to transferring it to any authorized agent. Prior to obtaining consent, the LFI must proactively disclose to the consumer in writing its intent to use and or share personal data, and with who such personal data will be shared.

The Regulations require active, express consent. Moreover, consent must be freely given, explicit to a request for the use/and or sharing of personal data and must be withdrawable. The consumer shall have the right to withdraw expressed consent for either of the following:

- The processing of personal data by the LFI except were personal data is required for business operations.
- Personal data sharing with any other third parties for purposes such as sales or marketing.

Note that consent, is separate from, and does not replace the additional requirement for collecting data for a lawful basis directly related to the licensed financial activities of LFI. Overall, the requirements for what constitutes valid consent are almost identical to those in the GDPR. Additionally, the Regulations impose a minimum retention period of 5 years for consent/ a copy of the expressed consent.

Data security requirements

- Under the IoT Framework, providers of IoT services (including network provider platforms and machine-to-machine connectivity providers) are required to use such data encryption standards that fulfil the requirements established by the competent UAE authorities.
- The ICT Health Law (Federal Law No. 2/2019) and its implementing regulations ICT Health Regulations (Cabinet Decision No. 32/2020) mandates that all health service providers that use information communication technologies on personal health data ensure that such information will be kept confidential and will not be shared without

authorisation. In terms of security, the ICT Health Law requires that the 'validity and credibility' of health personal data be ensured by keeping it safe from 'non-authorised damage, amendment, alteration, deletion or addition.' In keeping with international data protection standards and best practices, ICT Health Law requires entities to introduce technical, operational and organisational procedures to ensure the integrity and security of personal health data.

- The TDRA CPR requires telecommunications service providers to 'take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information'. The TDRA CPR 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.
- The CB Regulations (Circular No. 8/2020) specifically requires LFIs amongst other requirements to have a proper data management control framework with policies', procedures, system controls and checks and balances to protect consumer data. LFIs must ensure that they are able to identify and resolve information security incidents as soon as they occur. LFIs must report regularly monitor their data management systems e.g. such as through penetration testing and must report any apparent vulnerabilities in the security and online systems to the Central Bank on a quarterly basis.
- The Dubai Electronic Security Center (DESC) issued the Dubai Government Information Security Regulation (ISR). The ISR directly applies to Dubai government entities only. Sub-Control 13.2.1.1 prevents a Dubai Government entity permitting the handling and storing of classified data with a Cloud Service Provider (CSP), outside the legal jurisdiction or geographical boundaries of the United Arab Emirates, including for CSP's backup or disaster recovery purposes.

Data transfers and data localisation

Under the ICT Health Law (Federal Law No. 2/2019), personal health data related to health services provided in the UAE may not be transferred to, stored, processed, generated or transformed in a jurisdiction outside the UAE unless the relevant health authority, in coordination with the Ministry for Health and Prevention, has issued a resolution authorising same.

MOHAP Ministerial Decision No. 51/2021 has been issued for this purpose and sets out 10 exceptions where transfer of health data is permitted.

Under the TDRA CPR, the service provider must obtain the subscriber's prior consent before sharing any his/her information with its affiliates and/or other third parties not directly involved in the provision of the telecommunications services, ordered by the consumer.

Under the IoT Framework, IoT service providers are required to:

- classify data collected based on the anticipated harm that could result should such information be disclosed without consent; and
- based on how the data is classified, comply with the data localisation requirements prescribed for each category of data.

The categories of data are:

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

Based on the above, the data localisation requirements are:

- "open data" may be stored either in the UAE or abroad;
- "confidential", "sensitive" or "secret" should primarily be stored in the UAE (unless certain adequacy requirements are satisfied) where it relates to individuals and businesses; and
- "confidential", "sensitive" or "secret" must be stored in the UAE without exception where it relates to the UAE government.

The UAE Central Bank Regulatory Framework for Stored Value Facilities 2020 requires those offering digital payment services in the UAE to physically store user and transaction data exclusively in the UAE for five years from the date the user relationship ends or the transaction date.

Similarly, the Central Bank's (CB) Consumer Protection Regulations (Circular No. 8/2020), which apply to all Licensed Financial Institutions (LFI) impose a strict data localisation requirement. As such, LFIs must store transactional and consumer data "within the UAE, as prescribed by" the CB.

Data breach notifications

As there is no Federal data protection law in the UAE, there is also no mandatory requirement to notify data security breaches.

The Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Markets (ADGM) both have data breach notifications regimes.

Under the Telecoms Law (Federal Decree-Law No. 3/2003) and the TDRA CPR, there is no explicit requirement on service providers to notify data breaches to the TDRA unless a subscriber has complained to the service provider about an unauthorised disclosure of their personal data. Notwithstanding however, service providers need only include such notification in its monthly report that is submitted to the TDRA. Subscribers may also complaint directly to the TDRA about unauthorised disclosures of their personal data however, the TDRA will generally only deal with such complaints if the service provider has already been notified by the subscriber and its customer complaints procedure has not satisfactorily resolved the matter.

Enforcement and sanctions

The Penal Code (Federal Law No. 3/1987) provides that anyone found guilty of disclosing secrets (which may include personal data) that were entrusted to them "by reason of his profession, craft, situation or art" may be subject to a fine of at least AED 20,000 and/or imprisonment for at least one year. In addition, anyone who attacks the sanctity of an individual's private or family life will be subject to a penalty of imprisonment and a fine.

Under the Telecoms Law (Federal Decree-Law No. 3/2003), anyone who:

- illegally copies, discloses, or distributes the content of a telephone call or message relayed through a public telecommunications network; or
- eavesdrops on telephone conversations without prior authorisation from the relevant judicial authorities will be subject to a penalty of imprisonment for not less than one year and/or a fine between AED 50,000 to 200,000.

Cybercrime is severely punished under the Cybercrimes Law (Federal Law No. 5 of 2012) and penalties are imposed for invasion of privacy, disclosure of confidential information, electronic piracy, email theft and other unlawful activities. Offences include:

- obtaining, acquiring, amending, damaging or disclosing information related to medical examinations, diagnoses, treatment or medical care or records through an information network without permission (carrying a penalty of imprisonment);
- accessing the numbers, statements, credit or electronic card, statements of bank accounts or any means of electronic payment through an information network without permission (carrying a penalty of imprisonment between six months and one year and/or a fine between AED 100,000 to 1 million);
- intentionally and without permission capturing or intercepting any communication (including emails) through any information network and disclosing it (carrying a penalty of imprisonment for not less than one year and/or a fine between AED 150,000 to 500,000);
- using an information network or other technology to invade a person's privacy (carrying a penalty of imprisonment for not less than six months and/or a fine between AED 150,000 to 500,000); and
- without permission, using an information network or other technology expose confidential information obtained during one's profession (carrying a penalty of imprisonment not less than six months and/or a fine between AED 500,000 to 1 million).

The ICT Health Law (Federal Law No. 2/2019) contains a regime of sanctions for non-compliance including disciplinary actions and monetary fines which may be imposed by a disciplinary committed within each health authority. These sanctions may be imposed, for example, for violating the data localisation rules. Specifically, sanctions include:

- the potential suspension or withdrawal of the licence to use the central IT system;
- a formal notice or warning from the relevant health authority; and/or
- fines ranging from AED 1,000 to 1 million.

The IoT Framework refers to the Telecoms Law (Federal Decree-Law No. 3/2003) for the range of penalties that may be imposed by the TDRA 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 one year; and/or
- fines ranging between AED 50,000 to 200,000.

GDPR

Companies in the UAE that process the Personal Data of Data Subjects within the territorial scope of the EU and target goods or services to EU Data Subjects, or that process Personal Data in the context of the activities of an European establishment, may be caught by the GDPR. Subject to certain exceptions, businesses outside the EU within the scope of the GDPR must appoint an EU representative, located in one of the European countries of the data subjects who are offered products or subject to behavioural monitoring. The representative acts on behalf of the non-EU company and may be addressed by any EU data protection supervisory authorities and data subjects.

Conclusion

Media reports indicate that a draft data protection focused law modelled largely on the GDPR has been circulated internally amongst certain UAE government departments by the Ministry of Transport and Communications as part of the UAE National Cybersecurity Strategy 2020-2025. Reports also suggest that more than one federal data protection law may be published in the future, from both the financial services regulator (for all banks and financial services organisations) and the TDRA (for all other public and private organisations). However, this has not been confirmed.

From a practical compliance perspective, for those UAE entities that are caught by the GDPR, any compliance steps currently being taken will supplement existing measures adopted as a matter of good practice or to comply with local regimes.

Related Content

Legislation

- Federal Law No. 3/1987 Concerning the Penal Code
- Federal Decree-Law No. 5/2012 on Combating Cybercrimes
- Federal Decree-Law No. 3/2003 on Organising the Telecommunications Sector
- Federal Law No. 2/2019 Concerning the Use of Information and Communication Technology

Regulations

- ADGM Data Protection Regulations
- EU General Data Protection Regulation[5 p.10]
- UAE Central Bank 2017 Regulatory Framework for Stored Values and Electronic Payment Systems[6 p.10]
- TRA Consumer Protection Regulations, Version 1.3, issued 10 January 2017[7 p.10]
- UAE Central Bank Consumer Protection Regulations Circular No. 8/2020
- Insurance Authority Board of Directors' Decision No. 18/2020 Concerning the Electronic Insurance Regulations;
- Information Assurance Regulations (the IAR)[2 p.10];
- Internet of things (IoT) Regulatory Policy and Procedures[3 p.10];
- Consumer Protection Regulations Version 1[4 p.10];

Authors

Martin Hayward
Head of Technology, Media & Telecommunications, Al Tamimi & Company (Dubai, UAE)
+971 04 364 1641
m.hayward@tamimi.com

Education

- Legal Practice Certificate, College of Law, London, UK
- Graduate Diploma in Law, College of Law, London, UK
- MA (Japanese History and Language) School of Oriental and African Studies (SOAS), University of London, London, UK
- MA (History), Peterhouse, Cambridge University, Cambridge, UK

Memberships

Admitted as Solicitor in England & Wales

Biography

Martin has over 12 years' experience advising on the full range of commercial, outsourcing, telecommunications, technology, intellectual property and information law issues.

After qualifying into the Information, Communications & Technology team at Simmons & Simmons LLP in 2006, Martin spent several years working in their London office before relocating to Dubai in 2009. In 2012, Martin joined an Abu Dhabi government owned IT services provider as General Counsel and Company Secretary, and most recently held the position of Senior Corporate Counsel EMEA and Middle East Regional Counsel at a major US telecommunications solution provider.

Martin has spent extensive periods of time on secondment at a major UK telecoms company, in the supply management function of an international investment bank in the UK, and at one of the largest UAE telecommunications services provider.

Noriswadi Ismail
Managing Director, Global Data Privacy & Governance, Breakwater (London, UK)
noriswadi.ismail@breakwatersolutions.com

Areas of expertise

Global Data Privacy; Governance & Technology Implementation

Education

- Oxford Advanced Management & Leadership Programme Candidate, Saïd Business School, University of Oxford, UK
- Certified Oxford Scenarios Planning Practitioner, Saïd Business School, University of Oxford, UK
- LLM, Information Technology & Telecommunications Law, University of Strathclyde, UK
- Certified Information Privacy Professional (CIPP)/Asia
- LLB (Hons), International Islamic University Malaysia

Memberships

International Association of Privacy Professionals

Biography

Global Data Privacy & Data Governance Consulting Practice Leader at Breakwater Solutions, based in London. Former EMEA & APAC Data Privacy Consulting Leader of Ankura, former GDPR Lead of Ernst & Young (EY) U.K & Ireland LLP and interim Data Protection Officer of EY UK & Ireland LLP. Experienced in Financial Services, Automotive, Defense, Healthcare, Technology, Media & Telecommunications, Energy & Asset, Products & Services, (Consumer Products), Retail, Public Sector (Regulatory), Food and Beverages, Hospitality, Life Sciences and Oil & Gas -ranging from Start up, mid-sized, mid-markets to Fortune 500, FTSE 100 and FTSE 250. Experienced in comparative regulatory leadership and enforcement in the U.K, E.U (Bulgaria, France, Germany, Ireland, The Netherlands, Greece and Malta); Africa (Mauritius); China, India, ASEAN (Malaysia, Indonesia, Singapore and the Philippines); APAC & Oceania (Australia, Japan and New Zealand). Experienced in implementing data privacy and information security programmes including, requirements definition, data flow analysis, risk assessments and strategy development relating to policies and procedures, business process controls, incident response plans, monitoring, reporting, coaching, training and awareness programmes. Association of Overseas Technical Scholar, Japan (2005); British Chevening Scholar (2006/2007); Fulbright Professional Exchange Fellow (2014/2015); and Oxford Alumni Business Network. Author of 2 books in Data Protection. Currently writing 3rd book (forthcoming publication in 2022).