ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

United Arab Emirates

Rima Mrad

Nadim Bardawil

BSA Ahmad Bin Hezeem & Associates LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The laws in the United Arab Emirates can be divided into mainland/onshore UAE laws and free-zone specific laws. The mainland of the UAE does not have any principal data protection legislation existing in its own right. Data privacy and protection is addressed across a number of separate regulations, not specifically focused on data protection.

Certain free-zones have their own respective data protection legislation which only applies within the confines of said free-zone, such as the Dubai International Financial Center ("**DIFC**"), the Abu Dhabi Global Market ("**ADGM**"), the Dubai Healthcare City ("**DHCC**") and the mainland of the United Arab Emirates ("**UAE**").

The principal data protection regulations in the DIFC are:

- DIFC Law Number 1 of 2007 (as amended by DIFC Law Number 5 of 2012).
- DIFC Data Protection Regulations (consolidated version number 2 of 2012) ("**DIFC Regulations**").

The principal data protection regulations in the ADGM are:

- The Data Protection (Amendment) Regulations 2018 ("**ADGM 2018 Data Protection Regulations**").
- The Data Protection Regulations of 2015 ("**ADGM 2015 Data Protection Regulations**" or "**ADGM Regulations**") (enacted under Article 6(1) of Law Number 4 of 2013 concerning the Abu Dhabi Global Market) which are consistent with the Organisation for Economic Co-operation and Development's guidelines and the European Union's Directives on the protection of privacy and personal data.

The principal data protection legislation in the DHCC is the Health Data Protection Regulation Number 7 of 2013. It contains several detailed provisions relating to the protection of patient data and patient health information, including information about the patient's health, medical history, disabilities, and donations of body parts and bodily substances.

The only legislation in the UAE that directly addresses Data Protection is the Dubai Law Number 26 of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai ("**the Dubai Data Dissemination Law**"). However, the Dubai Data Dissemination Law only applies to Federal Government Entities that have any data relating to Dubai, to local government entities, and to persons who produce or spread any data relating to Dubai.

1.2 Is there any other general legislation that impacts data protection?

The following pieces of legislation impact data protection matters in the UAE:

- Article 378 of Federal Law Number 3 of 1987 (the "**Penal Code**"), as amended by Federal Law Number 34 of 2005, provides that the violation of private or familial life by recording or transmitting private conversations and by capturing or transmitting the picture of a person in a private place is punishable by a fine and imprisonment. Article 379 of the Penal Code further provides that any individual who, by reason of his profession or situation, is entrusted with a secret and who discloses it in unauthorised cases, or uses it for his own advantage, is punishable by a fine and by imprisonment.
- Article 31 of the UAE constitution of 1971 (the "**UAE Constitution**") provides for a general right to privacy with respect to correspondence and other means of communication: "Freedom of corresponding through the post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law". However, this only applies to UAE nationals.

1.3 Is there any sector-specific legislation that impacts data protection?

The following pieces of sector-specific legislation impact data protection matters in the UAE:

- Federal Law Number 5 of 2012 on Combatting Cybercrimes (the "**Cybercrime Law**"). Article 2 of the Cybercrime Law prohibits the disclosure, publication and re-publishing of any information that was obtained by unauthorised access to websites or electronic information systems or networks. Article 21 prohibits the use of a computer network, an electronic information system or any information technology means for the invasion of privacy. Further, Article 22 states that any person who uses, without permission, any information network, electronic site or information technology tool to expose confidential information shall be punished by imprisonment and a fine.
- Federal Law by Decree Number 3 of 2003 regarding the Organisation of the Telecommunications Sector (the "**Telecommunications Law**"). The Telecommunications Law provides protection to all data obtained through any means of communication. In addition, the 2014 Customer Protection Regulations address to what extent the UAE's two telecommunication companies can share the personal details of their customers.
- Telecommunications Regulatory Authority Consumer Protection Regulations Version 1.3 protect data and

information relating to telecommunications subscribers, including their name, address, bank account details, credit card details, and message and call recordings.

- Dubai Law Number 23 of 2006 (the "**Dubai Statistics Law**") prevents the disclosure of any data collected for statistics.
- Federal Law Number 15 of 1980 regarding Printed Matters and Publications provides that publishing news and comments connected with a person's private life is prohibited.
- UAE Cabinet Resolution No. 21 of 2013 addressing data security for Federal Authorities (the "**Data Security Resolution**") specifically outlines how data belonging to the UAE federal government, authorities, ministries and other official entities must be stored, treated and disseminated.

In the healthcare settings, privacy and data protection matters are governed by the regulations listed below. Emirate-specific regulatory bodies have begun drafting more comprehensive medical data legislation.

- Health Authority of Abu Dhabi ("**HAAD**") Data Standards and Procedures, of January 2008, as revised by the April 2014 version. The HAAD Data Standards and Procedures outlines the policies and procedures which must be followed when handling Confidential Health Information ("**CHI**") focusing on four areas: the necessary and authorised access to CHI; the unauthorised access to CHI; the storage of CHI; and the transmission of CHI. It further provides regulations relating to health insurance fraud. The HAAD has created a Data Standards Panel whose role is to "review and recommend to HAAD changes and additions to electronic data exchange standards, such as transactions, codes and business rules".
- Dubai Health Authority ("**DHA**") Home Healthcare Regulations, issued in 2012, outline the procedures healthcare facilities must follow with respect to healthcare records and their management. Similarly, the Health Record Guidelines outline the essential requirements which healthcare facilities must implement with regards to the management of health records including record keeping, retention of health records and destruction of health records. The DHA also created the Health Data and Information Analysis Department whose role is to improve the manner and method in which health data is handled and exchanged, as well as to "focus on transparency and confidentiality" between patients and healthcare providers.
- Federal Law Number 7 of 1975 concerning the Practice of the Human Medicine Profession (the "**Human Medicine Profession Law**"). Article 13 of the Human Medicine Profession Law states that a doctor has no right to divulge a private secret concerning a patient and relating to his profession. Certain exceptions apply to this, namely if divulging the secret is held to serve the interests of the individual or to prevent a crime from occurring.
- The Ministry of Health Code of Conduct 1988 (the "**Code of Conduct**") states that pharmacists are required to uphold the confidentiality of any information acquired in the course of professional practice relating to patients and their families. In this case, confidential information and data extends beyond the customer's medical details and includes their address, telephone, and any family or financial data contained in the medical record and hospital registration details.
- Other guidelines on the ethical principles to respect in relation to confidentiality and privacy are covered by "the Good Clinical Practice Principles" and "the Basic Principle for all Medical Research".

1.4 What authority(ies) are responsible for data protection?

There is no single authority responsible for the regulation of data protection in the United Arab Emirates. The following sector-specific authorities are responsible for matters related to data protection in the United Arab Emirates:

- National Electronic Security Authority (pursuant to the Cybercrime Law).
- Telecommunications Regulatory Authority (pursuant to the Telecommunications Law).
- The Dubai Statistics Centre (pursuant to the Dubai Statistics Law).
- The Dubai Health Authority and the Health Authority of Abu Dhabi.

In the DIFC, the Office of the Data Protection Commissioner is responsible for the regulation of data protection.

In the ADGM, the Office of Data Protection is responsible for regulating data protection matters.

In the DHCC, the Centre for Healthcare Planning and Quality is responsible for the regulation of data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  The DIFC Law Number 1 of 2007 defines "Personal Data" as any data referring to an identifiable natural person, which in turn is defined as a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their biological, physical, biometric, physiological, mental, economic, cultural or social identity.

  The ADGM 2018 Data Protection Regulations define "Personal Data" as any information relating to an identified natural person or identifiable natural person. "Identifiable natural person" is defined as a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their biological, physical, biometric, physiological, mental, economic, cultural or social identity.

- **"Processing"**

  In the DIFC Law Number 1 of 2007, "Processing" is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

  The ADGM 2018 Data Protection Regulations define "Processing" as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and "Processed", "Processes" and "Process" shall be construed accordingly.

- **"Controller"**

  In the DIFC Law Number 1 of 2007 and the ADGM 2018 Data Protection Regulations, "Data Controller" is defined as any person in the DIFC or the ADGM, respectively, who alone or jointly with others determines the purposes and means of the processing of personal data. A data controller is equivalent to a data protection officer.

- **"Processor"**

  In the DIFC Law Number 1 of 2007 and the ADGM 2018

Data Protection Regulations, a "Data Processor" is any person who processes personal data on behalf of a data controller.

- **"Data Subject"**

  In the DIFC Law Number 1 of 2007, "Data Subject" is defined as any individual to whom personal data relates. The ADGM 2018 Data Protection Regulations define "Data Subject" as the natural person to whom personal data relate.

- **"Sensitive Personal Data"**

  In the DIFC Law Number 1 of 2007, "Sensitive Personal Data" is defined as personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life. The ADGM 2018 Data Protection Regulations provides the same definition of "Sensitive Personal Data" although it does include communal origin in the definition.

- **"Data Breach"**

  None of the applicable laws provide a definition of "Data Breach".

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  - **"Data"**

    In the DIFC Law Number 1 of 2007 and the ADGM 2018 Data Protection Regulations, "Data" is defined as any information which:

    (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

    (b) is recorded with the intention that it should be processed by means of such equipment; or

    (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

    In the Dubai Data Dissemination Law, "Data" is defined as a collection of organised or unorganised information, facts, concepts, instructions, observations, or measurements, in the form of numbers, alphabets, symbols, images, or any other form, that are collected, produced or processed by data providers. "Data" also includes information.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The UAE's data protection laws only apply to businesses established in the mainland of the UAE and to businesses established in free-zones which are not governed by any specific data protection laws. Free-zones that have issued their own data protection legislation, such as the DIFC and the ADGM, are not governed by the laws of the United Arab Emirates that relate to data protection.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Although there is no explicit reference to having a right to transparency in the mainland of the UAE, an individual's right to a private life may mean that they have a right to transparency, or a right to know how their personal data is being used.

  In the DIFC and the ADGM, the rights to access to and rectification, erasure or blocking of personal data and the rights to object to processing provided by Articles Article 17-18 of the DIFC Law Number 1 of 2007 and Articles 10-11 of the ADGM 2015 Data Protection Regulations give individuals located in these jurisdictions a right to transparency.

- **Lawful basis for processing**

  In the mainland of the UAE, the DIFC and the ADGM, there must be a lawful basis for processing data. The DIFC and the ADGM have set out similar circumstances in which sensitive personal data can be processed. Article 10(1) of the DIFC Law Number 1 of 2007 and Article 3 of the ADGM 2015 Data Protection Regulations both state that sensitive personal data shall only be processed in the following circumstances: (a) if the data subject has given his written consent to the processing of the sensitive personal data; (b) if the processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller; (c) if the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; (d) if the processing is carried out in the course of its legitimate activities with appropriate guarantees by any non-profit seeking body, provided that the personal data is not disclosed to a third party without the consent of the data subject; (e) if the processing relates to personal data which are manifestly made public by the data subject or which is necessary for the establishment, exercise or defence of legal claims; (f) if the processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject; (g) if the processing is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets; (h) if the processing is necessary to comply with any regulatory requirements; and (i) if the processing is required for medical reasons.

  In the DIFC, sensitive personal data can also be processed in the following circumstances: (j) if the processing is required for protecting members of the public against: (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by persons concerned in the provision of certain business activities; and (ii) dishonesty, malpractice or other seriously improper conduct by persons concerned in the provision of certain business activities.

  If a business wishes to process data in any circumstances other than those mentioned above in the DIFC and the ADGM, Article 10(2)(a) of the DIFC Law Number 1 of 2007 and Article 3(2) of the ADGM 2015 Data Protection Regulations state that they should obtain a permit to process this sensitive personal data.

- **Purpose limitation**

  Please see "Data minimisation" below.

- **Data minimisation**

  In the mainland of the UAE, an individual's right to privacy is protected. If, however, this individual consents to their personal information being used for a specific purpose, the information should not be used for a purpose that goes beyond the purpose agreed on.

  In the DIFC and the ADGM, given that an individual's consent must be obtained to be able to process their personal data, the data collected and processed should not be used for any purpose beyond the purpose agreed on.

  In all jurisdictions, information should be used in a manner proportionate to what it was initially collected for.

- **Proportionality**

  Please see "Data minimisation" above.

- **Retention**

  In the mainland of the UAE, there are no specifications as to how long personal data can be retained.

  In the DIFC and the ADGM, Article 8 of the DIFC Law Number 1 of 2007 and Article 1 of the ADGM 2015 Data Protection Regulations provide that personal data should not be kept for longer than is necessary for the purposes for which the personal data was collected or for which they are further processed.

  In the ADGM, Article 51 of the ADGM Employment Regulations on processing personal data by the employer also provides that personal data must not be kept for longer than is necessary by the employer (having regard to the purpose or purposes for which they are being processed).

- *Other key principles – please specify*

  There are no other key principles to be aware of.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  There is no such right for individuals in the mainland of the UAE.

  Article 17 of the DIFC Law Number 1 of 2007 and Article 10 of the ADGM 2015 Data Protection Regulations each respectively give data subjects in the DIFC, and in the ADGM, the right to access and to rectify, erase or block personal data. This must be done at reasonable intervals and without excessive delay or expense. This includes the right to delete information.

- **Right to rectification of errors**

  Please see "Right of access to data/copies of data" above.

- **Right to deletion/right to be forgotten**

  Please see "Right of access to data/copies of data" above.

- **Right to object to processing**

  In the mainland of the UAE, an individual's privacy is protected by the UAE Constitution, the UAE Penal Code and the UAE Cybercrime Law. This gives individuals an implied right to object to the processing of their personal data, to restrict its processing, and to object to its marketing.

  Article 18 of the DIFC Law Number 1 of 2007 and Article 11 of the ADGM 2015 Data Protection Regulations each give data subjects in the DIFC, and in the ADGM, the right to object to processing on reasonable grounds at any time. Given that the objection can be done at any time, this implies that data subjects in the DIFC and the ADGM also have a right to restrict processing and to withdraw consent. A data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses. Data subjects have the right to object to marketing in the DIFC and the ADGM.

- **Right to restrict processing**

  Please see "Right to object to processing" above.

- **Right to data portability**

  No explicit references are made to the right to data portability under UAE, DIFC and ADGM regulations.

- **Right to withdraw consent**

  Please see "Right to object to processing" above.

- **Right to object to marketing**

  Please see "Right to object to processing" above.

- **Right to complain to the relevant data protection authority(ies)**

  In the mainland of the UAE, an individual's privacy is protected by the UAE Constitution, the UAE Penal Code and the UAE Cybercrime Law. This gives individuals an implied right to complain to the relevant authority.

  In the DIFC, according to Article 7(1)(1) of the DIFC Data Protection Regulations, a person has a right to complain. A person may file a claim with the commissioner of data protection by lodging a written notice that provides the following information:

  (a) full name and address of the person making the claim;

  (b) the data controller whom the person believes has contravened the law;

  (c) a detailed statement of facts which the person believes gives rise to contravention of the law; and

  (d) the relief sought by the person making the claim.

  In the ADGM, under Article 18 of the ADGM 2015 Data Protection Regulations, a person has a right to complain to the Registrar in respect of the processing of their personal data.

- *Other key rights – please specify*

  There are no other key rights to be aware of.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In the United Arab Emirates, there are no legal obligations on businesses to register with or notify any authority that manages data protection matters in respect of data processing activities. Data can be processed as long as data relating to an individual was obtained with their consent or if it is required by law. Further, there is no specific data protection authority in the United Arab Emirates. The lone exception here relates to data belonging to the UAE government. The Data Security Resolution outlines that consent must be provided before any data owned by the UAE government can be stored, transferred or shared.

The DIFC has seen the implementation of a more regulated system of data protection. Companies operating in the DIFC must appoint a data controller. Article 19 of the DIFC Law Number 1 of 2007 and Article 6 of the DIFC Data Protection regulations state that the data controller of a business which is processing personal data must file a notification with the commissioner of data protection. The data controller should establish and maintain records of any personal data processing operations. It should be noted that even where a data controller does not process personal data, it must still submit a notification reflecting this.

Similarly, companies operating in the ADGM must appoint a data controller. Article 12 of the ADGM Data Protection Regulations of 2015 provides that to be entitled to operate as a data controller, an individual must first be registered as a data controller with the ADGM Registrar.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

In the DIFC, according to clause 6(3)(2) of the DIFC Data Protection Regulations, when a data controller gives a notification to the commissioner of data protection, it must be specific. The notification must contain the following information:

(a) a general description of the personal data Processing being carried out;

(b) an explanation of the purpose for the personal data processing;

(c) the data subjects or class of data subjects whose personal data is being processed;

(d) a description of the class of personal data being processed; and

(e) a statement of the jurisdictions to which personal data will be transferred by the data controller, along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection in accordance with the terms of the DIFC Law Number 1 of 2007.

Details of the person responsible for data protection compliance must also be provided.

The ADGM Data Protection Regulations do not set any specific requirements for the registration of a data controller with the Registrar. Article 12 of the ADGM 2015 Data Protection Regulations states that a data controller must notify the Registrar of its intention to become a data controller in the required form. They should also establish and maintain records of any personal data processing operations or any set of such operations.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

According to Article 19(2) of the DIFC Law Number 1 of 2007, in the DIFC, notifications are made based on data categories. Clause 6(3)(1) of the DIFC Data Protection Regulations provides that a data controller must notify the commissioner of data protection in the following circumstances:

(a) for any personal data processing operation or set of operations involving the processing of sensitive personal data; and

(b) for any personal data processing operation or set of operations involving the transfer of personal data to a recipient outside of the DIFC which is not subject to laws and regulations which ensure an adequate level of protection.

Further, if the manner of processing is changed, the data controller must submit a notification to the commissioner of data protection informing them of this.

Even where a data controller does not process personal data, it must still submit a notification reflecting this.

In the ADGM, notifications are also made based on data categories.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

In the mainland of the UAE, there is no requirement to register with or notify any data protection authority as there is no such data protection authority.

Entities operating in the DIFC and the ADGM must register with the relevant data protection authority in the DIFC and the ADGM, respectively.

According to Article 19 of the DIFC Law Number 1 of 2007, in the DIFC, the appointed data controller is responsible for filing the notification with the relevant data protection authority.

According to Article 12 of the ADGM 2015 Data Protection Regulations, the data controller must register themselves with the relevant data protection authority.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

For the information that must be included in a notification, please see question 6.2.

6.6 What are the sanctions for failure to register/notify where required?

As stated previously, there is no requirement to register/notify in the mainland of the UAE.

In the DIFC, failure to register with the Office of the Commissioner of Data Protection will result in a fine of $25,000.

The ADGM regulations do not set out any sanctions for failure to register, although they should be levied in this event.

6.7 What is the fee per registration/notification (if applicable)?

According to the DIFC Data Protection Regulations, the fee for the notification is $1,000 for entities regulated by the Dubai Financial Services Authority (the regulating authority of the Dubai International Financial Center), $500 for Dubai Financial Services Authority non-regulated entities except for retail, and $200 for retail entities. A notification filed by a data controller who does not process any personal data does not require a fee.

According to ADGM 2015 Data Protection Regulations, the fee for the application for the initial registration as a data controller is $300.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

In the DIFC, the notification validity period is one year. Failure to renew the notification constitutes a breach of the DIFC Law Number 1 of 2007.

In the ADGM, according to Article 12(4) of the ADGM 2015 Data Protection Regulations (as amended by the 2018 Regulations) registration notifications must be submitted to the Registrar on annual basis where the personal data processing is to continue in the subsequent year.

6.9 Is any prior approval required from the data protection regulator?

In the DIFC, there is no prior approval required from the data protection regulator. In the ADGM, approval to work as a data controller will be granted after the registration notification has been submitted.

6.10 Can the registration/notification be completed online?

In the DIFC, the notification must be completed online; it is available on the Client Portal. In the ADGM, the registration can also be completed online.

6.11 Is there a publicly available list of completed registrations/notifications?

Both in the DIFC and the ADGM, there is no publicly available list of completed notifications.

6.12 How long does a typical registration/notification process take?

No specific period of time is provided as to how long a typical notification process takes in the DIFC and ADGM regulations.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a data protection officer is optional in the mainland of the United Arab Emirates. In contrast, in the DIFC and the ADGM, the appointment of a Data Protection Officer is mandatory. Certain requirements are imposed on data controllers in these free-zones. As per Article 8 of the DIFC Law Number 1 of 2007 and Article 1 of the ADGM 2015 Data Protection Regulations, data controllers should ensure that the personal data which they process is processed securely, and for specified and legitimate purposes.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the DIFC and the ADGM, failure to appoint a Data Protection Officer will result in a fine.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

The DIFC and ADGM data protection regulations do not provide any such protection to the data protection officer.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The DIFC and ADGM regulations do not provide any guidance on whether a single data protection officer can cover multiple entities.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DIFC and ADGM regulations do not set out any specific qualifications that data controllers are required to have.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Article 8(1) of the DIFC Law Number 1 of 2007 and Article 1 of ADGM 2015 Data Protection Regulations require data controllers to ensure that the personal data which they process be:

(a) processed fairly, lawfully and securely;

(b) processed for specified, explicit and legitimate purposes in accordance with the data subject's rights and that it is not processed in a way incompatible with those purposes or rights;

(c) adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;

(d) accurate and, where necessary, kept up to date; and

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected or for which they are further processed.

Moreover, in the DIFC, according to Article 8(2) of the DIFC Law Number 1 of 2007, every reasonable step must be taken by the data controller to ensure that personal data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified. According to Article 16(1) of the DIFC Law Number 1 of 2007, the data controller should also implement appropriate technical and organisational measures to protect personal data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure of access and against all other unlawful forms of processing.

In this vein, Article 9 of the ADGM 2015 Data Protection Regulations provides that the data controller must implement appropriate technical and organisational measures to protect Personal Data in the ADGM.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

In the DIFC, the appointment of a data protection officer must be registered. The commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller, and a general description of their processing of personal data.

According to Article 12 of the ADGM 2015 Data Protection Regulations, the appointment of a data protection officer must be registered with the ADGM Registrar.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

In the DIFC, the data controller must be named in a public register maintained by the commissioner. Individuals can consult the public register to find out details of the processing of personal data being carried out by a specific data controller.

Similarly, in the ADGM, data controllers are listed in the data controller register. The data controller register is incorporated within the ADGM Public Register of Companies.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Although it is not explicitly set out in the DIFC and ADGM regulations, it is advisable for a business wishing to appoint a processor to process personal data on its behalf to enter into a service agreement with that processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is advisable to have a signed and stamped agreement written on letterhead, that addresses the data controller's responsibilities with respect to the procedure for processing personal data, keeping this data secure, only processing it in accordance with instructions and in accordance with the provisions of a specific law.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

In 2009, the Telecommunications Regulation Authority issued its 'Regulation on Unsolicited Electronic Communication' addressing electronic direct marketing, including spam emails, spam text messages and telephone calls. The Regulation on Unsolicited Electronic Communication confirms that mobile phone marketing providers must obtain consent from customers before they send them marketing messages, before they email them or even before they call them. The issue is that people will have generally unknowingly consented to their information being used for marketing purposes. In support of this, Article 72 of the UAE Telecommunications Law penalises copying or disclosing the content of any sort of communication without having the right to do so.

It is worth noting that Article 31 of the UAE Constitution states that an individual has the right to enjoy freedom of communication by post, telegraph or other means of communication and the secrecy thereof is to be guaranteed in accordance with the law.

The UAE Cybercrime Law sets out harsh penalties for using an individual's personal information without their consent or that is otherwise unauthorised by law. Article 21 of the UAE Cybercrime Law states that whoever uses a computer network, an electronic information system or any information technology means for the invasion of privacy of another person shall be sanctioned.

Further, Article 17.22 of the Consumer Protection Regulations, issued on 10 January 2017, provides that advertising (which is defined to include electronic direct marketing) must not be unduly intrusive or coercive and shall not harass or be likely to harass customers. If the marketing method in question is judged to be unduly intrusive or harassing, restrictions will be imposed on this marketing method.

In the DIFC and the ADGM, personal data may only be processed in certain conditions, according to Article 9 of the DIFC Law Number 1 of 2007 and article 2 of the ADGM 2015 Data Protection Regulations. The principal condition is obtaining the data subject's written consent for the processing. Restrictions will be imposed on electronic direct marketing conducted without the individual's consent.

In addition, according to Article 13 of the DIFC Law Number 1 of 2007 and Article 7 of the ADGM 2015 Data Protection Regulations, where information about a data subject has been obtained, the data subject will need to be informed of whether their information will be used for direct marketing purposes, in so far as such information is necessary to guarantee fair processing in respect of the data subject.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.)

Please see question 11.1.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions noted above are aimed at protecting an individual's right to consent to their personal information being used. Although the laws and regulations referred to above will protect this right for an individual living in the UAE, the UAE Government does not have the authority to impose any sanctions on marketing sent from other jurisdictions.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Telecommunications Regulation Authority (mainland UAE jurisdiction), the Office of the Data Protection Commissioner (DIFC jurisdiction) and the Office of Data Protection (ADGM jurisdiction) are active in the enforcement of breaches of marketing restrictions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

To be able to purchase marketing lists from third parties, the information of the business/individual on the list must have been obtained with their consent and the individual must have also consented to their information being used by a third party.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 21 of the UAE Cybercrime Law states that whoever uses a computer network, an electronic information system or any information technology means for the invasion of privacy of another person shall be punished by imprisonment of a period of at least six months, and a fine not in excess of five hundred thousand dirhams, or either of these two penalties.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In the mainland jurisdiction of the UAE, there are no specific legislative restrictions relating to the use of cookies. Despite this, the UAE Cybercrime Law can be construed to apply to cookies. Given that Article 21 of the UAE Cybercrime Law prohibits the use of a computer network for the invasion of privacy, the storage of information by a cookie can be held as an invasion of privacy, and therefore a breach of the Cybercrime Law.

Although the DIFC and ADGM regulations do not set out any legislative restrictions directly concerned with cookies, they do set out restrictions with regards to the processing of personal data – which is stored by cookies. Cookies that store personal data can therefore be indirectly restricted by the DIFC Regulations.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The applicable restrictions do not make a distinction between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The relevant data protection authorities in the mainland of the UAE, in the DIFC and in the ADGM have not taken any enforcement actions in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

In the mainland jurisdiction of the UAE, the maximum penalty for the breach of restrictions relevant to cookies (the breach of Article 21 of the UAE Cybercrime Law) is imprisonment of a period of at least six months and a fine not in excess of five hundred thousand dirhams, or either of these two penalties.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

In the mainland of the UAE, there are no restrictions on the transfer of personal data to other jurisdictions. Notwithstanding this, Article 378 of the Penal Code provides that data subjects should provide their consent to the transfer of data relating to them both inside and outside the UAE.

In the DIFC and the ADGM, according to Article 11 of the DIFC Law Number 1 of 2007 and Article 4 of the ADGM 2015 Data Protection Regulations, a transfer of personal data to a recipient located in a jurisdiction outside the DIFC and the ADGM may take place only if an adequate level of protection for that personal data is ensured by regulations that are applicable to the recipient (if the jurisdiction is listed as an acceptable jurisdiction under the regulations). Transfers of personal data to a recipient which is not subject to regulations and which ensure an adequate level of protection may take place if certain conditions are met, according to Article 12 of the DIFC Law Number 1 of 2007 and Article 5 of the ADGM 2015 Data Protection Regulations. For instance, among other conditions, the following requirements must be met:

(a) the data controller has obtained a permit from the commissioner of data protection;

(b) the data subject has given his written consent to the proposed transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken in response to the data subject's request; and

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

In the mainland of the UAE, the data subject's written consent must be obtained.

In the DIFC and the ADGM, companies will typically utilise the performance of a contract with the data subject and the performance of a contract in the interest of the data subject, among other conditions, to transfer personal data abroad.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No prior approval is required in the mainland of the UAE.

In the DIFC and the ADGM, approval is required, respectively, from the DIFC Commissioner of Data Protection and from the ADGM Registrar to be able to transfer personal data to a recipient located outside the jurisdiction; this is given to the data controller in the form of a permit.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

In Dubai, Article 19 of Dubai Law Number 4 of 2016 on Financial Crimes provides protection to whistle-blowers, or people who report crimes related to financial matters – in this case to the Dubai Centre for Economic Security. The law does not set out any specification on whistle-blowing in these circumstances. In contrast, with regards to non-financial crimes in Emirates other than Dubai, Article 379 of the Penal Code states that it is an offence for an individual to disclose secrets which they have been entrusted with as a result of their employment.

The DIFC regulations do not provide any guidance on the permitted scope of corporate whistle-blowing, although Article 10(1)(h) of the DIFC Law Number 1 of 2007 allows the processing of personal data if it is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering, or counter-terrorist financing obligations or the prevention or detection of any crime that apply to a data controller.

Similarly, the ADGM Regulations do not provide any guidance on the permitted scope of corporate whistle-blowing, although Article 3(1)(h) of the ADGM 2015 Data Protection Regulations allows the processing of personal data if it is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering, or counter-terrorist financing obligations or the prevention or detection of any crime that applies to a data controller.

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?

Anonymous reporting is not prohibited in the United Arab Emirates. On the contrary, it is encouraged. In 2011, the police launched a service called 'Najeed' which allows the public to report crimes to the police in a fully confidential manner.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In the mainland of the UAE, there is no separate registration requirement for the use of CCTV (Closed Circuit Television). In accordance with Article 378 and 379 of the UAE Penal Code and the UAE Cybercrimes Law, given that a person's right to privacy is protected, this right to privacy will need to be taken into account when installing CCTV. Article 378 of the UAE Penal Code stipulates that 'a person shall be punished by detention and a fine if he prejudices the privacy of the individual or family life by committing any of the following acts other than in the events as permitted by law or without the consent of the victim: to eavesdrop, record or transmit by any device of any kind whatsoever conversations in a private place or by way of telephone or any other device, to take or transmit by any device of any kind whatsoever a photo of a person in a private place [...]'. This means that a high-visibility sign, or other forms of appropriate signage, needs to be displayed, if CCTV is installed or that prior written consent needs to be obtained from individuals who may be recorded by CCTV in a specific area.

Dubai Law Number 24 of 2008 (as amended by Law Number 10 of 2014) provides regulations on the use of CCTV in the Emirate of Dubai. Article 16 of the Dubai Law Number 24 of 2008 enumerates the business activities that must satisfy certain security specifications including employing CCTV surveillance. These include hotels and short-stay residences, financial and monetary institutions, the manufacture and sale of precious metals and stones, shooting ranges, military and hunting equipment stores, shopping and leisure centres, precious materials storage facilities, hazardous materials storage facilities, precious commodities stores/outlets, large department stores, petrol stations, internet services, storage services, aircraft and balloon clubs.

The use of CCTV does not require separate registration/notification in the DIFC and the ADGM.

13.2 Are there limits on the purposes for which CCTV data may be used?

The purposes for which CCTV data may be used remains largely unregulated in the UAE. There are no specifications as to the purpose of carrying out monitoring through CCTV yet companies are usually equipped with these devices when they are necessary for the organisation and maintenance of security, depending on the type of activity carried out by the company. Nevertheless, as a general rule, recorded footage should not be used abusively by the employer and the CCTV must not be placed in private areas such as in the toilets and in the prayer rooms.

The DIFC and ADGM Regulations do not provide any limits on the purposes for which CCTV data may be used.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Although there are no sector-specific legislations relevant to employee monitoring in the UAE, a combination of federal, local and free-zone laws are applicable on employers and employees. These laws (such as Article 31 of the UAE Constitution which gives individuals a right to secrecy in their communications) guarantee the right to privacy and safeguarding of personal data of the employee, and may be potentially applicable on instances such as the monitoring and recording of telephone conversations in the workplace. There are no specifications on monitoring employees through the use of CCTV, although employees will have a right of privacy in this regard. As a general rule, employers have the right to monitor and access the company's property which include email servers, devices such as mobile phone, laptops and tablets.

Many businesses are required, by nature, to monitor telephone conversations as a way for managing risk such as banks, trading houses, insurance and brokerage companies. Other companies that are not required by nature to monitor telephone conversations may decide to do so for training purposes and/or to ensure the quality of the services provided by its employees.

In the DIFC, according to DIFC Law Number 1 of 2007, the employee's consent must be obtained to be able to monitor, record or process any personal data related to them (whether by telephone, by CCTV or by email).

In the ADGM, Article 51 of the ADGM Employment Regulations on processing personal data by the employer provides that personal data must not be kept 'for longer than is necessary' by the employer (having regard to the purpose or purposes for which they are being processed).

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

In the mainland of the UAE, according to Federal Laws, specifically the Cybercrime Law, Telecommunications Law and the Penal Code, the employee's consent will have to be obtained in order to be able to monitor them. This provision can be included in the employee's employment contract or in the company's internal policies. With respect to monitoring the employee's emails, the fact that the email server belongs to the company's assets implies that the company will have full access to the server.

In the DIFC, according to DIFC Law Number 1 of 2007, the employee's consent must be obtained to be able to monitor, record or process any personal data related to them (whether by telephone, by CCTV or by email). The same requirements apply to the ADGM.

14.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There are no work councils or any such unions in the UAE.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the mainland of the UAE, the protection guaranteed to an individual's right to privacy implies that there is a general obligation to ensure the security of their personal data. There is no specific authority responsible for ensuring that data are kept secure.

In the DIFC, article 16 of the DIFC Law Number 1 of 2007 imposes an obligation on the data controller to ensure the security of personal data. Article 16 provides that the data controller must implement appropriate technical and organisational measures to protect personal data.

In the ADGM, article 9 of the ADGM 2015 Data Protection Regulations provides that the data controller must ensure the security of the personal data being processed by implementing appropriate technical and organisational measures.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

In the mainland of the UAE, there is no such requirement given that there is no data protection authority.

In the DIFC, Article 16(4) of the DIFC Law Number 1 of 2007 provides that the data controller or the data processor must inform the commissioner of data protection in the event of an unauthorised intrusion to any personal database, whether physical, electronic or otherwise. This must be done 'as soon as practicably possible'. Failure to do so will result in a fine of $5,000.

In the ADGM, there is no specific requirement to report data breaches.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

In the mainland of the UAE, there is no such requirement given that there is no data protection authority.

In the DIFC, there is no requirement to report data breaches to affected data subjects. There is a requirement, according to Article 13 of the DIFC Law Number 1 of 2007, for the data controller to provide the data subject with the following information upon commencing to collect personal data about them:

(a) the identity of the data controller;

(b) the purposes of the processing for which the personal data are intended; and

(c) other information such as the recipients or categories of recipients of the personal data, the existence of the right of access to and the right to rectify the personal data concerning them, and whether the personal data will be used for direct marketing purposes, among other conditions.

In the ADGM, there is no legal requirement to report data breaches to affected data subjects. However, according to Article 6 of the ADGM 2015 Data Protection Regulations, data controllers must provide a data subject whose personal data has been collected with the following information:

(a) the identity of the data controller;

(b) the purposes of the processing for which the personal data are intended; and

(c) other information such as the recipients or categories of recipients of the personal data, the existence of the right of access to and the right to rectify the personal data concerning them, and whether the personal data will be used for direct marketing purposes, among other conditions.

15.4 What are the maximum penalties for data security breaches?

In the mainland of the UAE, the penalties for non-compliance are as follows:

- Article 15 of the UAE Cybercrimes Law states that any person who captures or intercepts any communication through any information network, intentionally and without permission, shall be punished by imprisonment and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments. Any person who disclosed the information obtained unlawfully by receiving or interception of communications shall be punished by imprisonment for a period not less than one year.
- Article 21 of the UAE Cybercrime Law stipulates that a person who used an information network, electronic information system or any of the information technology tools in invading the privacy of a person in cases other than those permitted in Law shall be punished by imprisonment for a period not less than six months, and a fine not less than AED 150,000 (approx. €33,870) and not exceeding AED 500,000 (approx. €112,910) or by any of these punishments by any of the following methods:
  - overhearing, interception, recording, transferring, transmitting or disclosure of conversations, communications or audio or visual materials;
  - capturing pictures of a third party or preparing electronic pictures or transferring, exposing, copying or keeping those pictures; and/or
  - publishing electronic news or pictures or photographs, scenes, comments, statements or information even if they were correct and real.
- Article 22 of the UAE Cybercrime Law states that any person who used without permission any information network, electronic site or information technology tool to expose confidential information obtained by occasion or because of

his work shall be punished by imprisonment for a period not less than six months, and a fine not less than AED 500,000 (approx. €112,910) and not exceeding AED 1,000,000 (approx. €225,815) or by any of these punishments.

In the DIFC, the following penalties apply:

- Maximum fine of $15,000 for failing to process data in accordance with Article 8 of the DIFC Law Number 1 of 2007.
- Maximum fine of $15,000 for failing to comply with legitimate processing requirements in accordance with Article 9 of the DIFC Law Number 1 of 2007.
- Maximum fine of $20,000 if a data controller transfers personal data outside the DIFC in accordance with Article 12(1)(a) of the DIFC Law Number 1 of 2007 and failing to obtain a permit from the commissioner of data protection.

In the ADGM, according to Article 17(3) of the ADGM 2015 Data Protection Regulations, a data controller who fails, without reasonable excuse, to comply with any direction issued by the registrar under section 17(3) shall be liable to a fine of $15,000.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Authority	Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
Commissioner of Data Protection (DIFC)	■ Accessing personal data processed by data controllers or data processors	■ Issuing warnings or admonishments and making recommendations to data controllers ■ Initiating proceedings for contraventions of the law before the Court ■ Imposing fines in the event of non-compliance with its directions ■ Imposing fines for non-compliance with the DIFC Law Number 1 of 2007 ■ Initiating a claim for compensation on behalf of a data subject before the court ■ Acquiring, holding and disposing of property of any description	
Registrar (ADGM)	■ Access personal data processed by data controller or data processors ■ Collect all the information necessary for the performance of its supervisory duties	■ Issue warnings and make recommendations to data controllers ■ Require a data controller by written notice to give specified information or to produce specified documents which relate to the processing of personal data	
Board of Directors (ADGM): Its main function is to make rules in respect to personal data processing activities			

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

There are no data protection authorities in the UAE.

In the DIFC, according to Article 26 of the DIFC Law Number 1 of 2007, the commissioner of data protection has the right to prepare draft regulations and standards or codes of practice with respect to data processing activities. This implies that he may have the right to issue a ban on a particular processing activity.

In the ADGM, according to Article 16 of the ADGM 2015 Data Protection Regulations, the Board of Directors may make rules in respect of any matters related to the processing of personal data. This implies that the Board may have the right to issue a ban on a particular processing activity.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DIFC Law Number 1 of 2007 is largely modelled on the data protection principles emanating from EU Directives, which provide guidance to the DIFC Commissioner of Data Protection in the administration of the DIFC Law Number 1 of 2007. In *Maximillian Schrems v Data Protection Commissioner* [Case no C-362/14] of 6 October 2015, the European Court of Justice invalidated Commission Decision 2000/520/EC which provided protection for personal data transfers from European Union Member States to US Safe Harbor recipients. This has led the DIFC Commissioner of Data Protection to reconsider the adequacy status previously given to transfers of personal data to US Safe Harbor Recipients.

16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

In the ADGM, according to Article 17 of the ADGM 2015 Data Protection Regulations, if the Registrar is satisfied that a data

controller, data processor or data controller established outside the Abu Dhabi Global Market has contravened or is contravening these regulations or any rules made under these Regulations, the Registrar may issue a direction to the data controller requiring him to do or refrain from doing an act, or to refrain from processing any personal data.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In the mainland of the UAE, in the DIFC and in the ADGM, companies are expected to cooperate with foreign e-discovery requests, although there is no legislation forcing them to do so.

17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued on this matter.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In January 2018, the Ministry of Finance addressed the importance of protecting sensitive personal data in financial transactions with respect to collecting, processing and retaining personal data.

18.2 What "hot topics" are currently a focus for the data protection regulator?

Data available on social media is currently a focus for the data protection regulator, as discussions have emerged on whether such data should be kept private or if it can indeed be used to target advertisements on a particular individual.

Acknowledgment

The authors would like to thank Jad Doudar, a Paralegal at BSA Ahmad Bin Hezeem & Associates LLP, for his invaluable assistance in the preparation of this chapter.

Rima Mrad
BSA Ahmad Bin Hezeem & Associates LLP
Gate Precinct 3
DIFC
P.O. Box 262
Dubai
United Arab Emirates

Tel: +971 4 368 5555
Email: rima.mrad@bsabh.com
URL: www.bsabh.com

Rima is a Partner with the Corporate and M&A practice, based in our DIFC offices in Dubai. She is an experienced corporate and insurance lawyer who has practised in the UAE for over eight years. Rima specialises in advising insurance companies, corporate organisations, financial institutions, energy companies and private equity funds on a wide range of legal issues including M&A transactions, due diligence, commercial agreements, commercial-related disputes, IT-related transactions and various regulatory matters.

Rima has also advised and assisted international clients in developing their business throughout the GCC, particularly in relation to regulatory and compliance matters and provides employment advice to companies in relation to policies, structuring and breach of contract.

Nadim Bardawil
BSA Ahmad Bin Hezeem & Associates LLP
Gate Precinct 3
DIFC
P.O. Box 262
Dubai
United Arab Emirates

Tel: +971 4 368 5555
Email: nadim.bardawil@bsabh.com
URL: www.bsabh.com

Nadim is a Senior Associate in our Corporate and M&A, and Intellectual Property practices based in our DIFC office in Dubai. He specialises in transactional corporate work across various industries including media, technology and healthcare.

Nadim advises on a range of local and international corporate and commercial matters including joint ventures, commercial agency, private equity, employment and regulatory. He has assisted clients with implementing mergers and acquisitions as well as represented clients in the negotiation of IP transfer and licensing provisions.

Nadim is fluent in a number of key languages including English, French and Arabic. Nadim holds a J.D. degree from the Hofstra University School of Law and is admitted to practice in the State of New York. He also holds a business management degree.

BSA
BSA Ahmad Bin Hezeem & Associates LLP

BSA Ahmad Bin Hezeem & Associates LLP traces its roots to 2001 when it was first founded in Dubai, with the primary mission of offering legal services that combine comprehensive knowledge of local law with a modernised and progressive approach to legal practice.

Today, following the joining of Senior Partner Dr. Ahmad Bin Hezeem, former Director General of Dubai Courts, and the opening of further offices across the Middle East and now France, we have consolidated our excellence-driven regional reach. Our access to key local authorities and our solid legal expertise across a broad spectrum of industries set us apart as one of the few Dubai-headquartered legal practices that have exceeded their original boundaries.

The growth of BSA is built by teams of innovative legal minds, possessing extensive regional experience and local rights of audience before all courts in the jurisdictions in which we operate, and through the support network of our affiliates in the Middle East and North Africa region (including the GCC), Asia and Europe.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com