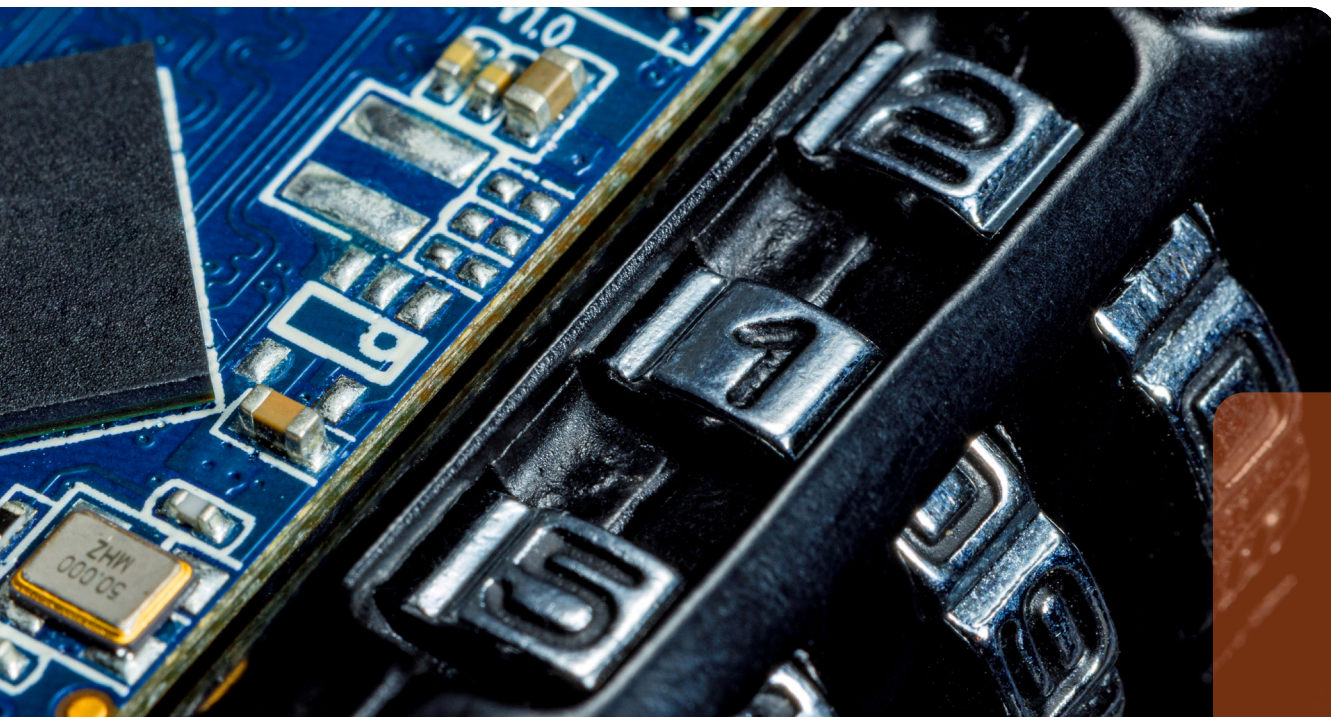


**International
Comparative
Legal Guides**



Data Protection

2024

11th Edition

Contributing Editors:

Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

- 1** **The Rapid Evolution of Data Protection Laws**
Tim Hickman & Detlev Gabel, White & Case LLP
- 8** **Trends in AI Governance in Japan, the Stricter Stance of Data Protection Authorities and Possible Amendments to the Act on the Protection of Personal Information in the Near Future**
Takashi Nakazaki, Anderson Mōri & Tomotsune

Q&A Chapters

- 17** **Australia**
Nyman Gibson Miralis: Dennis Miralis, Arman Salehirad, Darren Pham & Phillip Salakas
- 33** **Brazil**
Pinheiro Neto Advogados: Larissa Galimberti & Luiza Fonseca de Araujo
- 48** **China**
King & Wood Mallesons: Susan Ning & Han Wu
- 64** **Cyprus**
Raphael Legal in association with Privacy Minders: Maria Raphael & Loukis Mavris
- 78** **France**
White & Case LLP: Clara Hainsdorf & Bertrand Liard
- 89** **Germany**
activeMind.legal Rechtsanwalts-gesellschaft mbH: Martin Röleke & Evelyne Sørensen
- 100** **Greece**
Nikolinakos & Partners Law Firm: Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos
- 115** **India**
LexOrbis: Srinjoy Banerjee & Puja Tiwari
- 126** **Indonesia**
ATD Law in association with Mori Hamada & Matsumoto: Abadi Abi Tisnadisastra & Prayoga Mokoginta
- 137** **Ireland**
ByrneWallace LLP: Victor Timon, Zelda Deasy, Seán O'Donnell & Mark Condy
- 150** **Isle of Man**
DQ Advocates: Karen Daly, Kathryn Sharman & Sinead O'Connor
- 161** **Israel**
Barnea Jaffa Lande: Dr. Avishay Klein & Karin Kashi
- 173** **Italy**
FTCC Studio Legale Associato: Pierluigi Cottafavi & Santina Parrello
- 184** **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa
- 197** **Korea**
Bae, Kim & Lee LLC: Kwang Hyun Ryoo, Taeuk Kang, Minwoon Yang & Hyoung Gyu Lee
- 208** **Lithuania**
Sorainen: Stasys Drazdauskas, Sidas Sokolovas & Raminta Matulytė
- 219** **Mexico**
OLIVARES: Abraham Díaz, Gustavo Alcocer & Carla Huitron
- 228** **Morocco**
BFA & Co.: Ayoub Berdai & Idriss Fadel
- 239** **Netherlands**
Kennedy Van der Laan: Hester de Vries
- 252** **Nigeria**
Udo Udoma & Belo-Osagie: Jumoke Lambo, Chisom Okolie & Opeyemi Adeshina
- 267** **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten, Wegard Kyoo Bergli & Ekin Ince Ersvaer
- 282** **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan
- 291** **Saudi Arabia**
Droua Al-Amal Consultants: Saifullah Khan & Saeed Hasan Khan
- 301** **Singapore**
Drew & Napier LLC: Lim Chong Kin & Anastasia Su-Anne Chen
- 317** **Switzerland**
FABIAN PRIVACY LEGAL GmbH: Daniela Fábíán Masoch & Aranya di Francesco
- 327** **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Sam Huang
- 337** **Turkey/Türkiye**
SEOR Law Firm: Okan Or & Derya Aysima Kantarcı
- 348** **Ukraine**
Axon Partners: Oksana Zadniprovska
- 364** **United Arab Emirates**
Bizilance Legal Consultants: Saifullah Khan & Saeed Hasan Khan
- 375** **United Kingdom**
White & Case LLP: Tim Hickman & Aishwarya Jha
- 388** **USA**
White & Case LLP: F. Paul Pittman, Abdul Hafiz & Andrew Hamm

United Arab Emirates



Saifullah Khan



Saeed Hasan Khan

Bizalance Legal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Federal Decree Law No. 45 of 2021 on personal data protection is the principal legislation applicable in the United Arab Emirates (UAE), except for the free zones, which have a specific law on personal data protection (the UAE Law).

The Dubai International Financial Centre (DIFC) Law No. 5 of 2020 (the DIFC Law) is applicable over the DIFC. The DIFC is a free zone.

The Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (the ADGM Regulations) are applicable over the ADGM. The ADGM is also a free zone.

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

Federal Decree Law No. 34 of 2021 on Countering Rumours and Cybercrimes criminalises certain acts to be offences punishable with imprisonment and fine. Collecting and processing personal data and information in violation of the legislation is among one of the crimes that are subject matter of the referred law.

Federal Decree Law No. 33 of 2021, regarding the regulation of employment relationships, provides that workers shall keep the confidentiality of information and data to which they have access by virtue of their work.

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

Sector-specific legislation governs data protection in their respective sectors, as follows:

- Federal Law No. 14 of 2018 (concerning the Central Bank of the UAE) governing data protection of customers of the banks.
- Federal Law No. 3 of 2003 (concerning telecommunication) governing data protection of telecom consumers.
- Federal Law No. 2 of 2019 (concerning use of information and communication technology in health fields) governing confidentiality of the patients' information.

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

- The UAE Data Office is the regulator for the purposes of the UAE Law.
- The Commissioner is to administer the DIFC Law.
- The Commissioner of Data Protection is responsible for the monitoring and enforcement of the ADGM Regulations.
- The Central Bank of the UAE and the Telecommunication and Digital Government Regulatory Authority (TDRA) are the regulators concerning the banking and telecommunication sectors, responsible for (among others) the protection of their respective consumers' data.
- Health authorities (federal or local government) are entrusted for the protection of patients' data.

2 Definitions

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

- **“Personal Data”**
 - **The UAE Law:** Any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, through the linking of data, by reference to an identifier such as his or her name, voice, picture, identification number, electronic identifier, geographical location, or one or more physical, physiological, cultural or social characteristics. Personal data includes sensitive personal data and biometric data.
 - **The DIFC Law:** Any information referring to an identified or identifiable natural person.
 - **The ADGM Regulations:** Any information relating to a data subject.
- **“Processing”**
 - **The UAE Law:** An operation or set of operations which is performed on personal data using any electronic means including other means, such as collection, storage, recording, structuring, adaptation or alteration, handling, retrieval, exchange, sharing, use, characterisation, disclosure by transmission, dissemination, distribution or otherwise making available, alignment, combination, restriction, erasure, destruction or creation of a model of personal data.

- **The DIFC Law: Process, Processed, Processes and Processing (and other variants):** Any operation or set of operations performed upon personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored personal data with the aim of limiting processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on personal data by:
 - (a) a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or
 - (b) law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.
- **The ADGM Regulations:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
 - **The UAE Law:** The establishment or the natural person who is in the possession of the personal data and who by virtue of its activity alone or jointly with others determines the means, methods, standards and purposes of the processing of personal data.
 - **The DIFC Law:** Any person who alone or jointly with others determines the purposes and means of the processing of personal data.
 - **The ADGM Regulations:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“Processor”**
 - **The UAE Law:** An establishment or a natural person who processes the personal data on behalf of the controller and under his or her supervision and instructions.
 - **The DIFC Law:** Any person who processes personal data on behalf of a controller.
 - **The ADGM Regulations:** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **“Data Subject”**
 - **The UAE Law:** The natural person to whom personal data relates.
 - **The DIFC Law:** The identified or identifiable natural person to whom personal data relates.
 - **The ADGM Law:** An identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
 - **The UAE Law:** Any information that directly or indirectly reveals a person’s race, ethnicity, political or philosophical views, religious beliefs, criminal record, biometric data, or any data related to such person’s health such as his or her physical, psychological, mental, corporal, genetic or sexual state, including any information related to such person’s provision with health-care services that reveal his or her health condition.
 - **The DIFC Law: Special Categories of Personal Data:** 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 and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.
 - **The ADGM Regulations: Special Categories of Personal Data:**
 - (a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
 - (b) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation; and
 - (c) personal data relating to criminal convictions and offences or related security measures.
- **“Data Breach”**
 - **The UAE Law:** A breach of security and personal data through unauthorised or unlawful access thereto, such as replication, transmission, distribution, exchange, transfer, circulation or processing in such a manner leading to the disclosure or divulgence to third parties, or otherwise the destruction or modification of such data while being stored, transferred and processed.
 - **The DIFC Law/the ADGM Regulations: Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Consent”**
 - **The UAE Law:** The consent by which the data subject authorises third parties to process personal data relating to him or her, provided that such consent is a clear, specific and unambiguous indication of the data subject’s agreement by a statement or clear affirmative action, to the processing of the personal data relating to him or her.
 - **The DIFC Law:** Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent if it is to be relied on as a basis for processing. If the performance of an act by a controller, a data subject or any other party (including the performance of contractual obligations) is conditional on the provision of consent to process personal data, then such consent will not be considered to be freely given with respect to any processing that is not reasonably necessary for the performance of such act or where the consent relates to excessive categories of personal data. (The term “consent” is not defined. Conditions of consent are described at Section 12(1) of the DIFC Law.)
 - **The ADGM Regulations:** Consent means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they (whether in writing, electronically or orally), by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to him or her.

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 Law, the DIFC Law and the ADGM Regulations have extra territorial scope. In the following circumstances, a business established in another jurisdiction would be subject to these laws:

- **The UAE Law:** A controller or processor not established in the UAE that conducts personal data processing activities for data subjects who are in the UAE.
- **The DIFC Law:** The DIFC Law is applicable to a controller or processor regardless of its place of incorporation that processes personal data in the DIFC as part of stable arrangements.
- **The ADGM Regulations:** The ADGM Regulations are applicable when a processor is processing personal data for a controller outside the ADGM. In this case, the processor is to comply with the ADGM Regulations to the extent possible, taking into account whether the controller is subject to similar obligations under its home jurisdiction.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The UAE Law

The UAE Personal Data Protection Law carves out certain processing activities from its material scope, which are as follows:

- (a) Government data.
- (b) Processing or control of personal data by government authorities.
- (c) Personal data that is being processed/held by the security and judicial authorities.
- (d) A data subject who processes his or her personal data for personal purposes.
- (e) Personal health data that is subject to legislation regulating the protection and processing thereof.
- (f) Any processing of personal banking and credit data that has been done under the relevant legislation which govern the protection of this type of personal data.
- (g) The law is not applicable to companies and institutions situated in freezones and that are under the scope of special data privacy laws.

The DIFC Law

The DIFC Law carves out the natural persons from its material scope, as per the law, to which it does not apply to for the processing of personal data by natural persons, when such personal data processing is being carried out for purely household and personal purposes and does not involve any commercial purpose.

The ADGM Law

As per the ADGM Law, the following two categories have been excluded from its material scope:

- (a) The processing of personal data by a natural person for the purposes of purely personal or household activity.
- (b) When the processing of the personal data has been carried out by the public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or for the execution of any criminal

penalties. Also, when a public authority processes the personal data to safeguard against any anticipated threats to national security and also when such processing is carried out for the prevention of threats to national security.

4 Key Principles

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

The key principles common in the UAE Law, the DIFC Law and the ADGM Regulations are:

- **Fairness, lawfulness and transparency**
Personal data must be processed fairly, lawfully and in a transparent manner.
- **Purpose limitation**
Personal data must be processed for a specified purpose.
- **Data adequacy**
Personal data must be adequate and limited to what is necessary in relation to the purpose of processing.
- **Accuracy**
Personal data must be accurate and updated.
- **Retention**
Once the purpose of processing is completed, personal data must be kept in a manner that does not permit identification of the data subject.
- **Security**
Personal data is to be processed ensuring security of the personal data, including unauthorised or unlawful processing and against accidental loss, destruction or damage by the use of appropriate technical and organisational measures.

5 Individual Rights

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

The following rights are available to individuals under the UAE Law, the DIFC Law and the ADGM Regulations:

- **Right to be informed**
A data subject is to be informed about the collection of his or her personal data, with certain specified information, irrespective of whether the personal data is received from the data subject or from any other source.
- **Right to access to (copies of) data/information about processing**
A data subject has the right to have confirmation and a copy of his or her personal data being processed by the controller.
- **Right to deletion/right to be forgotten**
A data subject has the right to have his or her personal data erased.
- **Right to rectification**
A data subject has the right to have rectified inaccurate personal data or to complete the incomplete personal data.
- **Right to data portability**
A data subject has the right to receive his or her personal data in a structured and commonly used machine-readable format and to transmit the personal data to another controller.
- **Right related to automated decision-making and profiling**
A data subject has the right to not be subjected to a decision solely based on automated decision-making (without human intervention), including profiling.

- **Right to withdraw consent**
A data subject has the right to withdraw his or her consent.
- **Right to object**
A data subject has the right to object to the processing of his or her personal data, including when personal data is being used for direct marketing.
- **Right to complain to the relevant data protection authority**
A data subject has the right to complain to the relevant personal data protection authority in case of any contravention of any of the legal provisions of the UAE Law/the DIFC Law/the ADGM Regulations.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The data subjects have no right to mandate not-for-profit organisations to seek remedies on their behalf.

As regards collective redress, the UAE Law does not have such a provision; however, the DIFC Law and the ADGM Regulations permit class actions. Where multiple data subjects are affected by the same alleged contravention, they may raise a collective complaint. In addition, the Commissioner/Commissioner of Data Protection may choose to deal collectively with multiple allegations which relate to the same contravention, whether or not such allegations are brought collectively.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The UAE Law, the DIFC Law and the ADGM Regulations do not address the processing of children's personal data.

7 Registration Formalities and Prior Approval

7.1 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?

There is no requirement for the registration of controllers or processors under the UAE Law.

The DIFC Law requires that a controller or processor shall register with (and pay the prescribed fee to) the Commissioner.

The ADGM Regulations requires a controller to pay a data protection fee and notify (to the Commissioner of Data Protection) its name, address and the date it commenced processing personal data.

7.2 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)?

The DIFC Law provides that the notification must provide:

- A general description of the personal data processing being carried out.
- An explanation of the purpose of processing.

- The data subjects or class of data subjects whose personal data is being processed.
- A description of the class of personal data being processed.
- A statement of jurisdictions to which personal data will be transferred along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection.

The ADGM Regulations require a controller to notify, to the Commissioner of Data Protection, its name and address and the date it commenced processing personal data.

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

The DIFC Law requires the notification on a controller or processor basis.

The ADGM Regulations requires notification on a controller basis.

7.4 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)?

The DIFC Law requires that a controller or a processor must notify the Commissioner the following processing operations including but not limited to:

- processing of personal data;
- special category data; and
- transfer of personal data to a recipient outside the DIFC which is not subject to laws and regulations that ensure an adequate level of protection.

The ADGM Regulations require that a controller, before or as soon as reasonably practicable, after it starts processing, notify the Commissioner of Data Protection.

7.5 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)?

As stated in question 7.2.

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

The maximum fine, under the DIFC Law, for failure to register/notify is US\$ 25,000.

The ADGM Regulations does not provide for a specific sanction or fine for failure to register/notify. The maximum general administrative fine is up to US\$ 28 million for doing an act prohibited or to omit to do an act, under the ADGM Regulations.

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

The fee for registration/notification under the DIFC Law ranges between US\$ 250 to US\$ 1,250.

The fee for ADGM is US\$ 300.

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

Both the DIFC Law and the ADGM Regulations require renewal on an annual basis.

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

Prior approval from the data protection regulator is not required.

7.10 Can the registration/notification be completed online?

The notification can be completed online, both for the DIFC and the DGM.

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

Under the DIFC Law, the Commissioner is to keep the notifications on a publicly available register maintained by the Commissioner.

The information on ADGM registered controllers is available in the ADGM Public Register of companies.

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

The time to process a notification, at the DIFC and ADGM, depends on the individual circumstances of each controller or processor (how detailed the information to be fed in is).

8 Appointment of a Data Protection Officer

8.1 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.

- A Data Protection Officer (DPO) is required to be appointed when the processing is likely to result in a high risk to the privacy and confidentiality of personal data, due to the adoption of new technologies or due to the amount of data.
- A DPO is required to be appointed where the processing involves a systematic and overall assessment of sensitive personal data, including profiling and automated processing. The executive regulations will specify the kinds of technologies and standards of determination of the amount of data related to the above.

The DIFC Law

- A DPO is required to be appointed by the Commissioner, DIFC Authority and by the Dubai Financial Services Authority.
- A DPO is required to be appointed by a controller or processor performing high-risk activities on a systematic or regular basis.
- A controller or processor (other than above) may be required to designate a DPO by the Commissioner.

The ADGM Regulations

- A DPO is required to be appointed where processing is carried out by a public authority except for courts acting in their judicial capacity.
- A DPO is required to be appointed where core activities of a controller or processor require (on the basis of nature, scope and purposes of processing) regular and systematic monitoring of data subjects on a large scale.
- A DPO is required to be appointed where core activities of a controller or processor consist of processing of a large scale or special categories of personal data.

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

The sanctions/fines under the UAE Law are yet to be prescribed.

Under the DIFC Law, the maximum fine for failure to appoint a DPO is US\$ 50,000.

The ADGM Regulations does not provide for a specific sanction or fine for failure to appoint a DPO. The maximum general administrative fine is up to US\$ 28 million for carrying out a prohibited act or omitting to do an act, under the ADGM Regulations.

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

The UAE Law, the DIFC Law and the ADGM Regulations do not provide any such protection.

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

The UAE Law has no such provision.

The DIFC Law and the ADGM Regulations do allow appointment of a single DPO by a group, provided that the DPO is easily accessible from each entity in the group.

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

There are no specified qualifications for the appointment of a DPO. The general requirement is having adequate skills and knowledge with the applicable data protection law.

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

The responsibilities of a DPO, among others, include:

- Monitoring the compliance of the controller or processor within the applicable legal framework.
- Informing and advising the controller, processor and their respective employees (who carry out personal data processing) about their obligations under the applicable legal framework.
- Acting as the contact point for the concerned regulator.

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

Under the UAE Law, the controller or processor is to designate the contact details of the DPO and inform the UAE Data Office.

There is no such requirement under the DIFC Law.

The ADGM Regulations require that the controller or processor must notify the appointment of a DPO, within one month of appointment, to the Commissioner of Data Protection.

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

There is no such requirement under the UAE Law or the ADGM Regulations.

The DIFC Law requires that a controller or processor shall publish the contact details of its DPO in a manner that is readily accessible to third parties.

9 Appointment of Processors

9.1 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?

The UAE Law requires that controllers are to appoint processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that provisions of the UAE Law could be met.

The DIFC Law/the ADGM Regulations

The processing by a processor is to be governed by a legally binding written agreement between the controller and processor. A processor is to provide sufficient assurances/guarantees to implement appropriate technical and organisational measures to ensure that processing meets the legal requirements and to ensure the protection of rights of the data subjects.

9.2 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.)?

- **The UAE Law:** The processor is to process the personal data upon instructions from the controller and pursuant to the contract between the controller and processor. The said contract is to identify scope, subject, purpose, nature and type of personal data and categories of data subject.
- **The DIFC Law/the ADGM Regulations:** The agreement between the controller and processor is to contain, among others:

The DIFC Law	The ADGM Regulations
<ul style="list-style-type: none"> ■ Subject-matter and duration of the processing. ■ Nature and purpose of the processing. ■ Type of personal data and categories of data subjects. ■ Obligations and rights of the controller. ■ Commitment by the processor to process personal data based on documented instructions from the controller. ■ Ensuring that persons authorised to process relevant personal data are under legally binding written agreements or duties of confidentiality. 	<ul style="list-style-type: none"> ■ The processor is to process the personal data only on documented instructions from the controller. ■ Ensuring that persons authorised to process the personal data have committed themselves to confidentiality. ■ Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures. ■ At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services.

10 Marketing

10.1 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?)

The TDRA has outlined the “Regulatory Policy for Spam Electronic Communications” (the Policy). The Policy requires that licensees (of the TDRA) are to put all practical measures in place to minimise the transmission of spam having a UAE link across their telecommunication networks. The Policy further states that licensees shall not sell, supply, use or knowingly allow access or right to use any tools, software, hardware or mechanisms that facilitate the harvesting and generation of electronic addresses.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The above-mentioned policy does not differentiate as to business-to-consumer or business-to-business.

10.3 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 refer to question 10.1.

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

The above-mentioned policy is applicable only to licensees of the TDRA.

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

No such information is available.

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

The purchase of marketing lists from third parties is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

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

The penalties under the UAE Law are yet to be prescribed. The DIFC Law and the ADGM Regulations do not specifically provide for a penalty for sending marketing communications in breach of applicable restrictions.

11 Cookies

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

The UAE Law confers on the data subject a “right to stop processing” where personal data is processed for direct marketing purposes, including profiling to the extent that profiling is related to such direct marketing.

The DIFC Law provides that 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 that the data subject be expressly offered the right to object for direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling to the extent that such profiling is related to such direct marketing.

The ADGM Regulations carry the same provisions as in the DIFC Law regarding direct marketing. The ADGM Regulations, in addition, provide that when a data subject objects to direct marketing then personal data must not be processed for direct marketing purposes.

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

The restrictions, as stated above, do not distinguish between different types of cookies.

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

No such information is available.

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

The penalties under the UAE Law are yet to be prescribed.

The DIFC Law and the ADGM Regulations do not specifically provide for a penalty for breach of applicable cookie restrictions.

12 Restrictions on International Data Transfers

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

The UAE Law

The UAE Law provides that personal data may only be transferred outside the UAE to a jurisdiction that has a law in place covering various aspects as to the protection of personal data (adequate level of protection). The personal data may also be transferred to those countries with whom the UAE has bilateral or multilateral agreements in respect of personal data protection.

In the absence of an adequate protection, under the UAE Law, personal data may be transferred outside the UAE in the following cases (subject to the controls to be specified by the executive regulations):

- In jurisdictions where data protection law does not exist, on the basis of a contract or agreement binding the establishment (to whom personal data is being transferred) to follow the provisions, measures, controls and conditions of the UAE Law. The said contract or agreement must also specify a supervisory or judicial entity in that foreign country for imposition of appropriate measures against the controller or processor in that foreign country.
- Expressed consent of the data subject, in such a manner that does not conflict with the public and security interest of the UAE.
- Transfer is necessary for performing obligations and establishing rights before judicial entities.
- Transfer is necessary for entering or performance of a contract between the controller and the data subject, or between the controller and a third party for the interests of the data subject.
- Transfer is necessary for the performance of an act relating to international judicial cooperation.
- Transfer is necessary for the protection of public interest.

The DIFC Law

The DIFC Law provides that personal data may be transferred abroad on the basis of adequate level of protection as determined by the Commissioner. A list of adequate jurisdictions is issued through the DIFC Data Protection Regulations.

The ADGM Regulations

The ADGM Regulations permits transferring personal data abroad where the Personal Data Commissioner has decided that the receiving jurisdiction ensures an adequate level of protection. A list of jurisdictions designated as having an adequate level of protection is available at the ADGM website.

Transfer on the Basis of Appropriate Safeguards – The DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection, personal data may be transferred abroad on the basis of “appropriate safeguards”. The “appropriate safeguards” include:

- A legally binding instrument between the public authorities.
- Binding corporate rules.
- Standard data protection clauses.
- Approved code of conduct.
- Approved certification mechanism.

Specific Derogations – The DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection and appropriate safeguards, the data may be transferred outside under the following derogations:

- Explicit consent of the data subject.
- Transfer is necessary for the performance of a contract between the data subject and controller.
- Transfer is necessary for the conclusion or performance of a contract between a controller and a third party which is in the interest of the data subject.
- Transfer is necessary for reasons of public interest.
- Transfer is necessary in accordance with an applicable law.
- Transfer is necessary for establishment, exercise or defence of a legal claim.
- Transfer is necessary to protect the vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent.
- Transfer is made in compliance with applicable law and data minimisation principles to provide information to the public, and is open for viewing by the public in general or by a person who can demonstrate a legitimate interest (under the DIFC Law only).
- Transfer is necessary for compliance with any obligation under applicable law to which the controller is subject, or transfer is made at the reasonable request of a regulator, police or other government agency or competent authority (under the DIFC Law only).
- Transfer is necessary to uphold the legitimate interests of a controller (in international financial markets), subject to international financial standards, except where such interests are overridden by the legitimate interest of the data subject (under the DIFC Law only).
- Transfer is necessary to comply with the anti-money laundering or counter-terrorist financing obligations applicable to a controller or a processor (under the DIFC Law only).

12.2 Please describe the mechanisms businesses 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.).

Please refer to question 12.1.

12.3 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.

Under the DIFC Law, in the absence of an adequate level of protection, absence of appropriate safeguards and absence of derogations, the personal data may be transferred outside only if:

- the transfer is not repeating or part of a repetitive course of transfers;
- the transfer concerns only a limited number of data subjects;
- the transfer is necessary for the purpose of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject; and
- the controller has completed a documentary assessment of all circumstances surrounding data transfer and has on the

basis of such an assessment provided suitable safeguards for the protection of personal data.

In the above case, the controller is to inform the Commissioner and also inform the data subject about the transfer and the controllers' compelling legitimate interests.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The DIFC Law/ADGM Regulations: where a controller or processor will receive a request from any public authority over the person, for the disclosure and transfer of any personal data, the controller or processor should assess the impact of the proposed transfer in light of the potential risks to the right of any affected data subject and, where appropriate, implement measures to minimise risks, including by redacting or minimising the personal data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer of personal data.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

In the background of the *Schrems II* case followed by the US–EU Trans-Atlantic Data Privacy Framework: the DIFC has guided that in case a DIFC entity is part of a multinational or group business that engages in transfers/onward transfers from the EU, then the DIFC entity is to ensure (once personal data leaves the DIFC for processing in the EU) that transfers remain compliant with Article 27 of the DIFC Law (transfers outside the DIFC in the absence of an adequate level of protection).

The ADGM Office of Data Protection has invalidated the EU–US Privacy Shield and confirmed that the ADGM will not continue to recognise the Shield as a legitimate transfer mechanism.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

No guidance has been issued.

13 Whistle-blower Hotlines

13.1 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.)?

The concept of whistle-blowing is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

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

None, in view of the answer to question 13.1.

14 CCTV

14.1 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)?

The use of CCTV is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

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

None, in view of the answer to question 14.1.

15 Employee Monitoring

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

Employee monitoring is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

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

None, in view of the answer to question 15.1.

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

None, in view of the answer to question 15.1.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

It is stipulated in all three laws that a Controller (herein "employer") can process the personal data of the data subject ("employee") for the execution of the contract to which the data subject is party to. An employer, while entering into an employment contract with the employee wherein it is mentioned that the employer can monitor the employee's attendance, is entitled to process the personal data of the employee.

16 Data Security and Data Breach

16.1 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.)?

The UAE Law

The controller and processor are to put in place and implement appropriate technical and organisational measures and actions to ensure a high security level which is appropriate to the risks associated with the processing. These measures are to be in accordance with the best international standards and practices.

The DIFC Law/the ADGM Regulations

The controllers (and processors also under the DIFC Law) are required to implement appropriate technical and organisational measures to protect personal data. In addition, the controllers are required to ensure the security of personal data by following the principles of "data protection by design" and "data protection by default".

16.2 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) expect(s) voluntary breach reporting.

The data controller is required to notify a data breach to the Data Office/Commissioner/Commissioner of Data Protection when the breach is likely to result in a risk to the privacy, confidentiality, security or rights of the data subjects. The processor is to notify, without delay, any such breach to the controller.

The UAE Law requires to notify the breach immediately. The DIFC Law requires to notify the breach as soon as practicable in the circumstances. The ADGM Regulations provides that breach notification be made within 72 hours after having become aware of the breach, and, in case the notification is not reported within 72 hours, then reasons of delay must also accompany the breach notification.

The breach notification is to contain at least the following information:

- description of the nature of the breach;
- details of the DPO;
- likely effects/consequences of the breach;
- description of measures taken or proposed to be taken by the controller to rectify/remedy the breach and the measures to mitigate its effects; and
- any other requirement of the Data Office (only in case of the UAE Law).

16.3 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) expect(s) voluntary breach reporting.

Where a breach is likely to result in a high risk to the security or rights of a data subject, the controller is required to also notify the breach to the data subject. In that case, the reporting requirements and timeframe are the same as those mentioned at question 16.2.

16.4 What are the maximum penalties for personal data security breaches?

The penalties under the UAE Law are yet to be prescribed.

Under the DIFC Law, the maximum fine for failure to implement and maintain technical and organisational measures to protect personal data is US\$ 50,000.

The ADGM Regulations do not provide for a specific sanction or fine for data security breaches. The maximum general administrative fine is up to US\$ 28 million for carrying out a prohibited act or to omit to carry out an act, under the ADGM Regulations.

17 Enforcement and Sanctions

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

The UAE Law

The UAE Data Office is responsible for enforcing data privacy under the UAE Law. The UAE Data Office is competent to receive and decide the complaints of data subjects regarding contravention of the provisions of the UAE Law. The Data Office is also competent to impose administrative sanctions.

The DIFC Law

The Commissioner (DIFC) administers the DIFC Law. The Commissioner (DIFC) is empowered to receive and decide complaints concerning the contravention of the DIFC Law. The Commissioner (DIFC) is also empowered to investigate complaints and to issue directions or declarations on the complaints and impose fines.

The ADGM Regulations

The Commissioner of Data Protection for the ADGM (the ADGM Commissioner) is responsible for enforcement of the ADGM Regulations. The ADGM Commissioner is empowered to receive and decide complaints regarding the contravention of the ADGM Regulations and to impose fines. The ADGM Commissioner is also competent to carry out investigations and to issue directions.

17.2 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?

The UAE Data Office has no such powers.

The Commissioner (DIFC) is empowered to issue directions to refrain from processing personal data specified in the direction, for a purpose or in a manner specified in the direction. A court order is not required in this regard.

The Commissioner of Data Protection (ADGM) has the power to impose a temporary or permanent limitation (including a ban) on the processing. A court order is not required in this regard.

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

No such information is available.

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

No such information is available.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Foreign e-discovery requests are responded to considering the relevant circumstances in each particular case.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued in this regard.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

No details are available concerning enforcement trends.

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

Executive regulations pursuant to the UAE Law are to be announced, which will provide procedural aspects with respect to matters provided for in the UAE Law.



Saifullah Khan is an international trade, IT and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to the emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Bizilance Legal Consultants

D 3-4, Office 302
Al Sarab Tower, Level 15
ADGM Abu Dhabi
United Arab Emirates

Tel: +971 58 184 8960
Email: saifullah.khan@bizilancelegal.ae
LinkedIn: www.linkedin.com/in/saifullahkhan



Saeed Hasan Khan has more than 20 years' experience advising clients on issues such as taxation, corporate, regulatory compliance and contractual obligations, and in representing clients before the authorities. Mr. Khan has developed a keen professional interest in emerging laws on personal data protection, and has gained an understanding of the underlying concepts and principles governing global data protection laws, including the EU's General Data Protection Regulation. He has carried out a great deal of research on personal data protection laws in various jurisdictions in order to compare their core legal principles. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course from the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Bizilance Legal Consultants

D 3-4, Office 302
Al Sarab Tower, Level 15
ADGM Abu Dhabi
United Arab Emirates

Tel: +971 52 914 1118
Email: saeed.hasan@bizilancelegal.ae
LinkedIn: www.linkedin.com/in/saeed-hasan-khan-1338a63a

Bizilance Legal Consultants practises trade remedy laws, privacy and data protection, taxation, and antitrust and competition, among others. The firm is backed by the rich experience of its partners, spread over two decades. The partners have served clients in multiple jurisdictions, including the UAE, the USA, the UK, Switzerland, Singapore, China, Malaysia, Indonesia, Korea, Thailand and Pakistan. In the personal data and privacy space, Bizilance Legal Consultants at Abu Dhabi Global Market is strategically well placed to serve multi-jurisdictional clients in an era when laws related to personal data protection have either just been implemented or are in the process of being implemented.

www.bizilancelegal.ae

Bizilance
Legal Consultants

International Comparative Legal Guides

The **International Comparative Legal Guide (ICLG)** series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

