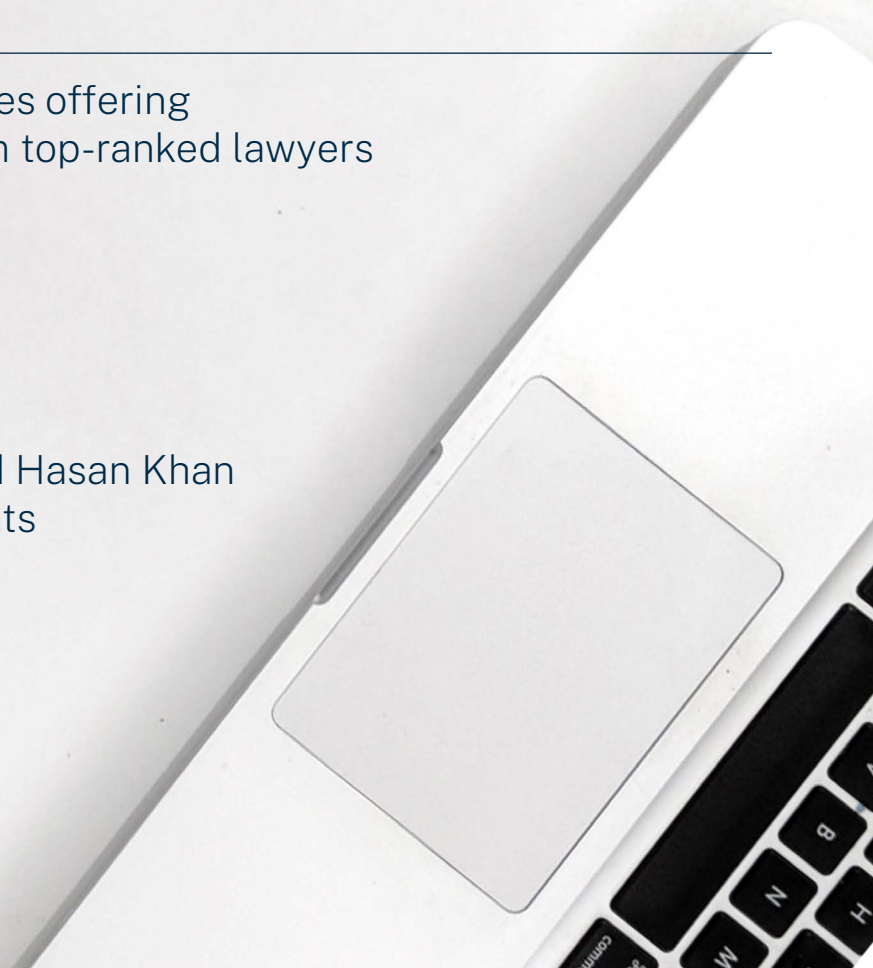

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

Definitive global law guides offering
comparative analysis from top-ranked lawyers

UAE: Law & Practice

Saifullah Khan and Saeed Hasan Khan
Bizilance Legal Consultants





Law and Practice

Contributed by:

Saifullah Khan and Saeed Hasan Khan

Bizilance Legal Consultants

Contents

1. Basic National Regime p.5

- 1.1 Laws p.5
- 1.2 Regulators p.5
- 1.3 Administration and Enforcement Process p.6
- 1.4 Multilateral and Subnational Issues p.6
- 1.5 Major NGOs and Self-Regulatory Organisations p.6
- 1.6 System Characteristics p.6
- 1.7 Key Developments p.7
- 1.8 Significant Pending Changes, Hot Topics and Issues p.7

2. Fundamental Laws p.7

- 2.1 Omnibus Laws and General Requirements p.7
- 2.2 Sectoral and Special Issues p.10
- 2.3 Online Marketing p.11
- 2.4 Workplace Privacy p.12
- 2.5 Enforcement and Litigation p.12

3. Law Enforcement and National Security Access and Surveillance p.13

- 3.1 Laws and Standards for Access to Data for Serious Crimes p.13
- 3.2 Laws and Standards for Access to Data for National Security Purposes p.13
- 3.3 Invoking Foreign Government Obligations p.13
- 3.4 Key Privacy Issues, Conflicts and Public Debates p.13

4. International Considerations p.13

- 4.1 Restrictions on International Data Issues p.13
- 4.2 Mechanisms or Derogations That Apply to International Data Transfers p.14
- 4.3 Government Notifications and Approvals p.15
- 4.4 Data Localisation Requirements p.15
- 4.5 Sharing Technical Details p.15
- 4.6 Limitations and Considerations p.15
- 4.7 "Blocking" Statutes p.15

5. Emerging Digital and Technology Issues p.16

- 5.1 Addressing Current Issues in Law p.16
- 5.2 "Digital Governance" or Fair Data Practice Review Boards p.16
- 5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation p.16
- 5.4 Due Diligence p.16
- 5.5 Public Disclosure p.16
- 5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI) p.16
- 5.7 Other Significant Issues p.16

Bizilance Legal Consultants practises trade remedy laws, privacy and data protection, taxation, and antitrust and competition, among other areas. 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 is strategically well placed in Abu Dhabi Global Market 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.

Authors



Saifullah Khan of Bizilance Legal Consultants 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 customs law, competition law, data privacy, and WTO trade remedy laws. With regard to the emerging discipline of data privacy, Saifullah advises clients from different jurisdictions about data privacy compliance and cross-border transfer of data. 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.



Saeed Hasan Khan of Bizilance Legal Consultants has more than 20 years' experience of advising and representing clients on issues such as taxation, corporate, regulatory

compliance and contractual obligations. Saeed 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. Saeed 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.

Bizilance Legal Consultants

D 3-4
Office 302
Al Sarab Tower
Level 15
ADGM Abu Dhabi
UAE

Tel: +971 52 914 1118
Email: Saeed.hasan@bizilancelegal.ae
Web: www.bizilancelegal.ae

Bizilance
Legal Consultants

1. Basic National Regime

1.1 Laws

The Constitution of the United Arab Emirates (“the Constitution” provides that safety and security for all citizens shall be the pillars of the society. The Constitution further provides that freedom of corresponding through post, telegraph or other means of communication, and the secrecy thereof, is guaranteed in accordance with the law and that dwellings are inviolable. These constitutional provisions serve as the foundational guidelines to respect privacy.

The statutory regime concerning data protection is chiefly found in the following laws/regulations.

- Federal Decree Law No 45 of 2021 on personal data protection (the “UAE Law”) – the UAE Law is a federal-level law applicable across the UAE, except for the following:
 - (a) governmental data;
 - (b) government authorities which control and process personal data;
 - (c) security and judicial authorities;
 - (d) health-related personal data;
 - (e) banking and credit personal data; and
 - (f) companies and organisations incorporated in free zones.
- Dubai International Financial Centre (DIFC) Law No 5 of 2020 (the “DIFC Law”) – DIFC is a free zone and the DIFC Law applies in the jurisdiction of DIFC.
- Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (the “ADGM Regulations”) – ADGM is a free zone and the ADGM Regulations apply in the context of the establishment of a controller or a processor in ADGM.

Apart from the above, sector-specific regulations govern 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 telecommunications) governing data protection of telecommunications consumers; and
- Federal Law No 2 of 2019 (concerning use of information and communication technology in health fields) governing confidentiality of the patients’ information.

The above-mentioned laws/regulations provide for matters related to offences, penalties and enforcement in their respective sphere.

1.2 Regulators

The UAE Data Office is the regulator for the purposes of the UAE Law.

The Commissioner administers 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 Telecommunications and Digital Government Regulatory Authority (TDRA) are the regulators concerning banking and telecommunications sectors, responsible for (among others) the protection of their respective consumers data.

Health authorities (federal or local government) are entrusted to protect patients’ data.

The above-mentioned authorities have the powers to conduct investigations and handle complaints in their respective spheres.

1.3 Administration and Enforcement Process

The Data Office is competent to receive complaints by data subjects regarding contravention of provisions of the UAE Law. The Data Office also has the authority to impose administrative sanctions on contravention of provisions of the UAE Law. A person aggrieved by any decision, administrative sanction or any action of the Data Office may file a grievance with the Director General of the Data Office. The grievance must be filed within 30 days of the date of the decision, administrative sanction or action by the Data Office. The Director General of the Data Office must determine such grievance within 30 days of its filing. The executive regulations to be issued pursuant to the UAE Law will specify the procedural aspects for filing and deciding the grievances.

The Commissioner (under the DIFC Law) is competent to receive complaints from data subjects concerning contravention of the DIFC Law or any breach of the rights of data subjects. The Commissioner has the authority to investigate the complaints and to issue direction or a declaration. The Commissioner is empowered to impose fines in the event of non-compliance with a direction they issue. The Commissioner, concerning a complaint lodged with the Commissioner, may follow such practices and procedures that – in their view – will lead to the most timely, fair and effective resolution of the claim in the complaint. The controller or processor or data subject being aggrieved by the decision of the Commissioner may appeal to the DIFC Court within 30 days.

A data subject may lodge a complaint, on contravention of the ADGM Regulations, with the Commissioner of Data Protection under the ADGM Regulations. Following an assessment,

the Commissioner of Data Protection may dismiss the complaint, uphold the complaint, uphold the complaint but with no further action, or take any further action. The controller, processor or data subject being aggrieved may refer the matter to the court for review. The court may make any orders that the court thinks just and appropriate in the circumstances, within three months following the penalty notice, direction, or the date of complaint.

1.4 Multilateral and Subnational Issues

The UAE Law, the DIFC Law and the ADGM Regulations conceptually follow the basic principles of the EU's GDPR. The UAE Law is a federal-level law and there are no subnational (emirate)-level laws concerning personal data protection.

1.5 Major NGOs and Self-Regulatory Organisations

There are no NGOs or industry self-regulatory organisations (SROs) concerning data protection.

1.6 System Characteristics

The UAE Law follows a hybrid system, which is not applicable to free zones, banks, and health-related personal data. Apart from these exceptions, the UAE Law is applicable to all sectors. Further, the Data Office is empowered to exempt certain establishments that do not process personal data on a large scale from any or all requirements of the UAE Law, in accordance with the standards and controls to be specified by the executive regulations.

The DIFC Authority Board of Directors is empowered to make regulations to exempt controllers (within DIFC jurisdiction) from compliance with the DIFC Law or any part of the DIFC Law.

The ADGM Regulations do not apply to the processing of personal data by public authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This includes processing data for the purposes of safeguarding against and preventing threats to national security.

1.7 Key Developments

The UAE Law was issued on 20 September 2021 and came into effect on 2 January 2022.

1.8 Significant Pending Changes, Hot Topics and Issues

The executive regulations were to be issued by the Cabinet of the UAE within six months of the date of issuance of the UAE Law. However, the executive regulations have not been issued so far. The controllers and processors must comply with the provisions of the UAE Law within a period of six months following the issuance of executive regulations. The referred period of six months may be extended by the Cabinet for additional similar periods.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

General Requirements

The general requirements (general principles) regarding processing of personal data under the UAE Law, the DIFC Law and the ADGM Regulations are:

- fairness, transparency and lawfulness;
- purpose specification;
- adequacy and relevance; and
- safety and security.

Data Protection Officers

The requirements for appointment of a Data Protection Officer (DPO) are as follows.

UAE Law

Under the UAE Law, a DPO is required to be appointed where:

- the processing is likely to result in a high risk to the privacy and confidentiality of personal data, owing to the adoption of new technologies or owing to the amount of data; and
- 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 related to the foregoing.

DIFC Law

A DPO is required to be appointed by:

- the Commissioner, the DIFC Authority and the Dubai Financial Services Authority; and
- a controller or processor performing high-risk activities on a systematic or regular basis.

A controller or processor (other than the aforementioned) may be required to designate a DPO by the Commissioner.

ADGM Regulations

Under 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;
- the core activities of controller or processor require (on the basis of the nature, scope and purposes of processing) regular and system-

- atic monitoring of data subjects on a large scale; and
- the core activities of the controller or processor consist of large-scale processing of special categories of personal data.

Responsibilities of a DPO

Among other things, the DPO is responsible for:

- monitoring the compliance of 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; and
- acting as contact point for the regulator concerned.

Consent

The UAE Law provides certain exceptions where processing may be carried out without consent. These include circumstances where:

- processing is necessary for reasons of public interest;
- processing relates to personal data made publicly available by the data subject;
- processing is necessary to initiate or defend proceedings related to legal actions and claims of rights or in relation to judicial or security procedures;
- processing is necessary for the purposes of medical diagnosis, occupational or preventive medicine, to assess working capacity of employee, etc (in accordance with the applicable law);
- processing is necessary for the protection of public health (in accordance with the applicable law);

- processing is necessary for archiving, scientific, historical or statistical studies (in accordance with the applicable law);
- processing is necessary to protect the interests of the data subject;
- processing is necessary for the performance of obligations and the establishment of rights related to recruitment or social security (in accordance with the applicable law);
- processing is necessary for the performance of a contract to which the data subject is a party or for taking actions at the request of the data subject for the purpose of concluding, amending or terminating a contract;
- processing is necessary for compliance with obligations prescribed under laws of the UAE to which the controller is subject to; or
- situations specified by the executive regulations.

However, in case of the DIFC Law and the ADGM Regulations, consent is one of the “lawful” bases to process the personal data.

Privacy by Design and Privacy by Default

The UAE Law does not specifically mention the concept of “privacy by design” or “privacy by default”. However, the DIFC Law and the ADGM Regulations provide that a controller protects the privacy by design and by default. The DIFC Law imposes this requirement on a processor as well.

Data Protection Impact Assessment

Controllers are required to undertake a “data protection impact assessment” before carrying out processing that is likely to result in a high risk to the rights of natural persons. In addition, the DIFC Law imposes a mandatory requirement for a data protection impact assessment in cases where:

- processing involves systematic and extensive evaluation of personal aspects of the data subject, which is based on automated processing (including profiling) having legal effects that significantly impact the data subject; and
- processing involves large amounts of sensitive personal data.

Data Protection Policy

The UAE Law does not require the adoption of any internal or external data protection policy. The DIFC Law and the ADGM Regulations do require that a data protection policy is put in place and implemented.

Rights of data subjects

Data subjects enjoy the following rights (under the UAE Law, the DIFC Law and the ADGM Regulations):

- rights of access, rectification and erasure;
- the right to withdraw consent;
- the right to restrict processing;
- the right to object to processing;
- the right not to be subjected to automated decision-making, including profiling; and
- the right to data portability.

Data breach notification

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 must notify any such breach to the controller without delay.

The UAE Law requires immediate notification of the breach. The DIFC Law requires the breach to be notified as soon as practicable in the circumstances. The ADGM Regulations provide that

breach notification be made within 72 hours of becoming aware of the breach and, if the notification is not reported within 72 hours, then reasons of delay must accompany the breach notification.

The breach notification must contain at least the following information:

- description of 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, as well as the measures to mitigate its effects; and
- any requirement of the Data Office (only in case of the UAE Law).

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 data subject of the breach.

Anonymisation/pseudonymisation

The UAE Law requires a controller to implement appropriate measures during the identification of means of processing or during processing for the purposes of compliance with the UAE Law. Such measures include pseudonymisation.

In the context of “cessation of processing”, the DIFC Law and the ADGM Regulations require the controller to ensure that all personal data (including personal data held by the processor) is anonymised and pseudonymised.

Automated decision-making

The data subject has the right to object to automated decision-making (including profiling) that has legal implications or consequences affecting a data subject.

Injury/harm

The UAE Law does not provide for any concept of injury/harm (nor compensation thereof) in relation to a grievance suffered by a data subject, whereas the DIFC Law and the ADGM Regulations provide that a data subject who suffers material or non-material damage as a result of contravention of the applicable law/regulations is entitled to compensation. The claim for compensation is to be brought before the court. The compensation will not limit or affect any fine to be imposed on a controller or a processor for contravention of any provision of the applicable law/regulations.

2.2 Sectoral and Special Issues

Banking Sector

Federal Law No 14 of 2018 (the “Central Bank Law”) requires that all data and information related to customers should be considered confidential in nature. The Central Bank of the UAE has published its Consumer Protection Regulations, which apply to all financial institutions licensed by the Central Bank of the UAE. These regulations require that licensed financial institutions are to collect the minimum amount of consumer data and information required in relation to the licensed financial institution’s activities. Under these regulations, licensed financial institutions must:

- establish a function in their respective organisations responsible for data management and protection, thereby maintaining policies, procedures, systems and controls to protect the personal data of consumers;
- have policies specifying time duration or record-keeping and retention in accordance with the applicable laws, regulations and business;
- have appropriate security and monitoring measures to detect and track unauthorised

internal access to or use of consumer information;

- notify all significant breaches of consumer data to the Central Bank of the UAE and notify the consumer without delay where a breach may have risk to the financial and personal security of the consumer; and
- ensure that consumers are able to make informed choices regarding their consent to sharing of their data with third parties and within the licensed financial institution.

Telecommunications Sector

The TDRA’s consumer protection regulations require telecommunications service providers to take all reasonable measures to prevent the unauthorised disclosure or unauthorised use of subscriber information. Telecommunications service providers are further required to take all reasonable measures to protect the privacy of subscriber information.

Health Sector

Federal Law No 2 of 2019 (on the use of information and communication technology in health fields) was issued to collect, analyse and keep health information and to ensure the safety and security of health data and information. This law requires that information related to patients is kept confidential and is not used for any non-health purpose without obtaining the written approval of the patient, except for:

- health information or data required by health insurance companies or by any health services funding entity;
- scientific and clinical research purposes, provided that the identity of the patients is not disclosed and that ethics and rules of scientific research are respected;
- to take preventive and curative measures related to public health;

- on the request of the competent judicial entities; and
- on the request of the Health Authority for the purposes of control, inspection and protection of public health.

Under Federal Law No 2 of 2019, health information and data may not be stored, processed, generated or transferred outside the UAE except on a decision issued by the Health Authority in co-ordination with the Ministry of Health and Prevention. Health information and data must be kept for a period commensurate with the need provided; it may not be less than 25 years from the date of the last health procedures provided to the concerned person.

Sensitive Personal Data/Special Categories of Personal Data

“Sensitive personal data”, under the UAE Law, refers to:

- any information that directly or indirectly reveals a person’s race, ethnicity, political or philosophical views, religious beliefs, or criminal record;
- biometric data;
- or any data related to a person’s health, such as physical, psychological, mental, corporal, genetic or sexual state (including information concerning the provision of healthcare services to the person if it reveals their health condition).

“Special categories of personal data”, under the DIFC Law, means personal data revealing or connecting (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade union membership and health or sex life, including genetic and biometric

data where it is used for the purpose of uniquely identifying a natural person.

The ADGM Regulations have a similar definition of special categories of personal data to the DIFC Law.

The UAE Law states that a personal data protection impact assessment is a necessity where processing involves large amounts of sensitive personal data.

The DIFC Law and the ADGM Regulations permit processing of special categories of personal data in certain specified situations, including:

- with the explicit consent of the data subject;
- where processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or data subject concerning employment;
- where processing is necessary to protect vital interests of the data subject;
- processing by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities;
- processing related to personal data that has been made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims; or
- where processing is necessary for compliance with a specific requirement of a law applicable to the controller.

2.3 Online Marketing

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

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

2.4 Workplace Privacy

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

The UAE Law, the DIFC Law and the ADGM Regulations do not contain any provisions concerning the role of labour organisations, whistleblowing or e-discovery.

2.5 Enforcement and Litigation

The executive regulations pursuant to the UAE Law have not yet been issued. The executive regulations will provide for the procedural aspects concerning enforcement and litigation arising out of the UAE Law.

The DIFC Law requires that the Commissioner, for the purposes of issuing any direction pursuant to a complaint or on the basis of other information within their knowledge, may under-

take reasonable and necessary inspections or investigations.

The ADGM Regulations require that, before a penalty notice is given to a controller or processor, the Commissioner of Data Protection must give a written “Notice of Intent” to the controller or processor concerned. The Notice of Intent must provide:

- the reasons for issuing a penalty notice;
- an indication of the amount of the penalty;
- the time within which controller or processor may make written representations to the Commissioner of Data Protection (at least 21 days from the date of Notice of Intent); and
- whether the Commissioner of Data Protection considers it appropriate to provide an opportunity to make oral representation.

The executive regulations to be issued under the UAE Law will specify the penalties/administrative sanctions to be imposed for contravention of the UAE Law.

Schedule 2 to the DIFC Law sets the administrative fines for contravention of provisions of the DIFC Law. The maximum fine is USD100,000.

The ADGM Regulations provide that the maximum administrative fine must not exceed USD28 million.

No details are available with regard to any enforcement cases.

The DIFC Law and the ADGM Regulations do allow class actions. However, 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 that relate to the same contravention, whether or not such allegations are brought collectively.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Federal Law No 20 of 2018 governs anti-money laundering and combating the financing of terrorism. Under this law, the supervisory authorities, financial intelligence unit, law enforcement authorities and designated non-financial businesses and professions are exempted from criminal, civil or administrative responsibility in relation to the following:

- providing any requested information; or
- violating any obligation under legislative, contractual and administrative directives aimed at securing confidentiality of information.

The above-mentioned exemption, however, is not available if the disclosure is made in bad faith or with the intent to cause damages to others.

3.2 Laws and Standards for Access to Data for National Security Purposes

Federal Law No 7 of 2014 governs the combating of terrorism offences. Under this law, the Central Bank of the UAE, financial institutions and other financial, commercial and economic institutions are not held responsible (criminally or civilly) upon violation of restrictions imposed for guaranteeing the confidentiality of the information in relation to implementation of the provisions of the law in question. This immunity, however, is not available in the case of procedures adopted by these institutions in bad faith.

This law also provides that all the authorities (concerned with the implementation of the law in question) must undertake to keep all the information obtained in connection with the implementation of said law confidential and not disclose such information unless to the extent necessary for evidence-gathering or for investigation.

3.3 Invoking Foreign Government Obligations

The laws (the UAE Law, the DIFC Law and the ADGM Regulations) do not provide for a foreign government access request to be a legitimate basis for transferring personal data outside the jurisdiction. The situations in which personal data may be transferred outside UAE are discussed in **4.1 Restrictions on International Data Issues** and **4.2 Mechanisms or Derogations That Apply to International Data Transfers**.

3.4 Key Privacy Issues, Conflicts and Public Debates

Currently, free zones (except for DIFC and ADGM, which have their own legal framework concerning personal data protection) do not have any law or regulation by which to govern and protect the collection and processing of personal data. It is likely that free zones will issue their respective laws or regulations in this respect.

4. International Considerations

4.1 Restrictions on International Data Issues

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 concerning the protection of personal data (ie, 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.

The DIFC Law provides that personal data may be transferred to a third country or to an international organisation on the basis of an adequate level of protection, as determined by the Commissioner. A list of adequate jurisdictions is issued through DIFC Data Protection Regulations.

The ADGM Regulations allow the transfer of personal data outside ADGM or to an international organisation where the Personal Data Commissioner has decided that the receiving jurisdiction or the international organisation ensures an adequate level of protection.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

In the absence of 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 without data protection laws, personal data can be transferred to establishments through a contract or agreement binding the establishment to follow the provisions, measures, controls, and conditions of the UAE Law (said contract should also specify a supervisory or judicial entity in that foreign country to enforce measures against the local controller or processor);
- with the express consent of the data subject, in such a manner that does not conflict with the public and security interest of the UAE;
- where transfer is necessary for performing obligations and establishing rights before judicial entities;

- where 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;
- where transfer is necessary for the performance of an act relating to international judicial co-operation; and
- where transfer is necessary for the protection of public interests.

In the absence of an adequate level of protection, personal data may be transferred to a third country under the DIFC Law and the ADGM Regulations on the basis of “appropriate safeguards”, which include:

- a legally binding instrument between the public authorities;
- binding corporate rules;
- standard data protection clauses;
- an approved code of conduct; and
- an approved certification mechanism.

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

- with the explicit consent of the data subject;
- where transfer is necessary for the performance of a contract between data subject and controller;
- where transfer is necessary for the conclusion or performance of a contract between a controller and a third party that is in the interest of data subject;
- where transfer is necessary for reasons of public interest;
- where transfer is necessary in accordance with an applicable law;

- where transfer is necessary for the establishment, exercise or defence of a legal claim;
- where transfer is necessary to protect vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent;
- where 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 DIFC Law only);
- where transfer is necessary for compliance with any obligation under an applicable law to which a controller is subject or where transfer is made at the reasonable request of a regulator, police or other government agency or competent authority (under DIFC Law only);
- where 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 DIFC Law only); or
- where transfer is necessary to comply with anti-money laundering or counter-terrorist financing obligations applicable to a controller or a processor (under DIFC Law only).

The DIFC Law permits the following further modes of international transfer of personal data (when transfer could not be made under any of the above-discussed modes):

- transfer that is not repeating or part of a repetitive course of transfers;
- transfer that concerns only a limited number of data subjects;
- transfer that is necessary for the purposes of compelling legitimate interests pursued by

the controller that are not overridden by the interests or rights of the data subject; and

- transfer where the controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data.

4.3 Government Notifications and Approvals

No government notifications or approvals are required to transfer data internationally, except in the case of health data (see **4.4 Data Localisation Requirements** for further discussion).

4.4 Data Localisation Requirements

There are no data localisation requirements, apart from in relation to health information and data. Under Federal Law No 2 of 2019, health information and data may not be stored, processed, generated or transferred outside the UAE, except following a decision issued by the Health Authority in co-ordination with the Ministry of Health and Prevention.

4.5 Sharing Technical Details

There are no such requirements to share any software code, algorithms or similar technical details with the government.

4.6 Limitations and Considerations

The limitations or considerations concerning international transfer of personal data are those discussed at **4.1 Restrictions on International Data Issues** and **4.2 Mechanisms or Derogations That Apply to International Data Transfers**.

4.7 “Blocking” Statutes

There are no blocking statutes in the UAE.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The Central Bank of the UAE, the Securities and Commodities Authority, DIFC's Dubai Financial Services Authority, and ADGM's Financial Services Regulatory Authority have issued Bank Guidelines on the application of the key principles in the use of:

- application programming interface (API);
- cloud computing;
- biometrics;
- big data analytics and AI; and
- distributed ledger technology.

The Bank Guidelines require that all APIs should be designed on a “privacy by design” basis – ie, in a way that only exposes relevant data elements to any party in order to fulfil the purpose of the API. The Bank Guidelines further require that financial institutions should ensure that personal data being transmitted or stored is in encrypted form so as to enable privacy and integrity.

Unmanned Aircraft Systems/Drones

The General Civil Aviation Authority (GCAA) of the UAE is the regulatory body concerning the registration of Unmanned Aircraft Systems (UAS)/drones in the UAE. GCAA registers the following two types of users of UAS/drones:

- individual/private (recreational);
- organisation/operator (commercial and non-commercial).

Under the relevant regulations issued by the GCAA, use of aerial photographic apparatus installed on UAS/drones will not be permitted without prior authorisation by the GCAA.

5.2 “Digital Governance” or Fair Data Practice Review Boards

There is no requirement with regard to digital governance or fair data practice review boards or committees.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

No details are available concerning any regulatory enforcement or litigation.

5.4 Due Diligence

There is no uniform process concerning due diligence in corporate transactions. The entities perform due diligence based upon their individual risk appetite and underlying circumstances with regard to the nature and complexity of a particular transaction.

5.5 Public Disclosure

There is no requirement for making public disclosure regarding an organisation's cybersecurity risk profile or experience.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

Law No 4 of 2022 regulating virtual assets in the Emirate of Dubai has been issued. Pursuant to this law, the Dubai Virtual Assets Regulatory Authority (DVARA) has been established. The DVARA regulates the operation of virtual asset platforms in the Emirate of Dubai (including all special development zones and free zones except DIFC).

5.7 Other Significant Issues

Federal Decree Law No 46 of 2021 on electronic transactions and trust services (the “Electronic Transactions Law”) came into effect on 2 January 2022 and has repealed Federal Law No 1 of

2006 on electric commerce and transactions. As regulator, the TDRA will implement this law. The Electronic Transactions Law provides means for regulating electronic identification systems and trust services. Executive regulations to implement the new law are to be issued. The Electronic Transactions Law fully recognises electronic signatures and electronic documents as having full legal validity and enforceability. Trust service providers must be licensed by the TDRA to render electronic signatures services.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com