Chambers
Global Practice
Guides

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

Data Protection & Privacy 2022

UAE: Law & Practice
Saifullah Khan and Saeed Hasan Khan
Bizilance Legal Consultants

practiceguides.chambers.com

UAE

Law and Practice

Contributed by:
Saifullah Khan and Saeed Hasan Khan
Bizilance Legal Consultants see p.15

CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

The Constitution of United Arab Emirates (UAE) 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 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:

- governmental data;
- government authorities which control and process personal data;
- security and judicial authorities;
- health-related personal data;
- banking and credit personal data;
- companies and organisations incorporated in free zones.

Dubai International Financial Center (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 processer in ADGM.

Apart from the above, sectoral 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 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.

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 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 Telecommunication and Digital Government Regulatory Authority (TDRA) are the regulators concerning 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.

The above-mentioned authorities have the powers of investigations and complaint handling in their respective sphere.

1.3 Administration and Enforcement Process

The Data Office (concerning the UAE Law) is competent to receive complaints by data subjects regarding contravention of provisions of the UAE Law. The Data Office is also competent 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 is to be filed within 30 days of the date of decision, administrative sanction or action of the Data Office. The Director General of the Data Office is to 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 is empowered 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 issued by him. The Commissioner, concerning a complaint lodged with him, may follow such practices and procedures that in the view of the Commissioner will lead to most timely, fair and effective resolution of the claim in the complaint. The controller or processer or data subject being aggrieved by the decision of the Commissioner may appeal, within 30 days, to the DIFC Court.

A data subject may lodge a complaint, on contravention of the ADGM Regulations, with the Commissioner of Data Protection under the ADGM Regulations. The Commissioner of Data Protection, after an assessment, may dismiss the complaint, uphold the complaint, uphold the complaint but with no further action, or take any further action. The controller, processer or data subject being aggrieved may refer the matter to the court for review. The court may make any orders that the court think just and appropriate in the circumstances, within three months of 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 non-governmental organisations (NGOs) or industry self-regulatory organisations (SROs) concerning data protection.

1.6 System Characteristics

The UAE Law follows a hybrid system; it is not applicable to free zones, banks and health-related personal data. Apart from these exclusions, the UAE Law is applicable to all sectors. Further, the Data Office is empowered to exempt certain establishments which do not process large scale of personal data 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 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, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding

against and the prevention of 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 are to be issued by the Cabinet of the UAE within six months of the date of issuance of the UAE Law. It is, therefore, expected that subject executive regulations containing procedural aspects will be issued by 20 March 2022. The controllers and processers are to 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. Accordingly, controllers and processers need to be in compliance with the UAE Law by 20 September 2022, unless the period is extended by the Cabinet.

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 as follows:

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

Data Protection Officer

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

UAE Law

- A 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 adoption of new technologies or due to 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 related to the above.

DIFC Law

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

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 controller or processer which 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 controller or processer consist of processing of large scale of special categories of personal data.

Responsibilities of a DPO

- Monitoring the compliance of controller or processer within the applicable legal framework;
- informing and advising the controller, processer 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 concerned regulator, among other responsibilities.

Consent

The UAE Law provides certain exceptions where processing may be carried out without consent, which include the following:

- processing is necessary for the reasons of public interest;
- processing relates to personal data made publicly available by data subject;
- processing is necessary to initiate or defend proceedings related to claim of rights and legal actions or in relation to judicial or security procedures;
- processing is necessary for the purposes of occupational or preventive medicine to assess working capacity of employee, medical diagnosis, etc, in accordance with the applicable law;
- processing is necessary for 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 data subject;
- processing is necessary for performance of obligations and establish rights related to recruitment or social security in accordance with the applicable law;
- processing is necessary for performance of a contract to which the data subject is a party or for taking actions on 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 subjected to;
- situations specified by the executive regulations.

Whereas, 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 Law provide that a controller protects the privacy by design and by default. The DIFC Law places this requirement on a processer as well.

Data Protection Impact Assessment

Controllers are required to undertake a "data protection impact assessment" before carrying out processing which is likely to result in a high risk to the rights of natural persons. In addition, the DIFC Law places a mandatory requirement for a data protection impact assessment in the following 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 to significantly impact the data subject;
- where processing involves large scale of sensitive personal data.

Data Protection Policy

The UAE Law does not require adoption of any internal or external data protection policy. The DIFC Law and the ADGM Regulations do require

to put in place and implement a data protection policy.

Rights of data subjects

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

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

Anonymisation/pseudonymisation

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

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

Automated decision-making

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

Injury/harm

The UAE Law does not provide for any concept of injury/harm, and compensation thereof, in relation to a grievance to 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 for a compensation. The claim for seeking 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 processer for contravention of any provision of the applicable law/regulations.

2.2 Sectoral and Special Issues

Banking Sector

The 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 that apply to all licensed financial institutions (licensed by the Central Bank of the UAE). These regulations requires that licensed financial institutions are to collect the minimum amount of consumer data and information required in relation to licensed financial institutions activities. The licensed financial institutions, under these regulations, are to:

- establish a function in their respective organisations responsible for data management and protection, maintaining policies, procedures, systems and controls to protect 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 or use of the consumer information;
- notify all significant breaches of consumer data to the UAE Central bank, and to notify (without delay) to the consumer where a breach may have risk to the financial and personal security of the consumer;
- ensure that consumers are able to make informed choices regarding their consent for sharing of their data with third parties and within the licensed financial institution.

Telecom Sector

Telecommunications and Digital Government Regulatory Authority (TDRA) consumer protection regulations require telecommunication service providers to take all reasonable measures to prevent the unauthorised disclosure or unauthorised use of subscriber information. Telecommunication 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) is 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 to be kept confidential and that the same shall not be used for any non-health purpose without obtaining the written approval of the patient, except in following cases:

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

Health information and data, under the Federal Law No 2 of 2019, 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. The health information and data is to 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, means 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 a person's health such as physical, psychological, mental, corporal, genetic or sexual state, including information related to a person's provision of healthcare services revealing 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 Law has a similar definition of special categories of personal data as in the DIFC Law.

The UAE Law states that a personal data protection impact assessment is a necessity where processing involves large scale 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;
- processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or data subject concerning employment;
- processing is necessary to protect vital interests of 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;
- processing is necessary for the establishment, exercise or defence of legal claims;
- 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 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 purpose, including profiling to the extent 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 purpose.

2.4 Workplace Privacy

The Federal Decree Law No 33 of 2021, regarding the regulation of employment relationships, provides that a worker shall keep 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 provide for any provision concerning the role of labour organisations, whistle-blowing 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 his knowledge, may undertake reasonable and necessary inspections or investigations.

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

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

The executive regulations to be issued under the UAE Law will specify the penalties/administrative sanctions to be imposed on 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 up to USD100,000.

The ADGM Regulations provides that the maximum amount of administrative fine must not exceed USD28 million.

No details are available concerning 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 which 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

The Federal Law No 20 of 2018 governs anti-money laundering and combating the financing of terrorism. The supervisory authorities, financial intelligence unit, law enforcement authorities and designated non-financial businesses and professions, under the referred law, 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 exemption, however, is not available in case 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

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

The referred law also provides that all the authorities (concerned with the implementation of the referred law) shall undertake to keep all the information, obtained in connection with the implementation of referred law, as confidential and not to disclose the same 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 to transfer personal data outside the jurisdiction. The situations under which personal data may be transferred outside UAE are discussed at **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 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 regard.

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 which has a law in place covering various aspects as to 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 allows to transfer 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 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 co-operation.
- Transfer is necessary for the protection of public interest.

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;
- an approved certification mechanism.

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

- with the explicit consent of the data subject;
- transfer is necessary for the performance of a contract between data subject and controller;
- transfer is necessary for the conclusion or performance of contract between a controller and a third party which is in the interest of 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 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 open for viewing by the public in general or by a person who can demonstrate a legitimate interest (under DIFC Law only);
- transfer is necessary for compliance with any obligation under applicable law to which a controller is subject to or transfer is made at the reasonable request of a regulator, police or other government agency or competent authority (under 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 DIFC Law only);
- transfer is necessary to comply with applicable anti-money laundering or counter-terrorist financing obligations applicable to a controller or a processer (under DIFC Law only).

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

- transfer is not repeating or part of a repetitive course of transfers;
- transfer concerns only a limited number of data subjects;
- transfer 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;
- 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 respect to the protection of personal data.

4.3 Government Notifications and Approvals

There is no requirement of any government notifications or approvals to transfer data internationally, except the one discussed at **4.4 Data Localisation Requirements**, related to health data.

4.4 Data Localisation Requirements

There is no requirement of data localisation, except health information and data, which – under the Federal Law No 2 of 2019 – 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.

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 UAE.

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

Guidelines for Financial Institutions Adopting Enabling Technologies

The Central Bank of the UAE, Securities and Commodities Authority (SCA), Dubai Financial Services Authority (DFSA) of the DIFC and Financial Services Regulatory Authority (FSRA) of the ADGM have issued Bank Guidelines on the application of the key principles covering the use of:

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

The Bank Guidelines require that all APIs should be designed on a "privacy by design" basis, in a way to only expose relevant data elements to any party in order to fulfil API purpose. The Bank Guidelines further require that financial institutions should ensure that personal data being transmitted or stored in encrypted form to enable privacy and integrity.

Unmanned Aircraft System (UAS/drones)

The General Civil Aviation Authority (GCAA) of the UAE is the regulatory body concerning registration of 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 shall not be permitted without a 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 committee.

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 Other Significant Issues

Federal Decree Law No 46 of 2021, on electronic transactions and trust services (the Electronic Transactions Law), has been come into effect on 2 January 2022 and has repealed the Federal Law No 01 of 2006 on electric commerce and transactions. As regulator, the Telecommunications and Digital Government Regulatory Authority (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 from TDRA to render electronic signatures services.

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.

AUTHORS

Saifullah Khan is an international trade, IT and policy lawyer, has 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 emerging discipline of data privacy, he advises clients from different jurisdictions about data privacy compliance, cross-border transfer of data. Additionally, he assists clients on preparation and review of the 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 from the London School of Economics and Political Science on “Data: Law, Policy and Regulation”.

Saeed Hasan Khan has more than 20 years’ experience in 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 4-5, Suite 408
Al Sarab Tower, Level 15
ADGM Abu Dhabi
United Arab Emirates

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