COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Uae

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

Bizilance Legal Consultants

Saifullah Khan

Partner | saifullah.khan@bizilancelegal.ae

Saeed Hasan Khan

Partner | saeed.hasan@bizilancelegal.ae

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in UAE.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

UAE
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

The United Arab Emirates has the following regulatory framework concerning personal data protection:

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law). The UAE Law is applicable al across the UAE except for a few specified sectors and the free zones. The UAE Law is regulated by the UAE Data Office (the Data Office). The UAE Law is not applicable to following:

- Governmental data
- Governmental authorities which control and process personal data
- Security and judicial authorities
- Banking and credit personal data
- Companies and organizations incorporated in free zones and governed by special personal data protection legislation

Data Protection Law 2020 of the Dubai International Financial Center (the DIFC Law). The DIFC Law is applicable in DIFC. The DIFC Law is regulated by the Commissioner (the Commissioner).

Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations). The ADGM Regulations are applicable in ADGM. The Commissioner of Data Protection (the Commissioner of Data Protection) is responsible to regulate the ADGM Regulations.

Sectoral specific regime concerning personal data protection is as follows:

- Federal Law No. 14 of 2018 (concerning Central Bank of the UAE) governs data protection of banks' customers
- Federal Law No. 3 of 2003 (concerning telecommunication) governs data protection of telecom consumers
- Federal Law No. 2 of 2019 (concerning use of Information and Communication Technology in health fields) governs the confidentiality of patient's information

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

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

The DIFC Law requires that a controller or processer shall register with 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.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The UAE Law

Processing: 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, characterization, disclosure by transmission, dissemination, distribution or otherwise making available, alignment, combination, restriction, erasure, destruction or creation of a model of personal data.

Processer: An establishment or a natural person who processes the personal data on behalf of the controller and under his supervision and instructions.

Controller: 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.

Data Subject: The natural person to whom personal data relates.

Personal Data: 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 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.

Sensitive Personal Data: 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 physical, psychological, mental, corporal, genetic or sexual state, including any information related to such person's provision of healthcare services that reveal his health condition.

Consent: The consent by which the data subject authorizes third parties to process personal data relating to him, provided that such consent is 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.

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, organization, 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.

Processer: Any person who Processes Personal Data on behalf of a Controller.

Controller: Any person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Data Subject: The identified or Identifiable Natural Person to whom Personal Data relates.

Personal Data: Any information referring to an identified or Identifiable Natural Person.

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.

Consent: 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

Processing: 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.

Processor: A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

Controller: 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.

Data Subject: 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.

Personal Data: Any information relating to a Data Subject.

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.

Consent: 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 them.

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The UAE Law

The UAE Law requires that processing of personal data is to take place in accordance with the following rules:

- Fairness, transparency and lawfulness
- Purpose specification
- Adequacy and relevance
- Correct, accurate and update
- Ensure to erase or rectify the incorrect data
- Safety and security
- Not to store the personal data after the end of the purpose (may be maintained if identity of data subject is anonymized)
- Any other controls as may be specified by the executive regulations

The DIFC Law/The ADGM Regulations

The lawful basis under above are:

- Consent
- Necessity for the performance of a contract to which data subject is a party
- Necessity for compliance with applicable law to which controller is subject to
- Necessity to protect vital interests of a data subject or of another natural person
- Necessity for the performance of a task carried out by DIFC body/public authority in the interest of ADGM, or in exercise of powers and functions of DIFC body/ADGM/Financial Services Regulatory Authority/ADGM Courts/Registration Authority, or exercise of powers and functions vested by DIFC body by a third party to whom personal data is disclosed by the DIFC body
- Necessity for the purposes of legitimate interests pursued by a controller or by a third party, except where such interests are overridden by the interests or rights of a data subject

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

The UAE Law

The UAE Law provides that processing of personal data without consent is prohibited. Following are the exceptions where processing may be carried out without consent:

- 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.

The DIFC Law/The ADGM Regulations

Consent is one of the "lawful" bases to process the personal data under above.

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The UAE Law

The UAE Law provides following in relation to consent:

- Controller is able to prove consent of data subject when processing is based on consent
- Consent is to be clear, simple, unambiguous and accessible (whether in written or electronic form)
- Consent must contain the right of data subject to withdraw consent and withdrawal process must be easy
- Data subject, at any time, has the right to withdraw consent

The DIFC Law

The DIFC provides following in relation to consent:

- When processing is based upon consent the controller must be able to demonstrate that consent has been freely given
- Consent must be obtained for each purpose in a manner that is clearly distinguishable in an intelligible and easily accessible form using clear and plain language
- The request for consent for the processing of personal data must be clearly distinguishable from other matters (consents other than for processing of personal data) in an intelligible and easily accessible form using clear and plain language
- Data subject may withdraw the consent at any time
- The controller is to implement appropriate and proportionate measures to assess the ongoing validity of the consent (except for a single discrete incident)
- Controller must be able to demonstrate to the Commissioner that appropriate methods and procedures are employed to manage the recording and withdrawal of consent and that periodic evaluations of the same are conducted
- Data subject be given opportunity to re-affirm or withdraw the consent on a periodic basis (except in case of a single discrete incident)

The ADGM Regulations

The ADGM Regulations provides following in relation to consent:

- When the processing is based upon consent, controller must be able to demonstrate that data subject has consented to the processing
- Silence, pre-ticked boxes or inactivity do not constitute consent
- Data subject to be aware of at least identity of the controller and the intended purposes of processing
- In case where consent is given in the context of a written declaration also containing other

matters the request for consent to process personal data is to be presented in a manner which is clearly distinguishable from other matters in an intelligible and easily accessible form using clear and plain language
- Any part of the written declaration, as aforesaid, which constitutes contravention of the ADGM Regulations will not be binding
- Data subject has the right to withdraw the consent at any time and withdrawal of consent must be as easy as it is to give consent

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

The UAE 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/The ADGM Regulations

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

- 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

8. How do the laws in your jurisdiction address children's personal data or PII?

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

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The UAE Law

The UAE Law is not applicable on data subject who processes data relating to him for personal purposes. The Data Office has the powers to exempt certain establishments which do not process a 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 Law

The DIFC Law is not applicable to the processing of personal data by natural persons in the course of purely personal or household activity that has no connection to a commercial purpose. The DIFC Board of Directors may make regulations to exempt controllers from compliance with the DIFC Law (or any part thereof). Certain provisions of the DIFC Law are not applicable on DIFC bodies. DIFC bodies are DIFC Authority, Dubai Financial Services Authority, DIFC courts and any other person, body, office, registry or tribunal established under DIFC laws or established upon approval of the President of the DIFC that is not revoked by the DIFC Law of by any other DIFC law.

The ADGM Regulations

The ADGM Regulations are not applicable to the processing of personal data by a natural person for the purposes of purely personal or household activity. In addition, the ADGM Regulations are not applicable on the processing of personal data by public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including safeguarding against and the prevention of threats to national security.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The UAE Law

The UAE Law does not specifically mention the concept of "privacy by design" or "privacy by default". However, it requires that controller is to implement appropriate

technical and organizational measures and actions for the protection and security of personal data to ensure that personal data is not subject to breach, corruption, modification or manipulation.

The DIFC Law

The DIFC Law places this requirement both on controller and processer. The requirement under the DIFC Law is that processing is designed to reinforce data protection principles at the time of determining the means for processing and the time of processing, and that personal data that is necessary for each specific purpose is processed and that personal data is not made accessible to an indefinite number of persons without intervention of data subject.

The ADGM Regulations

The ADGM Regulations requires that controller must take appropriate steps to ensure that its systems, business processes and practices are designed taking into account compliance with principles, rights and obligations of the ADGM Regulations. The controller is further to ensure that only that personal data is processed which is necessary for each specific purpose.

The businesses typically meet these requirements by way of documented policies and procedures and monitoring of their implementation.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

The UAE Law

The controller is to maintain the following records:

- Details of controller and the data protection officer
- Description of categories of personal data
- Data related to persons authorized to access personal data
- Timeframe, restrictions and scope of processing
- Erasure, modification or processing mechanism
- Purpose of the processing
- Data related to cross-border transfer and its processing
- Description of technical and organizational actions related to information security and processing

The DIFC Law/The ADGM Regulations

Following written records are required to be kept:

- Name and contact details of controller, joint controller (where applicable) and the data protection officer
- Purpose of processing
- Description of categories of data subjects and of personal data
- Categories of recipients to whom personal data has been or will be disclosed
- Identification of location (third country) or international organization to which personal data is transferred including documents in relation to suitable safeguards
- Time limits for erasure of the different categories of personal data (where possible)
- General description of the technical and organizational measures for security of personal data (where possible)

The businesses typically meet these requirements by way of documented policies and procedures.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The UAE Law

The UAE Law requires that personal data must not be stored after the completion of the purpose of its processing. The UAE Law further provides that personal data may be maintained (after completion of purpose) in case identity of the data subject is concealed through anonymization.

The DIFC Law/The ADGM Regulations

Controller and processer are required to have policy and process to securely and permanently delete, anonymize, pseudonymize, encrypt the personal data or to put it beyond further use when grounds for data retention no longer apply.

13. When are you required to, or when is it recommended that you, consult with data

privacy regulators in your jurisdiction?

The UAE Law

There is no mandatory requirement to consult the regulator under the UAE Law.

The DIFC Law/The ADGM Regulations

A controller is required to consult/notify the Commissioner/Commissioner of Data Protection where data protection impact assessment indicates that processing would have high risks to the rights of the data subject.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

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 UAE 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.

The data protection impact assessment is carried out either internally or on an outsourced basis.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

The requirements for appointment of a data protection officer (DPO) are as under.

The UAE Law

- 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
- 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.

The DIFC Law

- DPO is required to be appointed by the Commissioner, DIFC Authority and by Dubai Financial Services Authority
- 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

The ADGM Regulations

- DPO is required to be appointed where processing is carried out by a public authority except for courts acting in their judicial capacity
- 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
- 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 DPO

The responsibilities of DPO, among others, include:

- 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
- Acting as contact point for the concerned regulator

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There is no requirement for employee training in any of the laws being discussed here.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

The UAE Law

The UAE Law does not have any such requirement.

The DIFC Law/The ADGM Regulations

There is a requirement to provide information to data subject when (i) personal data is obtained from the data subject and when (ii) personal data has not been obtained from the data subject. The information required to be provided to data subject, among others, include:

- Identity and contact details of controller
- Contact details of data protection officer (where applicable)
- Purpose and lawful basis of processing
- Legitimate interest of controller (where applicable)
- Categories of personal data that is being processed
- Categories of recipients of personal data
- Safeguards in case of transfer of personal data to any other jurisdiction or to an international organization
- Period for which personal data will be stored
- Rights of the data subject
- The source from where personal data is obtained (when personal data is not obtained from data subject)

The information is to be provided in writing including, where applicable, by electronic means.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

There is a distinction between controllers and processers as per their given definitions, as explained at question 3.

Both the controllers and processers are required to implement measures in order to protect and secure the personal data. The obligations on the processers stem from the laws and contractual obligations with the controllers.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

The UAE Law

The UAE Law requires that controllers are to appoint processers providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that provisions of the UAE Law could be met. The processer is to process the personal data on instructions from the controller and pursuant to contract between controller and processer. 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 processing by a processer is to be governed by legally binding written agreement between controller and processer. A processer is to provide sufficient assurances/guarantees to implement appropriate technical and organizational measures to ensure that processing meets the legal requirements and to ensure the protection of rights of the data subjects.

The agreement between controller and processer is to contain, among others:

The DIFC Law	The ADGM Regulations
• 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 processer to process personal data based on documented instructions from controller • Ensuring that persons authorised to process relevant personal data are under legally binding written agreements or duties of confidentiality	• Processer is to processes 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 organizational 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

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

The relevant terms are given following definitions:

The UAE Law	The DIFC Law	The ADGM Regulations
Automated Processing: A processing operation which is performed using an electronic system or programme operating in an automated manner, either in a complete autonomous way without any human intervention or partially under a limited human supervisions and intervention.	Automated Processing is not defined.	Automated Processing is not defined.
Profiling: A form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to the data subject, in particular to analyze or predict aspects concerning his financial condition or performance, health, personal preferences, interest, behavior, location, movements or reliability.	Profiling: The automated processing of personal data to evaluate the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.	Profiling: Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

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 personal data processing for direct marketing purpose including profiling to the extent profiling is related to such direct marketing.

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

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

The cross-contextual behavioral advertising is not directly addressed in the laws, except and so far within the context of the right of automated decision making and profiling as discussed above.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or related terms defined and what restrictions are imposed, if any?

The sale of personal information is not addressed in the UAE Law, the DIFC Law and the ADGM Regulations.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

The Telecommunications and Digital Government Regulatory Authority (TDRA) has framed "Regulatory Policy for Spam Electronic Communications" (the Policy). The Policy requires that licensees (of TDRA) are to put all practical measures in place to minimize 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 address harvesting and generation of electronic addresses. A few important terms defined by the Policy are as follows:

"**Address-Harvesting**" means the collecting, capturing, and compiling of an Electronic Address by means of software, tools, technologies or other methods of generating an Electronic Address.

"**Electronic Address**" means a number or alphanumeric string by which a Recipient of an Electronic Communication can be identified and contacted on a particular type of Telecommunications Network, such as an electronic mail address, URL, SIP or a telephone number.

"**Electronic Communications**" means the communications conveyed by means of a Telecommunications Network to an Electronic Address.

"**Spam**" means Marketing Electronic Communications sent to a Recipient without obtaining that Recipient's Consent.

"**Unsolicited Electronic Communications**" means Electronic Communications sent to a Recipient without obtaining that Recipient's Consent.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

Biometric is included within the definition of "sensitive personal data"/ "special categories of personal data" and rules as explained at question 7 are applicable in relation thereto.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

The UAE Law

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 (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 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 DIFC Data Protection Regulations.

The ADGM Regulations

The ADGM Regulations allows to transfer personal data abroad where the Personal Data Commissioner has decided that the receiving jurisdiction ensures an adequate level of protection.

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

- 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 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)
- The 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)

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The UAE Law

The controller and processor are to put in place and implement appropriate technical and organizational 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 processers also under the DIFC Law) are required to implement appropriate technical and organizational measures to protect the 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".

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The term "data breach" is defined as follows.

The UAE Law

A breach of security and personal data through unauthorized 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

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.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The laws do not, as discussed here, provide any sector specific security requirements.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

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 privacy, confidentiality, security, rights of the data subjects. The processer is to notify, without delay, any such breach to the controller (the UAE Law/the DIFC Law and the ADGM Regulations).

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 be accompanied the breach notification.

The breach notification is to contain at least 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)

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The Federal Decree Law No. 34 of 2021 on Countering Rumors and Cybercrimes criminalizes certain acts to be offence punishable with imprisonment and fine.

Following are a few instances which are recognized as crimes (concerning cyber space) under the referred law:

- Hacking including hacking the Government Entities information system
- Causing harm to information system including that of Government Entity and Critical Facility
- Infringement of personal data and information
- Infringement of Government data and information
- Infringement of data of financial, commercial or economic establishments
- Unauthorized acquisition of third party's codes and ciphers
- Circumventing the information network with the intention of committing a crime
- Creating fake emails, websites and electronic accounts
- Illegal interception and disclosure of information
- Collecting and processing personal data and information in violation of the legislation
- Forging E-documents
- Hacking E-payment instruments
- Using electronic systems to commit crimes and to conceal evidence
- Crimes committed by administrator of website or electronic account
- Tampering with digital evidence
- Internet fraud
- Unauthorized fundraising
- Cyberextortion and cyber threats
- Advertisements and promotions misleading the consumers

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The National Electronic Security Authority (NESA), established under the Federal Decree Law No. 3 of 2012, is the UAE Federal Authority responsible for the advancement of cybersecurity.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The individual privacy rights, as below, are exercisable by data subject through submission of a request to data controller:

The UAE Law

Right	Exceptions
Right to access to information	• The request is not related to personal data being processed or is excessively repeated • The request is in contravention of the judicial procedures or investigations carried out by the competent entities • The request has a negative impact on controller's to protect information security • The request relates to privacy and confidentiality of personal data of a third party
Right to data portability	None
Right to rectification or erasure	• If the request relates to erasure of personal data related to public health with private institutions • If the request affects investigations, claim or defence of rights and legal actions in respect of controller • If the request is in conflict with other law to which controller is subject to • Any other cases to be specified by the Executive Regulations
Right to restriction of processing	• Where processing is restricted to storage of personal data • Where processing is necessary to initiate or defend in any procedures relating to claim of rights or judicial actions or judicial proceedings • Where processing is necessary for protection of rights of the third part under any law • Where processing is necessary for the reasons or protection of public interest
Right to stop processing	None
Right to object to automated decision making	• When automated decision making is performed under the terms of contract between data subject and controller • When automated decision making is necessary under any other law of the UAE • When data subject has given his consent
Right to withdraw consent	None

The DIFC Law

Right	Exceptions
Right to withdraw consent	None
Right to access, rectification and erasure	In cases where restriction is a necessary and proportionate measure to: • Avoid obstructing an official or legal inquiry, investigation or procedure • Avoid prejudicing the prevention, detention, investigation or prosecution of criminal offences or the execution of criminal penalties • Protect public security • Protect national security • Protect the rights of others
Right to object processing	• When at the time of collection of personal data from data subject the controller has explicitly stated that it would not be possible to implement an objection to processing
Right to restriction of processing	• For storage of personal data • Processing for establishment, exercise or defence of legal claims • Processing for the protection of rights of another person • Processing for reasons of substantial public interest
Right to data portability	• When data portability would infringe the rights of any other natural person
Right to object to automated decision-making including profiling	• When decision is necessary for entering into or performance of a contract between data subject and controller • When decision making is authorized by applicable law to which controller is subject to and which also provides suitable measures to safeguard the rights of data subject • When decision is based upon explicit consent of data subject

The ADGM Regulations

Rights	Restrictions
Right of access	• Prejudicial to national security, national defence, prevention or detection of crime, apprehension or prosecution of offenders, assessment or collection of a tax or duty or an imposition of similar nature • Request relates to legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights to the extent to prevent controller from complying with the obligations and rights • Likely to prejudice the discharge of public functions designed to protect public interests • Likely to prejudice the proper discharge of public functions designed to secure workers health, safety and welfare etc; or likely to prejudice to regulate preventing, restricting or distorting commercial competition or to regulate undertakings abusing a dominant market position • Likely to prejudice ADGM ability to comply with international obligations • Would require disclosure of information which is prohibited by applicable law • Likely to prejudice audit functions for supervising the quality of public accounting and financial reporting by a public authority • Likely to prejudice regulatory function of a public authority • Likely to prejudice judicial appointments, independence and proceedings including an individual or court acting in a judicial capacity
Right to rectification	
Right to erasure	
Right to restriction of processing	
Right to data portability	
Right to object	
Right not to subject to automated decision-making including profiling	

33. Are individual data privacy rights exercisable through the judicial system or

enforced by a regulator or both?

The UAE Law

A complaint is firstly to be filed with the Data Office. Grievances against any decision of the Data Office is to be filed with the Director General of the Data Office against any decision, administrative sanction or action taken by the Data Office. A decision, administrative sanction or action of the Data Office may not be challenged in appeal unless a grievance is filed with the Director General of the Data Office.

The DIFC Law/the ADGM Regulations

A complaint is firstly to be submitted before the Commissioner/Commissioner of Data Protection. The disputes are heard in appeal before the DIFC Court/ADGM Courts, respectively.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

The UAE Law

A data subject may lodge a complaint with the Data office on the reason of contravention of the provisions of the UAE Law.

The DIFC Law/The ADGM Regulations

A data subject has the right to lodge complaint with the Commissioner/Commissioner of Data Protection on breach/contravention of the DIFC Law/the ADGM Regulations.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

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.

36. How are the laws governing privacy and data protection enforced?

The laws are enforced by the Data Office, Commissioner, Commissioner of Data Protection respectively under the UAE Law, the DIFC Law and the ADGM Regulations.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

The UAE Law	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
The DIFC Law	Maximum fine upto US$ 100,000
The ADGM Regulations	Maximum fine upto US$ 28,000,000

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

The laws, discussed here, do not provide any guidelines regarding the calculation of fines or thresholds for the imposition of sanctions.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

The orders of the regulators are appealable before the court, as stated at question 33.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

No information is available regarding any proposal to reform data protection or cybersecurity laws.

Contributors

Saifullah Khan
Partner
saifullah.khan@bizilancelegal.ae

Saeed Hasan Khan
Partner
saeed.hasan@bizilancelegal.ae