Data Privacy Comparative Guide

Bizilance
Legal Consultants

mondaq
Connecting knowledge & people

Data Privacy Comparative Guide

Article Author(s)

Bizilance Legal Consultants

Saeed Hasan Khan

Saifullah Khan

United Arab Emirates

Contributing Editor

LATHAM & WATKINS LLP

Antony Kim

Contributing Editor

1.Legal and enforcement framework

1. 1. Which legislative and regulatory provisions govern data privacy in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The United Arab Emirates (UAE) has following legal framework to govern data privacy:

- Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law), this law is applicable all across the UAE except for the free zones;
- Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law), this Law is applicable in DIFC; and
- Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), these Regulations are applicable in ADGM.

1. 2. Do any special regimes apply in specific sectors (eg, banking, insurance, telecommunications, healthcare, advertising) or to specific data types (eg, biometric data)?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

Banking: Federal Law No. 14 of 2018 (concerning Central Bank of the UAE) governs data protection of banks' customers;

Telecommunications: Federal Law No. 3 of 2003 (concerning telecommunication) governs data protection of telecom consumers; and

Health: Federal Law No. 2 of 2019 (concerning use of Information and Communication Technology in health fields) governs the confidentiality of patients' information.

Biometric Data: Biometric data is included within the definition of "sensitive personal data" in the UAE Law. Further, the definition of "special categories of personal data" also includes biometric data in case of the DIFC Law and the ADGM Regulations.

The UAE Law, the DIFC Law and the ADGM Regulations have specific provisions governing "sensitive personal data" and "special categories of personal data" as a corollary whereof "biometric data" is also governed specifically.

1. 3. Do any bilateral and multilateral instruments on data privacy have effect in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

None.

1. 4. Which bodies are responsible for enforcing the data privacy legislation in your jurisdiction? What powers do they have?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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

The DIFC Law: The Commissioner (the Commissioner) is to administer the DIFC law. The Commissioner is empowered to receive and decide the complaints concerning contravention of the DIFC law. The Commissioner is also empowered to investigate the complaints and to issue direction or declaration on the complaints and to impose fines.

The ADGM Regulations: The Commissioner of Data Protection (the Commissioner of Data Protection) is responsible for enforcement of the ADGM Regulations. The Commissioner of Data Protection is empowered to receive and decide the complaints regarding contravention of the ADGM Regulations and to impose fines.

1. 5. What role do industry standards or best practices play in terms of compliance and regulatory enforcement?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law, the DIFC Law and the ADGM Regulations largely follow the underlying principles as of the General Data Protection Regulation (GDPR) of the European Union. The best practices being followed by the data controllers/data processors in the European Union (with reference to GDPR) would play an important role for the compliance and enforcement purposes, as data privacy regulatory regime in the UAE is largely based upon GDPR principles.

2.Scope of application

2. 1. Which entities are captured by the data privacy regime in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law, the DIFC Law and the ADGM Regulations are applicable on the “data controllers/data processers” carrying out personal data processing in their respective jurisdictions. As such these laws are not entity specific, unless exempted specifically as explained at 2.2.

2. 2. What exemptions from the data privacy regime, if any, are available in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law: The UAE Law is not applicable to following:

- Governmental data
- Government authorities which control and process personal data
- Security and judicial authorities
- Data subject processing data related to him for personal purposes
- Health personal data
- Banking and credit personal data
- Companies and organizations incorporated in free zones

Apart from above, 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 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.

2. 3. Does the data privacy regime have extra-territorial application?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law: The UAE Law is applicable to:

- A data controller or processer established in the UAE that carries personal data processing for data subjects who are outside the UAE.
- A controller or processer not established in the UAE that carries personal data processing of data subjects who are in the UAE.

The DIFC Law: The DIFC Law is applicable to a controller or processer, regardless of its place or incorporation, who processes personal data in DIFC.

The ADGM Regulations: The ADGM Regulations are applicable in the context of activities of an establishment of a controller or processers in ADGM, regardless of whether the processing takes place in ADGM or not.

3.Definitions

3. 1. How are the following terms (or equivalents) defined in your jurisdiction? (a) Data processing; (b) Data processor; (c) Data controller; (d) Data subject; (e) Personal data; (f) Sensitive personal data; and (g) Consent.

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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.

3. 2. What other key terms are relevant in the data privacy context in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

Data Breach (the UAE Law/the ADGM Regulations): 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.

Personal Data Breach (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.

4.Registration

4. 1. Is registration of data controllers and processors mandatory in your jurisdiction? What are the consequences of failure to register?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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.

4. 2. What is the process for registration?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The controller or processer is to register with the Commissioner by filing a notification of processing operations. The said notification is required to be kept up to date through amended notifications (the DIFC Law). The said notification is to be accompanied by a fee as may be prescribed by the regulations made by the DIFC Authority Board of Directors.

4. 3. Is registered information publicly accessible?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The notifications, under the DIFC Law as aforesaid, are to be kept on a publicly available register maintained by the Commissioner.

5.Data processing

5. 1. What lawful bases for processing personal data are recognised in your jurisdiction? Do these vary depending on the type of data being processed?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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 bases 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. 2. What key principles apply (eg, notice) when processing personal data in your jurisdiction? Do these vary depending on the type of data being processed? Or on whether it is outsourced?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law has no requirement of notice and the key principles are those as mentioned at 5.1.

The key principles under the DIFC Law and the ADGM Regulations include:

- Lawfulness, fairness and transparency
- Specified, explicit and legitimate purpose
- Adequacy and relevancy
- Accuracy and up to date
- Kept in a form that permits identification of data subject for no longer than is necessary for the purposes for which data is processed
- Security of the personal data

The DIFC Law and the ADGM Regulations requires a controller to provide information to the data subject when personal data is being collected from the data subject and when personal data has not been obtained from the data subject. The information, among others, to be provided includes:

- Identity and contact details of the controller
- Contact details of the Data Protection Officer (where applicable)
- Purpose of the processing and legal basis thereof

5. 3. What other requirements, restrictions and best practices should be considered when processing personal data in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

Apart from above, such procedures and processes may be deployed that facilitates a data subject to make an informed decision to share the personal data and to easily know the matters ancillary to the collection of personal data by controller.

6.Data transfers

6. 1. What requirements and restrictions apply to the transfer of data to third parties?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law, the DIFC Law and the ADGM Regulations requires that personal data must be processed so as to ensure that personal data is protected against unauthorized processing. It follows that transfer of personal data to third parties may be governed by means of a binding agreement ensuring security and confidentiality of the transferred personal data.

6. 2. What requirements and restrictions apply to the transfer of data abroad? Do these vary depending on the destination?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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)

6. 3. What other requirements, restrictions and best practices should be considered when transferring personal data, both within your jurisdiction and abroad?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The regulatory framework, as aforesaid, provides adequate requirements and restrictions to protect the data transfer based upon best practices, giving no room for any further considerations.

7.Rights of data subjects

7. 1. What rights do data subjects enjoy with regard to the processing of their personal data? Do any exemptions apply?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The data subjects have following rights under the UAE Law, the DIFC Law and the ADGM Regulations:

- Right to 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

Exemptions/Restrictions

The UAE Law

In the context of "right to access", the data controller has a right to reject the request in following cases:

- The request is not related to information that is subject to access under the UAE Law 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 endeavours to protect information security.
- The request relates to the privacy and confidentiality of personal data of a third party.

In the context of "right to erasure", the data subject shall not have the right to request for erasure in the following cases:

- The request relates to erasure of personal data relating to public health with private institutions.
- The request affects investigations, claim or defence of rights and legal actions in respect of controller.
- The request is in conflict with other laws to which controller is subject to.
- Other cases to be specified by the Executive Regulations.

The DIFC Law

In the context of "right to access", a controller may restrict, wholly or partly, the provision of information to the data subject if the restriction is necessary and proportionate measure to:

- Avoid obstructing an official or legal inquiry, investigations or procedure
- Avoid prejudicing the prevention, detection, investigation or prosecution or criminal offences or the execution of criminal penalties
- Protect public security
- Protect national security
- Protect rights of others.

In the context of "right of erasure", the controller is only required to erase personal data in following cases:

- The erasure request is specified under the DIFC Law.
- The controller is not required to retain the personal data in accordance with law applicable to controller or for establishment or defence of legal claims.

Where erasure is not feasible for technical reasons then the controller is not in violation of the DIFC Law.

The ADGM Regulations

The restrictions, to rights of data subjects, under the ADGM Regulations (among others) include:

- When such rights are likely to prejudice to national security, national defence, prevention or detection of crime, apprehension or prosecution of offenders, or the assessment or collection of tax or duty or an imposition of similar nature.
- When the right relates to information required to be disclosed by applicable law (including by court order) or in connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.
- When providing the rights would be likely to prejudice the discharge of public functions.

7. 2. How can data subjects seek to exercise their rights in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law

The controller is to provide clear and appropriate means and mechanisms enabling the data subjects to communicate and request the exercise of rights provided under the UAE Law.

The DIFC Law

- The controller is required to make available at least two methods (including but not limited to post, telephone, email or an online form) which must not be onerous.
- Where a controller maintains a website, at least one method of contact must be available free of cost through website and without any requirement to create an account of any sort.

The ADGM Regulations

There is no specific mention about the means and methods for the data subjects to exercise their rights.

7. 3. What remedies are available to data subjects in case of breach of their rights?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The data subjects have the right to lodge a complaint with the Data Office, the Commissioner and the Commissioner of Data Protection respectively under the UAE Law, the DIFC Law and the ADGM Regulations.

8.Compliance

8. 1. Is the appointment of a data protection officer mandatory in your jurisdiction? If so, what are the consequences of failure to do so?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law

- Data Protection officer (DPO) is required to be appointed when the processing is likely to result in a high risk to the privacy and confidentiality of personal data due to 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
- DPO is required to be appointed where the processing involves a large scale of sensitive personal data

The UAE Cabinet is to issue a decision specifying the acts that constitute contravention of the UAE Law and related administrative sanctions to be imposed in relation thereto.

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 failure to appoint DPO entails a maximum fine of US$ 50,000.

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

The failure to appoint DPO entails imposition of a fine, as determined by the Commissioner of Data Protection, not exceeding US$ 28 Million.

8. 2. What qualifications or other criteria must the data protection officer meet?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law provides that a DPO is to have adequate skills and knowledge to protect personal data.

The DIFC Law requires that a DPO must have knowledge of the DIFC Law and its requirements.

The ADGM Regulations requires that a DPO must be appointed on the basis of professional qualities and in particular having expert knowledge of data protection law and practices.

8. 3. What are the key responsibilities of the data protection officer?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The key responsibilities of a DPO, under the UAE Law, the DIFC Law and the ADGM Regulations, include:

- To monitor the compliance of controller or processer with applicable legal framework
- To inform and advise controller, processer and their respective employees (who carry out personal data processing) about their obligations under the applicable legal framework
- Act as contact point for the concerned regulator

8. 4. Can the role of the data protection officer be outsourced in your jurisdiction? If so, what requirements, restrictions and best practices should be considered in this regard?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The role of DPO may be outsourced, under the UAE Law, the DIFC Law and the ADGM Regulations. The outsourced role of DPO is to be governed on the basis of a well-defined service contract.

8. 5. What record-keeping and documentation requirements apply in the data privacy context?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law

The controller is required to maintain record of personal data processed, containing:

- Details of controller and DPO
- Description of categories of personal data
- Persons authorized to access personal data
- Timeframe, restrictions and scope of processing
- Erasure, modification or processing mechanism
- Purpose of processing
- Data related to cross-border transfer and processing of transferred data
- Description of technical and organizational actions relating to information security

The DIFC Law/the ADGM Regulations

- Names and contract details of controller, DPO and joint controller (where applicable)
- Purpose of processing
- Description of categories of data subjects and of personal data
- Categories of recipients to who, personal data has been or will be disclosed including recipients in third countries and international organizations
- Identification of third country or international organizations where personal data is transferred (where applicable)
- Time limits for erasure of different categories of personal data (where possible)
- General description of the technical and organizational security measures to protect the personal data

8. 6. What other requirements, restrictions and best practices should be considered from a compliance perspective in the data privacy context?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The controllers and processers may put in place appropriate documented policies and procedures in order to remain compliant with the applicable legal requirements and to monitor their observance of the legal requirements.

9.Data security and data breaches

9. 1. What obligations apply to data controllers and processors to preserve the security of personal data?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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 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".

9. 2. Must data breaches be notified to the regulator? If so, what information must be provided and what is the process for doing so? If not, under what circumstances is voluntary notification of a data breach expected?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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 Law).

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)

9. 3. Must data breaches be notified to the affected data subjects? If so, what information must be provided and what is the process for doing so? If not, under what circumstances is voluntary notification of a data breach expected?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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 (the UAE Law/the DIFC Law and the ADGM Law).

9. 4. What other requirements, restrictions and best practices should be considered in the event of a data breach?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The controllers and processers may put in place a mechanism for an early detection of a security breach and measures to mitigate the consequences of the any breach.

10.Employment issues

10. 1. What requirements and restrictions apply to the personal data of employees in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law

The personal data of employees may be processed without consent in following cases:

- The processing is required for the controller or processor to perform its obligations and establish its rights prescribed by law concerning recruitment.
- The processing is necessary for the purposes of occupational or preventive medicine to assess working capacity of an employee in accordance with the relevant law in the UAE.

The DIFC Law/the ADGM Regulations

Processing of special categories of personal data is allowed when processing is necessary for the purposes of carrying out obligations and exercising specific rights of controller or data subject in the context of data subject's employment.

10. 2. Is the surveillance of employees allowed in your jurisdiction? What requirements and restrictions apply in this regard?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law, the DIFC Law and the ADGM Regulations do not contain any provision with respect to surveillance of employees.

10. 3. What other requirements, restrictions and best practices should be considered from an employment perspective in the data privacy context

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The Controllers may have a documented policy concerning processing of personal data of their employees. In addition, the employees may be well trained about their organizational culture and policies & procedures concerning personal data protection.

11.Online issues

11. 1. What requirements and restrictions apply to the use of cookies in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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.

11. 2. What requirements and restrictions apply to cloud computing services in your jurisdiction from a data privacy perspective?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

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 the “Guidelines for Financial Institutions adopting Enabling Technologies” (the Guidelines).

The Guidelines provide guidance, to the financial institutions, on the application of the key principles covering the use of cloud computing. The Guidelines requires that all Application Programming Interface (APIs) should be designed on a “Privacy by Design” concept, in a way to only expose relevant data elements to any party in order to fulfil API purpose. The Guidelines further requires that financial institutions should ensure that personal data being transmitted or stored is encrypted to enable privacy and integrity.

11. 3. What other requirements, restrictions and best practices should be considered from a marketing perspective in the online and networked context?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The controllers may provide appropriate means to the data subjects to exercise their choices in a free and informed way with respect to use of cookies and online marketing.

12.Disputes

12. 1. In which forums are data privacy disputes typically heard in your jurisdiction?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law

A grievance is first 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

The disputes are heard in appeal before the DIFC Court/ADGM Courts, respectively.

12. 2. What issues do such disputes typically involve? How are they typically resolved?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

No details are available about the issues in disputes and their resolution.

12. 3. Have there been any recent cases of note?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

No details are available.

13.Trends and predictions

13. 1. How would you describe the current data privacy landscape and prevailing trends in your jurisdiction? Are any new developments anticipated in the next 12 months, including any proposed legislative reforms?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The UAE Law was issued on September 20, 2021 and has come into effect on January 02, 2022. The Executive Regulations of the UAE Law are to be issued which will have detail procedural aspects of the UAE Law. The Executive Regulations are to be issued by March 20, 2022 by the UAE Cabinet. Within six months of issuance of said Executive Regulations the UAE Law will be implemented, unless the UAE Cabinet extends the referred period of six months.

14.Tips and traps

14. 1. What are your top tips for effective data protection in your jurisdiction and what potential sticking points would you highlight?

United Arab Emirates
BIZILANCE LEGAL CONSULTANTS ADGM ABU DHABI

The data privacy regime in the UAE is not very old. In particular, the UAE Law has just come into effect in January 2022 and will be implemented by September 20, 2022. Therefore, at this point in time there is a need to develop an effective and efficient awareness campaign for the natural persons who are the centre point of data privacy legislations.

Secondly, the controllers and processers need to develop and upgrade their capacity and business processes in order to efficiently comply with their respective obligations.

mondaq

Connecting knowledge & people

Bristol | Essex | New York | Sydney

t: +44 (0) 20 8544 8300
e: enquiries@mondaq.com