DATA PROTECTION & PRIVACY

United Arab Emirates

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

United Arab Emirates

Saifullah Khan
saifullah.khan@bizilancelegal.ae
Bizilance Legal Consultants

Saeed Hasan Khan
saeed.hasan@bizilancelegal.ae
Bizilance Legal Consultants

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The following laws and regulations make up the legal framework that governs data privacy in the United Arab Emirates (UAE):

- Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law): this law is applicable across the UAE, except for in free zones, which have their own legislation on personal data protection;
- Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law): this law is applicable in the DIFC (the DIFC is a free zone); and
- the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations): these regulations are applicable in the ADGM (the ADGM is also a free zone).

The above laws largely follow the EU General Data Protection Regulation.

Law stated - 09 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The UAE Law

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

The DIFC Law

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

The ADGM Regulations

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

Law stated - 09 May 2023

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Data Office is competent to propose joining or signing international conventions and agreements and to propose partnership agreements with the Gulf, regional and international states, organisations and bodies with respect to the activities and competencies of the Data Office. This is done in coordination with the Ministry of Foreign Affairs and International Cooperation.

The DIFC Commissioner and the ADGM Commissioner are empowered to participate in and cooperate with other data protection authorities.

Law stated - 09 May 2023

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches are brought before the concerned authority (the Data Office, the DIFC Commissioner or the ADGM Commissioner, as the case may be), which is empowered to levy fines. Orders and directions of the respective authority are appealable before the concerned courts.

Law stated - 09 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

The UAE Law

A complaint must first be filed with the Data Office. Grievances against any decision, administrative sanction or action of the Data Office must be filed with the Director General of the Data Office. A decision, administrative sanction or action of the Data Office may not be appealed unless a grievance is filed with the Director General of the Data Office.

The DIFC Law and the ADGM Regulations

A complaint must first be submitted to the DIFC Commissioner or the ADGM Commissioner. The disputes are heard on appeal before the DIFC courts or the ADGM courts, respectively.

Law stated - 09 May 2023

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) is not applicable to the following:

- government data;
- government authorities that control and process personal data;
- security and judicial authorities;
- data subjects processing data related to them for personal purposes;
- personal health data;
- personal banking and credit data; and
- companies and organisations incorporated in free zones.

Except the above, the UAE Data Office (the Data Office) has the power to exempt certain establishments that do not process a large volume of personal data from any or all requirements of the UAE Law, in accordance with the standards and controls to be specified by executive regulations.

The DIFC Law

The Data Protection Law 2020 of the Dubai International Financial Centre (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 to DIFC bodies. DIFC bodies are the DIFC Authority, the Dubai Financial Services Authority, the DIFC courts and any other person, body, office, registry or tribunal established under DIFC law 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 Data Protection Regulations 2021 of the Abu Dhabi Global Market (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 to 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.

Law stated - 09 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The data protection laws do not cover the interception of communications or surveillance. However, they provide a right to the data subjects to not to be subjected to automated decision-making, including profiling in the context of electronic marketing.

Law stated - 09 May 2023

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The sector-specific framework concerning protection of personal data covers:

- banking: Federal Law No. 14 of 2018 (concerning the Central Bank of the UAE) governs data protection for bank customers;
- telecommunications: Federal Law No. 3 of 2003 (concerning telecommunications) governs data protection for telecom consumers; and
- health: Federal Law No. 2 of 2019 (concerning use of information and communication technology in health fields) governs the confidentiality of patient information.

Law stated - 09 May 2023

PI formats

What categories and types of PI are covered by the law?

The data protection laws are applicable to the processing of personal data irrespective of processing by automated means or otherwise.

Law stated - 09 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The laws have an extraterritorial effect as follows:

- The UAE Law is applicable to:
  - a data controller or processor established in the UAE that carries out personal data processing for data subjects who are outside the UAE; and
  - a controller or processor not established in the UAE that carries out the personal data processing of data subjects who are in the UAE.
- The DIFC Law is applicable to a controller or processor, regardless of its place of incorporation, that processes personal data in the DIFC.
- The ADGM Regulations are applicable in the context of activities for the establishment of a controller or processor in the ADGM, regardless of whether the processing takes place in the ADGM.

Law stated - 09 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Processing by the controller or the processor is covered under data protection laws. The data protection laws provide for the responsibilities of the controllers and the processors.

Law stated - 09 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) prohibits the processing of personal data without the consent of the data subject (certain exceptions apply). Processing must:

- be fair, transparent and lawful;
- be carried out for the purpose specified;
- be adequate and relevant;
- be correct, accurate and up to date;
- ensure erasure or rectification of incorrect data;
- be safe and secure;
- not store the personal data after the completion of the purpose for which it was collected (it may be maintained if the identity of the data subject is anonymised); and
- be in accordance with any other controls as may be specified by executive regulations.

The DIFC Law and the ADGM Regulations

Data may be collected lawfully:

- with the consent of the data subject;
- when necessary for the performance of a contract to which the data subject is a party;
- when necessary for compliance with the applicable law to which the controller is subject;
- when necessary to protect the vital interests of a data subject or another natural person;
- when necessary:
  - for the performance of a task carried out by a Dubai International Financial Centre (DIFC) body or public authority in the interest of the Abu Dhabi Global Market (ADGM);
  - in the exercise of powers and functions of a DIFC body, the ADGM, the Financial Services Regulatory Authority, the ADGM courts and the Registration Authority; or
  - in exercise of powers and functions vested by a DIFC body by a third party to whom personal data is disclosed by the DIFC body; and
- when necessary for the purposes of legitimate interests pursued by a controller or a third party, except where these interests are overridden by the interests or rights of a data subject.

Law stated - 09 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

'Sensitive personal data', under the UAE Law, means any information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, criminal record, biometric data, or any data related to a person's physical, psychological, mental, corporal, genetic or sexual health, including information related to a person's healthcare that reveals their health conditions.

'Special categories of personal data', under the DIFC Law, means personal data revealing or connecting (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade union membership and health or sex life, including genetic and biometric data where it is used for the purpose of uniquely identifying a natural person.

The Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) have a similar definition of special categories of personal data as the Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law).

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

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

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

Law stated - 09 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) requires that the following information be provided to data subjects by controllers before processing personal data:

- purpose of the processing;
- target sectors or enterprises with whom personal data is to be shared (within and outside the UAE); and
- safeguards put in place for cross-border transfer of personal data.

The DIFC Law and the ADGM Regulations

In the Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) there is a requirement to provide information to the data subject when personal data is obtained from them and when personal data has not been obtained from them. The information required to be provided to the data subject includes:

- the identity and contact details of the controller;
- the contact details of the data protection officer (where applicable);
- the purpose and lawful basis of processing;
- the legitimate interest of the controller (where applicable);
- the types of personal data that are being processed;
- the categories of the recipients of the personal data;
- safeguards in the case of the transfer of personal data to any other jurisdiction or to an international organisation;
- the period for which the personal data will be stored;
- the rights of the data subject; and
- the source the personal data is obtained from (when personal data is not obtained from the data subject).

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

Law stated - 09 May 2023

Exemptions from transparency obligations

When is notice not required?

Information the data subject already has need not be provided when personal data is obtained by the data subject.

When personal data is not obtained by the data subject, the information providing provision is not applicable in the following cases:

- the data subject already has the information;
- the provision of information proves impossible or would involve a disproportionate effort;
- where disclosure is expressly required by applicable law; and
- where personal data must remain confidential subject to the obligation of professional secrecy or the duty of confidentiality in accordance with applicable law.

Law stated - 09 May 2023

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

The data protection laws require that personal data is kept accurate and up to date.

Law stated - 09 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The data protection laws require that personal data is relevant and limited to what is necessary for the purpose for which it is being processed.

Law stated - 09 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The UAE Law

The UAE Law requires that personal data not be stored after the completion of the purpose of its processing. The UAE Law further provides that personal data may be maintained (after the completion of the purpose for which it was gathered) if the identity of the data subject is concealed through anonymisation.

The DIFC Law and the ADGM Regulations

The controller and the processor are required to have policies and processes to securely and permanently delete, anonymise, pseudonymise and encrypt personal data or prevent it from being used further when grounds for data retention no longer apply.

Law stated - 09 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The data protection laws provide that personal data must be processed for a clear, specified, explicit and legitimate purpose. The processing must not be incompatible with the stated purposes.

Law stated - 09 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

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

Law stated - 09 May 2023

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

According to Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law), the controller and processor must put in place and implement appropriate technical and organisational measures and actions to ensure a high level of security that is appropriate to the risks associated with the processing. These measures must be in accordance with the best international standards and practices.

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), the controllers (and processors, where applicable) are required to implement appropriate technical and organisational measures to protect the personal data. In addition, controllers are required to ensure the security of personal data by following the principles of data protection by design and data protection by default.

Law stated - 09 May 2023

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The data controller is required to notify a data breach to the UAE Data Office (the Data Office), the Commissioner of Data Protection for the DIFC (the DIFC Commissioner) and the Commissioner of Data Protection for the ADGM (the ADGM Commissioner) when the breach is likely to result in a risk to the privacy, confidentiality, security or rights of the data subjects. The processor must notify, without delay, any such breach to the controller.

The UAE Law requires immediate notification of the breach. The DIFC Law requires notification of the breach as soon as practicable in the circumstances. The ADGM Regulations require that breach notification be made within 72 hours of having become aware of the breach, and, if notification is not made within 72 hours, then the reasons for delay must also accompany the breach notification.

The breach notification must contain at least the following information:

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

Where a breach is likely to result in a high risk to the security or rights of a data subject, the controller is also required to notify the breach to the data subject.

Law stated - 09 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

According to Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law), the controller and processor must put in place and implement appropriate technical and organisational measures and actions to ensure a high level of security that is appropriate to the risks associated with the processing. These measures must be in accordance with the best international standards and practices.

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), the controllers (and processors, where applicable) are required to implement appropriate technical and organisational measures to protect the personal data. In addition, controllers are required to ensure the security of personal data by following the principles of data protection by design and data protection by default.

Law stated - 09 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

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

The UAE Law

A DPO must be appointed when processing is likely to result in a high risk to the privacy and confidentiality of personal data, owing to the adoption of new technologies or the amount of data. In addition, a DPO must be appointed where the processing involves a systematic and overall assessment of sensitive personal data, including profiling and automated processing

The executive regulations will specify the kinds of technologies and standards of determination of the amount of data related to the above.

The DIFC Law

A DPO must be appointed by the Commissioner of Data Protection for the DIFC (the DIFC Commissioner), the DIFC Authority and the Dubai Financial Services Authority. Further, a DPO must be appointed by a controller or processor performing high-risk activities on a systematic or regular basis. A controller or processor may be required to designate a DPO by the DIFC Commissioner.

The ADGM Regulations

A DPO is required to be appointed where:

- the processing is carried out by a public authority (excluding courts acting in their judicial capacity);
- the core activities of a controller or processor require (on the basis of the nature, scope and purposes of processing) regular and systematic monitoring of data subjects on a large scale; and
- the core activities of a controller or processor consist of the processing of a large number of special categories of personal data.

Responsibilities of DPO

The responsibilities of a DPO include:

- monitoring the compliance of the controller or processor within the applicable legal framework;
- informing and advising the controller and processor and their respective employees (who carry out personal data processing) of their obligations under the applicable legal framework; and
- acting as a contact point for the concerned regulator.

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

Law stated - 09 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The UAE Law

The controller must maintain the following records:

- details of the controller and the data protection officer;
- a description of categories of personal data;
- data related to persons authorised to access personal data;
- the time frame, restrictions and scope of processing;
- the erasure, modification and processing mechanisms;
- the purpose of the processing;
- data related to cross-border transfer and its processing; and
- a description of technical and organisational actions related to information security and processing.

The DIFC Law and the ADGM Regulations

The following written records must be kept:

- the name and contact details of the controller, joint controller (where applicable) and data protection officer;
- the purpose of the processing;
- a description of categories of data subjects and personal data;

- categories of recipients to whom personal data has been or will be disclosed;
- details of locations (third country) or international organisations to which personal data is transferred, including documents in relation to suitable safeguards;
- time limits for the erasure of the different categories of personal data (where possible); and
- a general description of the technical and organisational measures for the security of personal data (where possible).

Law stated - 09 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Controllers are required to undertake a data protection impact assessment before carrying out processing that is likely to result in a high risk to the rights of natural persons. In addition, the 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 that is based on automated processing (including profiling) and has legal effects that will significantly impact the data subject; and
- where processing involves a large volume of sensitive personal data.

Law stated - 09 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The UAE Law

The UAE Law does not specifically mention the concept of privacy by design or privacy by default. However, it requires that a controller implements appropriate technical and organisational 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 requirement under the DIFC Law is that processing must be designed to reinforce data protection principles at the time of determining the means for processing and the time of processing, that personal data that is necessary for each specific purpose must be processed and that personal data must not made accessible to an indefinite number of persons without intervention of the data subject.

The ADGM Regulations

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

Law stated - 09 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement for the registration of controllers or processors under Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law).

Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) requires that a controller or processor register with the Commissioner of Data Protection for the DIFC (the DIFC Commissioner). The DIFC Law requires that a controller or a processor notify the DIFC Commissioner of the following processing operations:

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

The registration process is online and must be renewed annually. The maximum fine under the DIFC Law for failure to register or notify is US$25,000.

The ADGM Regulations require that a controller pay a data protection fee and provide (to the Commissioner of Data Protection for the ADGM) its name and address and the date it commenced processing personal data. The ADGM Regulations do not provide for a specific sanction or fine for failure to register or notify. The registration process is online and must be renewed annually. The maximum general administrative fine is up to US$28 million for committing a prohibited act or omitting to carry out an act.

Law stated - 09 May 2023

Other transparency duties

Are there any other public transparency duties?

No further duties are applicable.

Law stated - 09 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The UAE Law

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) requires that controllers appoint processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a

manner that provisions of the UAE Law could be met. The processor must process the personal data on instruction from the controller and pursuant to the contract between the controller and the processor. This contract must identify the scope, subject, purpose, nature and type of personal data and the categories of the data subject.

The DIFC Law and the ADGM Regulations

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) and the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations), processing by a processor is governed by a legally binding written agreement between the controller and the processor. A processor must provide sufficient assurances and guarantees that it will implement appropriate technical and organisational measures to ensure that processing meets the legal requirements and to ensure the protection of rights of the data subjects.

According to the DIFC Law, the agreement between the controller and the processor must contain, among other things:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects;
- the obligations and rights of the controller;
- commitment by the processor to process personal data based on documented instructions from the controller; and
- assurance that persons authorised to process relevant personal data are under legally binding written agreements or duties of confidentiality.

According to the ADGM Regulations, the agreement between the controller and the processor must contain, among other things:

- that the processor is to process the personal data only on documented instructions from the controller;
- assurance that persons authorised to process personal data have committed themselves to confidentiality;
- taking into account the nature of the processing, assistance to the controller through appropriate technical and organisational measures; and
- at the choice of the controller, that all personal data will be deleted or returned to the controller after the provision of services.

Law stated - 09 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The UAE Law does not have any specific provisions related to the sharing of personal data.

The DIFC Law and the ADGM Regulations

When a controller or processor receives a request from a public authority for the disclosure of personal data, the controller or processor should:

- exercise reasonable caution and diligence to determine the validity and proportionately of the request;
- assess the impact of the data transfer; and
- obtain appropriate assurance from the public authority (where reasonably practicable) that it will respect the rights of the data subjects.

Law stated - 09 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The UAE Law

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

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

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

The DIFC Law

The DIFC Law provides that personal data may be transferred abroad if there is an adequate level of protection in the foreign country, as determined by the Commissioner of Data Protection for the DIFC. There is a list of adequate jurisdictions in the DIFC Data Protection Regulations.

The ADGM Regulations

The ADGM Regulations allow the transfer of personal data abroad where the Personal Data Commissioner has decided that the receiving jurisdiction ensures an adequate level of protection. A list of jurisdictions designated as having an adequate level of protection is available on the website of the ADGM Office of Data 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 if there are appropriate safeguards in place. Appropriate safeguards include:

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

Specific derogations – the DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection and appropriate safeguards, the data may be transferred outside of the UAE when the transfer:

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

Law stated - 09 May 2023

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Transfers outside the UAE to service providers are subject to the same restrictions as those not made to service providers.

Law stated - 09 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no requirement for data localisation, except in relation to health information and data, which – under Federal Law No. 2 of 2019 – may not be stored, processed, generated or transferred outside the UAE, except on a decision issued by the Health Authority in coordination with the Ministry of Health and Prevention.

Law stated - 09 May 2023

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Data subjects have the right to access their personal data.

The UAE Law

The controller must provide clear and appropriate means and mechanisms enabling the data subjects to communicate and request to exercise their rights provided under Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law).

The data controller has a right to reject the request in the 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 judicial procedures or investigations carried out by the competent entities;
- the request has a negative impact on a controller's endeavours to protect information security; and
- the request relates to the privacy and confidentiality of personal data of a third party.

The DIFC Law

According to Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law), the controller is required to make available at least two methods to access personal data (including, but not limited to, post, telephone, email or an online form), which must not be onerous to do. Where a controller maintains a website, at least one form of contact must be available free of charge through the website and without any requirement to create an account of any sort.

A controller may restrict, wholly or partly, the provision of information to the data subject if the restriction is a necessary and proportionate measure to:

- avoid obstructing an official or legal inquiry, investigation 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; or

- protect the rights of others.

The ADGM Regulations

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

Restrictions to the rights of data subjects under the Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) (among others) include:

- when such rights are likely to influence national security, national defence, the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of tax or duties, or an imposition of a 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; and
- when providing the rights would be likely under the discharge of public functions.

Law stated - 09 May 2023

Other rights

Do individuals have other substantive rights?

The data subjects have the following further rights:

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

Law stated - 09 May 2023

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The UAE Law does not provide for any concept of compensation in relation to a grievance of a data subject.

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 and regulations, is entitled to compensation. The claim for seeking compensation must be brought before the court. Compensation must not limit or affect any fine to be imposed on a controller or a processor for contravention of any provision of the applicable law and regulations.

Law stated - 09 May 2023

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The UAE Law

A complaint must first be filed with the UAE Data Office (the Data Office). Grievances against any decision, administrative sanction or action taken by the Data Office must be filed with the Director General of the Data Office. A decision, administrative sanction or action of the Data Office may not be challenged on appeal unless a grievance is filed with the Director General of the Data Office.

The DIFC Law and the ADGM Regulations

A complaint must first be submitted before the Commissioner of Data Protection for the DIFC or the Commissioner of Data Protection for the ADGM. Disputes are heard in appeal before the DIFC courts and ADGM courts, respectively.

Law stated - 09 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

No other derogations, exclusions or exemptions apply.

Law stated - 09 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (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 this direct marketing.

Data Protection Law 2020 of the Dubai International Financial Centre (the DIFC Law) provides that a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and that the data subject must be expressly offered the right to object to direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling, to the extent profiling is related to this direct marketing.

The Data Protection Regulations 2021 of the Abu Dhabi Global Market (the ADGM Regulations) carry the same provisions as the DIFC Law regarding direct marketing. The ADGM Regulations, in addition, provide that when a data subject objects to direct marketing, personal data must not be processed for direct marketing purposes.

Law stated - 09 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

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

Law stated - 09 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

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 this direct marketing.

The DIFC Law provides that a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and that the data subject must be expressly offered the right to object to direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling, to the extent profiling is related to this direct marketing.

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

Law stated - 09 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

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

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

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

Law stated - 09 May 2023

Profiling

Are there any rules regarding individual profiling?

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 this direct marketing.

The DIFC Law provides that a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and that the data subject must be expressly offered the right to object to direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling, to the extent profiling is related to this direct marketing.

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

Law stated - 09 May 2023

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The Central Bank of the UAE, the Securities and Commodities Authority, the Dubai Financial Services Authority of the DIFC and the Financial Services Regulatory Authority of the ADGM have issued the Guidelines for Financial Institutions adopting Enabling Technologies (the Guidelines).

The Guidelines provide guidance to financial institutions on the application of the key principles covering the use of cloud computing. The Guidelines require that all application programming interfaces (APIs) be designed based on the privacy-by-design concept, to only expose relevant data elements to any party to fulfil the API purpose. The Guidelines further require that financial institutions ensure that personal data being transmitted or stored is encrypted to enable privacy and integrity.

Law stated - 09 May 2023

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Federal Decree Law No. 45 of 2021 on Personal Data Protection (the UAE Law) only came into effect on 2 January 2022, and its executive regulations are still to be announced. Controllers and processors must adjust their respective positions (with reference to the provisions contained in the UAE Law) within a period of six months following the issuance of its executive regulations. Therefore, compliance with and the implementation of the UAE Law will start six months after the issuance of its executive regulations.

Law stated - 09 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP