Global Data and Cyber Handbook - UAE

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

While the UAE’s federal data protection law was issued in September 2021 and came into force on 2 January 2022, the implementing regulations required to supplement various aspects of the law had not been issued and the regulatory authority was not publicly operational as at the end of 2024. Organizations that are subject to the law have a grace period that extends until six months after the publication of the implementing regulations to ensure compliance with the law.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 18 December 2024*

☒ omnibus – all personal data

The UAE has enacted its own standalone data protection law, Federal Decree-Law No. 45 of 2021 regarding Personal Data Protection ("**PDPL**"). The PDPL borrows heavily, in terms of its concepts and content, from the EU General Data Protection Regulation but excludes government entities and government data from its scope. It also does not apply to financial or health data where that is subject to separate regulation or to any free zones that have their own data protection regime (see below).

☒ sector-specific

The UAE has introduced sector specific laws that regulate different categories of data, most notably in the healthcare, telecoms and financial services sectors. Certain economic zones are also subject to their own data protection laws, notably the financial free zones of Dubai International Financial Centre (“**DIFC**”) and Abu Dhabi Global Market (“**ADGM**”). There is also a patient health data regulation in the Dubai Health Care City free zone and, in the Emirate of Dubai, the Dubai Data Law mandates the sharing, use and reuse of data relating to the Emirate. Please refer to the separate chapters on DIFC and ADGM for analysis of those regimes.

☒ constitutional

## What are the key data privacy laws and regulations?

*Last review date: 18 December 2024*

The main UAE federal laws are:

Federal Decree-Law No. 45 of 2021 on Personal Data Protection ("**PDPL**")

Federal Decree-Law No. 44 of 2021 establishing the Emirates Data Office

Federal Decree-Law No. 31 of 2021 on Crimes and Penalties ("**Penal Code**")

Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes ("**Cybercrimes Law**")

Federal Law. No 2 of 2019 on the Use of Information and Communications Technology in Healthcare ("**Healthcare ICT Law**")

Federal Decree-Law No. 33 of 2021 on the Regulation of the Employment Relationship ("**The Labour Law**")

Further laws and regulatory requirements apply in particular contexts and to specific types of technology.

## What are the key cybersecurity laws and regulations?

*Last review date: 18 December 2024*

There is no federal law on cybersecurity. Instead, cybersecurity issues are regulated at a sector level and by a range of policies, standards and guidelines. Not all of these requirements are routinely made publicly available.

## What are the key laws and regulations relating to non-personal data?

*Last review date: 18 December 2024*

There is no general regulation of non-personal data.

Sectoral rules, such as those in telecoms, healthcare or financial services, may regulate categories of data that could include personal and non-personal data. The PDPL excludes from its scope government data and (to the extent that they are covered by separate legislation) financial and healthcare data.

In the Emirate of Dubai, the Dubai Data Law mandates the sharing, use and reuse of data relating to the Emirate.

Separate regulation on government data is anticipated, while the Central Bank of the UAE has issued various rules and standards imposing requirements on financial institutions regarding the protection of banking information and the Healthcare ICT Law includes provisions relating to the protection of health information.

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 18 December 2024*

Yes.

The PDPL came into force on 2 January 2022. It is the first omnibus personal data protection law in the UAE and enshrines many of the core principles and concepts found in the EU General Data Protection Regulation ("**GDPR**").

The implementing regulations to the PDPL, which will expand on key topics including the penalties for breach, were set to be published within six months of the date the PDPL was published in the official gazette (i.e. by 28 May 2022). However, the regulations had not been published as at the end of 2024.

Controllers and processors will have six months from the date that the implementing regulations are issued to achieve compliance with the PDPL, although the data protection regulator has the ability to extend this period if necessary.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 18 December 2024*

The Emirates Data Office ("**Data Office**") was established under Federal Decree-Law No. 44 of 2021 as the new data regulator in the UAE. Among other responsibilities, the Data Office will be responsible for enforcing the PDPL and for issuing supporting legislation and guidance. As of the end of 2024, the Data Office was not publicly operational.

In relation to the Dubai Data Law (which regulates data relating to the Emirate and applies to federal and local government entities, as well as private sector companies designated to be in-scope), Digital Dubai is the entity that develops and oversees the implementation of policies and strategies relating to Dubai’s information technology, data, digital transformation, and cybersecurity.

In November 2020, the UAE established the UAE Cybersecurity Council with the aim of developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE. The council is chaired by the Head of Cyber Security for the UAE Government and contribute to creating a legal and regulatory framework that covers all types of cybercrimes, securing existing and emerging technologies and establishing a robust ‘National Cyber Incident Response Plan’ to enable swift and coordinated response to cyber incidents in the country.

## How active is each of the regulator(s)?

*Last review date: 18 December 2024*

**Data Office**

☒ Not very

**Digital Dubai**

☒ Moderately active

**National Cybersecurity Council**

☒ Moderately active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 18 December 2024*

Prior to the PDPL being enacted, the main privacy-related legislation in the UAE comprised a number of offences in the Penal Code and Cybercrimes Law relating to the disclosure of personal information or secrets. This required law enforcement authorities to investigate complaints and to refer any offenses that they identified to the public prosecutor to raise charges where they deemed appropriate. In our experience, the majority of cases brought by the public prosecutor under those provisions related to data theft by employees or financial crimes, as well as complaints in the context of broader disputes between the concerned parties.

While the PDPL was issued in September 2021 and came into force on 2 January 2022 according to its terms, the implementing regulations required to supplement various aspects of the PDPL had not been issued and the regulatory authority was not publicly operational by the end of 2024. Controllers and processors will be granted a grace period of six months from the issuance of the implementing regulations to become compliant with the PDPL. We anticipate that the regulator (once established) is likely to focus initially on outreach and education before taking substantive enforcement action.

Other governmental bodies and regulators (such as the Telecommunications & Digital Government Regulatory Authority (“**TDRA**”), Cybersecurity Council, UAE Council for Artificial Intelligence, and Digital Dubai) will continue their mandates to develop strategy and policy relating to data and cybersecurity within their relevant fields.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 18 December 2024*

**Regulatory investigations or direct enforcement activity by data or cyber regulators are**:

☒       Rare

**Class actions/group actions under data or cyber regulation are**:

☒       Not available in the jurisdiction

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 18 December 2024*

N/A. The PDPL does not currently detail the sanctions imposed for violations. These are to be clarified by a Cabinet decision stating the acts that constitute a violation of the PDPL and its implementing regulations and the administrative penalties to be imposed.

## If data subjects have private remedies, what form can these remedies take?

*Last review date: 18 December 2024*

The PDPL does not envisage representative or class actions. Accordingly, any such claims would likely need to be brought in accordance with the requirements of the UAE civil law.

# Key Definitions

## Personal data

*Last review date: 18 December 2024*

Personal data is defined in the PDPL as any data related to an identified natural person, or related to a natural person that can be identified directly or indirectly by linking the data, through the use of identification elements such as their name, voice, image, identification number, or electronic ID, geographical location, or one or more of their morphological, physiological, economic, cultural or social characteristics.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 18 December 2024*

Sensitive personal data is defined in the PDPL as any data that directly or indirectly reveals a natural person's family or ethnic origin, political or philosophical opinions, religious beliefs, criminal record, or biometric data, or any data related to the health of that person, including his physical, psychological, intellectual, mental, bodily, genetic or sexual condition or orientation, including information related to the provision of health care services to him that reveals his health condition.

**Sensitive data includes:**

☒    personal data revealing racial or ethnic origin
☒    personal data revealing political opinions
☒    personal data revealing religious or philosophical belief
☒    genetic data
☒    biometric data for the purpose of uniquely identifying a natural person
☒    data concerning health/medical information
☒    data concerning a natural person's sex life or sexual orientation
☒    personal data regarding an individual's criminal convictions or record

## Controller vs Processor

*Last review date: 18 December 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is 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

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** Yes. Both concepts are defined in a similar manner to the GDPR; namely a controller is an establishment or natural person who alone or jointly with others determines the way, method and standards for processing such personal data and the purposes and means of processing it, whether alone or jointly with other persons or facilities; and a processor is defined as any establishment or natural person who processes personal data on behalf of a controller, as directed and instructed by the controller. This should be noted however that the PDPL, unlike the GDPR, expressly excludes any government authorities from its scope of application.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 18 December 2024*

☒    applies to organizations located in the jurisdiction
☒    other

The PDPL applies to the processing of personal data, whether totally or partially, through automatically operated electronic systems or other means by: (i) every data subject who resides or has a place of business in the UAE; (ii) any controller or processor located in the UAE that carries out the activities of processing the personal data of data subjects inside or outside the UAE; and (iii) any controller or processor located outside the UAE that carries out the activities of processing personal data of data subjects in the UAE.

Notably, the personal data processing operations of government and judicial entities, as well as law enforcement authorities, and entities operating in free zones that are subject to specific personal data protection laws are expressly excluded from the scope of the PDPL. Similar to the GDPR, natural persons who process personal data for their own personal purposes are also excluded from the scope of the PDPL.

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 18 December 2024*

Yes.

In addition to the consent of the data subject that is considered the default legal basis, the PDPL provides for the following additional legal bases for processing personal data:

the processing is necessary for the protection of the public interest;

the processing is related to the personal data that has become publicly available and known by an act of the data subject;

the processing is necessary to initiate or defend any claim or legal proceedings or when the processing is in connection with judicial or security proceedings;

the processing is necessary for the purposes of occupational or preventive medicine in order to assess the employees' ability to work, for medical diagnosis, for health or social care, for treatment, for health insurance services or for the management of health or social care systems and services in accordance with the applicable legislation in the UAE;

the processing is necessary to protect public health, including protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of healthcare, medicines, drugs and medical devices, in accordance with the applicable legislations in the UAE;

the processing is necessary for archival purposes or for scientific, historical and statistical studies in accordance with the applicable legislation in the UAE;

the processing is necessary for the protection of the data subject's interests;

the processing is necessary for the purposes of the controller or data subject carrying out its obligations and exercising its legally established rights in the field of employment, social security or under the laws of social protection, to the extent permitted by such laws;

the personal data is necessary to perform a contract with the data subject or to take measures at the request of the data subject with the aim of concluding, amending or terminating a contract;

the processing is necessary to implement specific obligation in other laws in the country of the controller; and

any other cases to be specified in the implementing regulations.

The following are potential legal bases for processing personal data:

☒    the data subject has provided consent to the processing for the identified purposes
☒    the personal data is necessary to perform a contract with the data subject
☒    the personal data is necessary to comply with a legal obligation
☒    the personal data is necessary to protect the vital interests of a natural person
☒    the personal data is necessary for a public interest
☒    the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)
☒    other

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 18 December 2024*

☒ Yes

The same legal bases required for processing personal data apply to sensitive personal data; the PDPL does not currently differentiate between the processing of personal data and sensitive personal data.

The following are potential legal bases for processing sensitive personal data:

☒    the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data
☒    processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
☒    processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
☒    processing relates to personal data which are manifestly made public by the data subject
☒    processing is necessary for the establishment, exercise or defense of legal claims
☒    processing is necessary for reasons of substantial public interest
☒    processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
☒    processing is necessary for reasons of public interest in the area of public health
☒    processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
☒    other

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 18 December 2024*

There are no specific provisions in the PDPL regulating the processing of minors' data.

## In what circumstances do these special requirements apply?

*Last review date: 18 December 2024*

N/A

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 18 December 2024*

There are no special requirements on this regard, however consent should technically be obtained from an adult in order to be relied on in the local courts. Market practice varies greatly particularly in the context of downloading mobile applications and use of online services.

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 18 December 2024*

The list of information that must be provided to a data subject prior to beginning processing is less extensive than the equivalent list that must be provided pursuant to the GDPR. Indeed, under the PDPL, the only information that a controller needs to provide to the data subject before starting the processing are (i) the purposes of processing, (ii) the targeted sectors or establishments with whom his/her personal data will be shared from inside and outside the UAE, and (iii) the protection measures for cross border processing carried out in accordance with the relevant articles under the PDPL. However, further disclosures will likely need to be made in a privacy notice in order to comply with the general obligation to process personal data in a manner that is fair and transparent and, where relying on consent, to ensure that it is valid under the PDPL, and the implementing regulations may introduce further specific requirements.

☒    the identity and the contact details of the controller and, where applicable, of the controller's representative
☒    the legal basis for the processing
☒    the categories of personal data concerned
☒   the recipients or categories of recipients of the personal data, if any
☒    information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available
☒    the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
☒    the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.
☒    the existence of the right to withdraw consent if processing is based on consent
☒   the right to lodge a complaint with a supervisory authority
☒    if applicable, information regarding automated decision making, including profiling
☒    other

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 18 December 2024*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒   right to access the data subject's own personal data
☒   right to rectify/correct the data subject's own personal data where inaccurate or incomplete
☒   right to erasure of personal data
☒   right to restrict data processing
☒   right to data portability
☒   right to object to the processing of personal data
☒   right to withdraw consent
☒   other

In addition to the above rights, the data subject has the right to object to decisions issued with respect to automated processing that have legal consequences or seriously affect the data subject.

In addition, the PDPL (Right to obtain information) dictates the information that should be made available to the data subject on request: including details of the type of personal data; purposes of processing; decisions made based on automated processing (including profiling); targeted sectors or establishment with which personal data is to be shared; controls and standards for the periods of storing and keeping personal data; procedures for correcting, erasing or limiting the processing and objection to personal data; protection measures for cross-border processing; steps to be taken in the event of a breach or infringement of personal data; and the process for filing complaints with the Data Office.

## Are there accountability and governance requirements?

*Last review date: 18 December 2024*

☒ Yes

There are accountability and governance requirements, which oblige controllers to:

perform and document data protection impact assessments ("**DPIAs**") for high-risk processing;

maintain a record of processing activities;

implement appropriate measures to comply with data privacy and security;

demonstrate compliance with data privacy and security;

identify a specific individual as the data privacy contact for data subject or data protection authority inquiries;

audit or supervise data processors.

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 18 December 2024*

☒ Yes

Notably, the appointment of a DPO is mandatory where the processing:

would cause a high-level risk to the confidentiality and privacy of the data subject's personal data as a result of the adoption of new technologies or in connection with the volume of the data;

involves a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing; or

is carried out on a large volume of sensitive personal data.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: 18 December 2024*

☒ Yes

If yes, under what circumstances?

☒    the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
☒    the core activities of the controller or the processor consist of processing on a large scale of special categories of data
☒    other

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 18 December 2024*

☒ Yes

The DPO is required to have adequate skills and knowledge of personal data protection law.

**If yes, what are these requirements?**

☒ other professional qualifications / experience

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 18 December 2024*

There is no general licensing, registration or notification requirement under the PDPL. However, licenses and/or approvals may be required in certain circumstances, for example from the telecommunications regulator where providing a service which is reliant on Internet of Things technology.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 18 December 2024*

☒ Yes

The controller is obliged to appoint a processor who provides sufficient guarantees regarding security measures (i.e, those measures applied to protect personal data) in a manner that ensures that the processing satisfies the requirements of the PDPL. However, the PDPL does not set out any specific criteria that must be considered when selecting a processor or require that the appointment of the processor must be documented by the controller in writing (although this may be implied by other provisions of the PDPL).

The obligations are as follows:

☒    controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 18 December 2024*

☒ Yes

The processor must:

carry out processing in accordance with the instructions of the controller, and the agreements concluded between them that specify in particular the scope, subject, purpose, nature of the processing, the type of personal data and the categories of the data subjects;

adopt the appropriate technical and organizational measures and procedures to protect the personal data at the design stage, whether during the identification of the means of processing or during the processing itself, taking into account the cost of implementing these measures and procedures and the nature, scope and purposes of the processing;

carry out the processing in compliance with the purpose and for the specified period, and in the event that the processing exceeds the specified period, notify the controller of the same to allow the controller to authorize them to extend this period or to give the appropriate directions;

delete the data after the expiry of the processing period or hand it back to the controller;

not take any action that would disclose the personal data or the results of processing, except in cases authorized by law;

protect and secure the processing and secure the electronic media and devices used in the processing, as well as the personal data on them;

maintain a special record of the personal data processed on behalf of the controller, to include the data of the controller, processor and data protection officer, a description of the categories of the personal data it has, the data of the persons authorized to access the personal data, the processing periods, limitations and scope of processing, the mechanism for deleting, modifying or processing personal data, the purpose of processing, any data relating to the cross-border movement and processing of such data, and the technical and organizational measures for information security;

in the event of a data breach, immediately inform the controller and file a report with the Data Office; and

at the request of the controller or Data Office, provide all means to prove compliance with the provisions of the PDPL;

If more than one processor participates in the processing, such processing shall be carried out in accordance with a written contract or agreement that clearly defines their obligations, responsibilities and roles in respect of the processing, otherwise they will be jointly held liable for the obligations and responsibilities contained in the PDPL and its implementing regulations.

The implementing regulations may detail further requirements and technical standards related to compliance with these obligations.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 18 December 2024*

☒ Yes

Personal data may only be transferred outside of the UAE in the following cases:

the country to which the personal data will be transferred has special legislation in place for the protection of personal data, which includes the most important provisions, measures, controls, conditions and rules for protecting the privacy and confidentiality of the data subject's personal data and his/her ability to exercise his/her rights, as well as provisions that enable the application of appropriate measures to the controller or processor through a supervisory or judicial entity; and

if there is a bilateral or multilateral treaty concerning data protection signed between the UAE and the country to which the personal data is to be transferred.

In addition, a data transfer may be made to a jurisdiction which does not satisfy the requirements outlined above where: (i) the transfer is made under a contract that obligates the recipient to implement the most important provisions, measures, controls, conditions and rules to protect the privacy and confidentiality of the data subject's personal data and their ability to exercise the rights afforded by the PDPL; (ii) the data subject has given his/her express consent to transfer personal data outside the UAE in a manner that does not conflict with the public and security interest of the country; (iii) the transfer is necessary for the implementation of obligations and the establishment, exercise or defense of rights before the judicial entities; (iv) the transfer is necessary for the conclusion or execution of a contract concluded between the controller and the data subject or between the controller and a third party in pursuit of the data subject's interests; (v) the transfer is necessary to perform a procedure relating to international judicial cooperation; and (vi) the transfer is necessary for the protection of the public interest. The implementing regulations will set out further details on these controls regarding the cross border transfer of personal data.

Transfers of personal data to third countries are permissible only, if there is a legal basis for the processing/transfer and one of the following applies:

☒    approved adequate/whitelisted jurisdictions
☒    derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims
☒    other solutions

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

No.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 18 December 2024*

No. Under the PDPL, a data subject’s consent must first be obtained before a controller can engage in any processing, including direct marketing activities via calling, e-mailing, or texting consumers. This position is echoed in the UAE's Consumer Protection Law.  Under the PDPL, there is no alternative legal basis that can be relied upon to serve marketing, even where an existing relationship exists with the customer. As well as the right to withdraw their consent at any time, the PDPL provides data subjects with an express right to object to and suspend any processing of their personal data carried out for direct marketing purposes. However, the Consumer Protection Law establishes the default position that companies are not permitted to use consumer personal data for promotion and marketing purposes without prior obtaining the consumer's consent. Telemarketing Regulations issued in 2024 (Cabinet Decision No. 56 of 2024) created new obligations for all companies involved in telemarketing, including obligations aimed at safeguarding consumer privacy.

☒**email marketing**

☒  prior opt-in consent

☒**telephone marketing**

☒  prior opt-in consent

☒**SMS/text message marketing**

☒  prior opt-in consent

☒**postal marketing**

☒  prior opt-in consent

☒**online behavioral advertising targeting//social media targeting/ad personalization marketing**

☒  prior opt-in consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 18 December 2024*

Yes.

The PDPL identifies the following legal bases that specifically apply in an employment context:

the processing is necessary for the purposes of occupational or preventive medicine in order to assess the employees' ability to work, for medical diagnosis, for health or social care, for treatment, health insurance services or for management of health or social care systems and services in accordance with the applicable legislation in the UAE; or

the processing is necessary for the purposes of the controller or data subject carrying out its obligations and exercising its legally established rights in the field of employment, social security or under the laws of social protection, to the extent permitted by such laws.

More generally, in an employment context the employer may process an employee's personal data when the processing is necessary for compliance with the applicable law to which the controller (i.e. the employer) is subject.

## Can consent be validly obtained in the employment context?

*Last review date: 18 December 2024*

☒    Yes, same as for data subjects outside the employment context.

Unlike the GDPR, under the PDPL there is no reference to the fact that consent must be "freely given." This removes one argument that arises in respect of compliance with the equivalent requirements of the GDPR, whereby the unequal bargaining power of the parties in an employment context fails to satisfy this requirement. The pending implementing regulations may provide further clarity as to the context in which consent can be relied on as a valid means of legitimizing processing.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

No.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 18 December 2024*

☒ Yes

Data subjects are entitled to object to the decisions made by automated processing, which have legal consequences or seriously affect the data subject, including profiling.

The restrictions or requirements are as follows:

☒    qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 18 December 2024*

As an exception to the above rule, data subjects may not object to the decisions made by automated processing in the following cases:

if the automated processing is conducted pursuant to the terms of a contract between the data subject and the controller;

if the automated processing is necessary in accordance with other applicable laws in the UAE; or

if the data subject gives prior consent to the automated processing in accordance with the conditions specified under the PDPL.

Further, the controller must: (i) implement appropriate procedures and measures to protect the privacy and confidentiality of the data subject's personal data in the cases referred to in a) to c) above and must not to harm or prejudice the data subject's rights; and (ii) incorporate an element of human review to the automated decision making process at the request of the data subject.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 18 December 2024*

No.

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 18 December 2024*

No enforcement activity to date.

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 18 December 2024*

☒    Non-binding guidance or principles issued or in progress

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 18 December 2024*

No.

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 18 December 2024*

Unclear.

## If so, how would any regulatory fines be calculated?

*Last review date: 18 December 2024*

Unclear.

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 18 December 2024*

Unclear.

## If so, how would any regulatory fines be calculated?

*Last review date: 18 December 2024*

Unclear.

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 18 December 2024*

Yes

☒    general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

The technical and organizational measures and procedures adopted by controllers and processors have to ensure that the information security level is commensurate with the risks associated with the relevant processing, in accordance with best international standards and practices.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 18 December 2024*

☒   public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks?)
☒   network information security requirements (broader than telecommunications)
☒   health regulatory requirements
☒   financial services requirements
☒   telecommunication requirements
☒   providers of critical infrastructure
☒  digital or connected (IoT) products

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last review date: 18 December 2024*

☒    financial services
☒    critical infrastructure

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 18 December 2024*

Yes.

## Controllers/Owners have to notify:

*Last review date: 18 December 2024*

☒  data protection authorities

☒  affected individuals

The controller shall, immediately upon becoming aware of any breach or violation of the data subject's personal data that could prejudice the privacy, confidentiality and/or security of that data, report to the Data Office such breach or violation within the period and in accordance with the procedures and conditions to be determined by the implementing regulations of the PDPL, including by submitting the information and documents listed in the PDPL.

The controller must also notify the data subjects in the event that the violation or breach occurred would prejudice the privacy, confidentiality and security of their personal data and inform them of the measures undertaken in connection with the breach, in accordance with the procedures and conditions to be determined by the implementing regulations of the PDPL.

## Processors/Agents have to notify:

*Last review date: 18 December 2024*

☒    controller/ owner

The processor must immediately inform the relative controller when a violation or breach occurs, and the controller will in turn be responsible for reporting the breach to the Data Office.

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 18 December 2024*

☒  health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)
☒  financial services requirements
☒  telecommunication requirements
☒  providers of critical infrastructure

Under the UAE Central Bank ("**CBUAE**") Consumer Protection Regulations and Consumer Protection Standards, banks and other Licensed Financial Institutions ("**LFIs**") must notify (i) the CBUAE of all "*significant"* breaches affecting consumer personal data; and (ii) affected consumers if the breach poses a "*risk to their financial or personal security"*.

LFIs and banks are liable to reimburse consumers for actual harm suffered from a data breach.

With regard to the laws regulating healthcare activities: (i) the Abu Dhabi - Healthcare Information and Cybersecurity Standard issued on February 2019, under the standard control HI 2.1., states that the licensed entity has to establish processes to notify the health sector regulator of any probabilities of breaches involving healthcare information; and (ii) the Dubai Health Authority ("**DHA**") Policy on Health Data Protection and Confidentiality, under paragraph 4.18.5., states that the licensed entity must report any breach of health information to both the UAE Information Office and the DHA.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 18 December 2024*

☒ Yes

☒  a) data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may be also be stored outside of the jurisdiction):

In the context of electronic payment processing and for parties operating in or providing services to customers in the health sector.

☒  b) other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 18 December 2024*

☒         Obligation for public sector organizations to share or make accessible non-personal data

The Dubai Data Law includes data sharing and exchange commitments, including reference to the Dubai government’s Open Data Committee. Other Emirates (including Abu Dhabi and Ajman) and the federal government of the UAE also have open data portals and programs falling broadly under the TDRA’s Smart Data Strategy and National Smart Data Framework.

☒         Obligation for private organizations to share or make accessible other non-personal data

In relation to data relating to the Emirate of Dubai, the Dubai Data Law may be extended to specified private sector organizations upon a determination by Digital Dubai.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 18 December 2024*

☒         Obligation to share data on request

☒         Obligation to share data proactively

☒         Obligation to (re)design products or services to facilitate data accessibility

☒         Obligation to standardize products or services to facilitate data portability or interoperability

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.