Global Data and Cyber Handbook - Dubai International Financial Center (DIFC)

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

# What's new?

## Recently Updated Topics

In 2024, DIFC was accepted into the Global CBPR Forum’s Global Cooperation Arrangement for Privacy Enforcement (CAPE) and became the first jurisdiction in the Middle East to be designated by the Global Forum Association as an Associate Member.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

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

*Last review date: 23 December 2024*

omnibus – all personal data

The Dubai International Financial Centre (DIFC), a free trade zone in the Emirate of Dubai, is subject to its own data protection laws, which are derived from the EU data protection legal framework. The legal framework for the DIFC will be addressed in this chapter.

constitutional

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

*Last review date: 23 December 2024*

The main laws are:

[DIFC Data Protection Law (DIFC Law No. 5 of 2020)](https://www.difc.ae/business/laws-regulations/legal-database/data-protection-law-difc-law-no-5-2020/)

[UAE Penal Code (Federal Law No. 3 of 1987)](https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_PENALTIES%20AND%20CRIMINAL%20MEASURES/UAE-LC-En_1987-12-08_00003_Kait.html?val=EL1)

[UAE Cybercrime Law (Federal Law No. 5 of 2012)](http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf)

## What are the key cybersecurity laws and regulations?

*Last review date: 23 December 2024*

Cybersecurity tends to be regulated at a sector level, with requirements contained in a mixture of primary legislation, such as in regulations, as well as secondary legislation passed by sector regulators, such as policies, standards and guidelines. Not all of these requirements are routinely made public. Specific security requirements also apply to certain types of service or technology (e.g. Internet of Things solutions). Certain of these requirements will apply equally to organizations conducting business in the DIFC.

Aside from the data protection law, the main source of requirements that apply to organizations doing business in the DIFC are set out in the UAE’s Penal Code and Cybercrimes Law, which prohibits certain activities from being carried out in the digital space or using technological means. These criminal laws apply equally in the UAE's free zones, including financial free zones such as the DIFC.

Financial institutions that are regulated by the Dubai Financial Services Authority ("**DFSA**") are encouraged, although not mandated, to implement the DFSA Cyber Risk Management Guidelines issued in December 2020 ("**Guidelines**"). The Guidelines are mainly principle based and reflect good industry practices to assist financial institutions to: (i) establish a robust cyber risk management framework within which to identify, manage and mitigate cyber risks effectively in an integrated and comprehensive manner; and (ii) strengthen the security, reliability, resiliency and recoverability of their systems.

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

*Last review date: 23 December 2024*

There is no general regulation of non-personal data in the DIFC.

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

*Last review date: 23 December 2024*

No, although the DIFC Commissioner of Data Protection continues to develop supporting guidance and other aspects of the implementation framework for the DIFC Data Protection Law and its Regulations.

# 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: 23 December 2024*

The DIFC Commissioner of Data Protection oversees the enforcement of the DIFC Data Protection Law. They are appointed by the President of the DIFC in consultation with the Board of Directors of the DIFC Authority.

There are no regulators with specific responsibility for cybersecurity and non-personal data enforcement in the DIFC.

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

*Last review date: 23 December 2024*

Moderately active

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

*Last review date: 23 December 2024*

While details of fines issued for breaches of the DIFC Data Protection Law are not routinely published, inspection statistics are posted on a regular basis.

The DIFC’s reports indicate that the total number of administrative fines issued in 2023 was 323, compared to 41 in 2022. Such fines generally arise as a result of basic compliance contraventions, such as non-renewal of processing notifications or failure to reply to an investigation request.

In furtherance of the objectives referred to above and to support the DIFC Authority's broader aim to make the DIFC an attractive jurisdiction for conducting business, the Commissioner has confirmed that (i) he is in favor of adopting a balanced and objective approach to enforcement of the law; (ii) that he does not envisage imposing significant fines for minor breaches; (iii) that the imposition of general fines, which are not subject to a statutory maximum, will only be applied in exceptional cases; and that (iv) where businesses are proactive in their efforts to achieve compliance with the Law, the Commissioner's Office is likely to look upon them more favorably in the event of a branch in comparison to a business that has made little effort to reflect the requirements of the Law in its processes and procedures.

Given the introduction in the Regulations supplementing the DIFC Data Protection Law of specific regulation on the processing of personal data using autonomous and semi-autonomous systems, the DIFC Commissioner may start to place an increased level of scrutiny on the use of such systems, particularly in light of the nascent but growing international regulatory landscape with respect to the use and deployment of artificial intelligence.

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

*Last review date: 23 December 2024*

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

Rare

Increasing

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: 23 December 2024*

**There are:**

administrative remedies from regulators and law enforcement

Breaches of the DIFC Data Protection Law may result in statutory fines. The list of fines is set out in Schedule 2 of the DIFC Data Protection Law. Multiple fines may be levied where more than one of the law’s requirements have been breached. The Commissioner also has the power to impose overarching fines, for example in response to flagrant or multiple breaches of the law. These discretionary fines are currently uncapped but the Commissioner has the power to implement further specific guidance on this issue.

criminal penalties from regulators and law enforcement

The onshore criminal law also applies in the DIFC and privacy breaches could, in some circumstances, amount to a criminal offence punishable by a custodial sentence and/or a fine. All offences will be investigated by the Dubai police and referred to the public prosecutor if the police deem it necessary. In practice, the police are unlikely to interfere in data protection compliance matters, which are regulated by the DIFC Data Protection Law.

private remedies

It is possible for a data subject to apply to the DIFC Courts for damages for a breach of the DIFC Data Protection Law. The calculation of damages would be determined with reference to the DIFC Law of Damages and Remedies (DIFC Law No. 7 of 2005) and, where not addressed in the law, the principles of English common law.

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

*Last review date: 23 December 2024*

individual personal actions

# Key Definitions

## Personal data

*Last review date: 23 December 2024*

Under the DIFC Data Protection Law, personal data is defined as any information referring to an identified or Identifiable Natural Person (being a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity).

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

*Last review date: 23 December 2024*

Under the DIFC Data Protection Law, special category data is defined as personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

**Sensitive data includes:**

personal data revealing racial or ethnic origin

personal data revealing political opinions

personal data revealing religious or philosophical belief

personal data revealing trade union membership

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: 23 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?

Yes.

Both concepts are defined in a similar manner to the same terms used in the GDPR; namely a Controller is any person who alone or jointly with others determines the purposes and means of processing Personal Data; and a Processor is defined as any person who processes Personal Data on behalf of a Controller.

# Territorial Scope

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

*Last review date: 23 December 2024*

applies to organizations located in the jurisdiction

applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

The DIFC Data Protection Law applies to (i) the processing of personal data by organizations operating or conducting business in or from the DIFC regardless of where the actual processing takes place (i.e., DIFC incorporated or licensed entities); (ii) an entity that, regardless of its place of incorporation, processes personal data in the DIFC as part of stable arrangements, other than on an occasional basis; and (iii) processing activities conducted in the DIFC, including transfers of personal data out of the DIFC. For the purposes of the scope, the law specifies that the term "in the DIFC" means that the personnel used to conduct the processing activity are physically located in the DIFC.

Accordingly, the DIFC Data Protection Law could also apply to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction to the extent this requires processing to be conducted in the DIFC.

# 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: 23 December 2024*

Yes.

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

There are additional legal bases for processing personal data, which can be relied upon by DIFC authorities (i.e., the DIFC Authority).

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

*Last review date: 23 December 2024*

Yes

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 a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

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 is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

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

other

Other legal basis for processing sensitive personal data include the following:

processing is necessary to comply with applicable law that applies to a controller in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime

processing is required for protecting members of the public against dishonesty, malpractice, incompetence or other improver conduct of persons providing banking, insurance, investment, management consultancy, information technology services, accounting or other services or commercial activities (either in person or indirectly by means of outsourcing), including any resulting financial loss.

processing is proportional and necessary to protect a data subject from potential bias or inaccurate decision making, where such risk would be increased regardless of whether special category personal data is processed

In addition, it is worth noting that where processing is required for the purpose of medicine, the assessment of the working capacity of any employee etc., the personal data concerned must be processed under the responsibility of a health professional subject to an obligation of professional secrecy or by another person who is subject to an obligation of secrecy under the applicable law.

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

*Last review date: 23 December 2024*

No.

## In what circumstances do these special requirements apply?

*Last review date: 23 December 2024*

N/A

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

*Last review date: 23 December 2024*

N/A

# Information Requirements, Data Subject Rights, Accountability and Governance

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

*Last review date: 23 December 2024*

the identity and the contact details of the controller and, where applicable, of the controller’s representative

the contact details of the data protection officer, where applicable

the purposes of the processing for which the personal data is intended

the legal basis for the processing

the categories of personal data concerned

the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources

the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground

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

whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

if applicable, information regarding automated decision making, including profiling

In addition, the controller is required to provide any further information necessary, having regard to the specific circumstances in which the personal data is collected, to ensure fair and transparent processing of that data.

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

*Last review date: 23 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

Data subjects also have the right to object to any decision making based solely on automated personal data processing (see section on [Profiling and Automated Decision Making](https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/emea/dubai-international-financial-center-difc/topics/profiling-and-automated-decision-making)).

## Are there accountability and governance requirements?

*Last review date: 23 December 2024*

Yes.

**There are accountability and governance requirements to:**

take privacy by default and design measures for all processing of personal data

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

provide training to employees

audit or supervise data processors

# DPOs and Notification Requirements

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

*Last review date: 23 December 2024*

Yes.

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

Last review date: *23 December 2024*

Yes.

If yes, under what circumstances?

the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

other

Appointment of a DPO is mandatory where the controller performs High Risk Activities on a systematic or regular basis. Certain of these are based on the threshold tests set out above.

High Risk Processing Activities is defined as the processing of personal data where one or more of the following applies:

processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a data subject, including due to the sensitivity of the personal data or risks relating to the security, integrity or privacy of personal data;

a considerable amount of personal data will be processed (including staff and contractor personal data) and where such processing is likely to result in a high risk to the data subject, including due to the sensitivity of the personal data or risks relating to security, integrity or privacy of the personal data;

the processing will involve a systematic and extensive evaluation of personal aspect relating to natural persons, based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural persons or similarly significantly affect the natural person; or

a material amount of special categories of personal data is to be processed.

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

*Last review date: 23 December 2024*

Yes.

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

resident in the jurisdiction

other

Notably, the individual must be a resident in the region, unless he is employed by the organization's group and performs a similar function for the group on an international basis. In addition, they must have knowledge of the DIFC Data Protection Law and its requirements.

## 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: 23 December 2024*

Yes.

A notification must be filed with the Commissioner and it must be kept up to date through amended notifications, which are kept on a publicly available register maintained by the Commissioner.

# Data Processors

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

*Last review date: 23 December 2024*

Yes.

The obligations are as follows:

controllers must only use processors subject to a written agreement that complies with specific requirements

The agreement must be legally binding and must provide sufficient assurances that the processor will implement appropriate technical and organizational measures that ensure the processing meets the requirements of the DIFC Protection Law and protects data subjects' rights. The agreement must also satisfy a set of mandatory requirements that are broadly equivalent to those set out in Article 28 of the GDPR.

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

*Last review date: 23 December 2024*

Yes.

Create a record of processing activities carried out on behalf of the controller which documents the required information under Article 15(1) of the DIFC Data Protection Law.

Assess whether it is mandatory for the company to appoint a DPO as required under Article 16(2) of the DIFC Data Protection Law and if it is not necessary to appoint a DPO clearly allocate responsibility for oversight and compliance within its organization. If required under Article 16(2), appoint a DPO and publish their contact details and, on request, confirm their identity to the Commission on writing.

The processor will be obliged to enter into an agreement with any sub-processor which will oblige the processor to comply with the mandatory requirements under Article 24(5) of the DIFC Data Protection Law.

Put in place appropriate technical and organizational measures to protect the personal data against unauthorized or unlawful processing (including transfers), and against accidental loss, destruction or damage, with reference to appropriate to the risk, the nature, scope, context and purposes of the processing as well as the prevailing information security good industry practice.

A processor (or sub-processor) must immediately inform the controller or processor (as applicable) whether, in its opinion, the processing activities infringes the DIFC Data Protection Law. Notably, if the processor infringes the DIFC Data Protection Law by determining the means and purposes of the processing (i.e., by acting other than on the instructions of the controller), then they shall be considered to be a controller in respect of that processing and will assume all the responsibilities and obligations of a controller.

The processor (together with the controller) will be in breach of the DIFC Data Protection Law if they commence any mutually agreed processing without a written agreement in place.

The processor (in addition to the controller) must take steps to ensure that any person acting under their authority that has access to personal data does not process it except on the instructions of the controller, unless it is required to do so by law.

The processor is required to notify the relevant controller without undue delay after they become aware of a personal data breach.

Additional statutory requirements will apply in specific circumstances and certain requirements will be imposed by the contractor in the form of the data processing agreement.

# International Data Transfer

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

*Last review date: 23 December 2024*

Yes.

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

approved standard contractual clauses

binding corporate rules

derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

***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?

*Last review date: 23 December 2024*

No.

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

*Last review date: 23 December 2024*

Yes.

**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

Direct marketing activities are regulated by the DIFC Data Protection Law (i.e., data subjects must be notified if their data will be used to carry out direct marketing and must be told before it is disclosed to a third party for this purpose. However, consent does not provide the only legitimate legal basis to use data for marketing purposes. The DIFC Authority has also addressed the issue of marketing in guidance issued by the DIFC Authority in January 2019 (updated in July 2020). The guidance is not binding but does provide the DIFC Authority's view on best practice and those activities that should be avoided.

# 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: 23 December 2024*

Yes.

There are a range of legal bases that can be relied upon for this purpose, including where the processing relates to personal data:

the processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of a controller or a data subject in the context of the data subject's employment, including but not limited to recruitment, visa or work permit processing, the performance of an employment contract, termination of employment, the conduct of proceedings relating to employment and the administration of a pension, retirement or employee money purchase benefit; and

the processing is necessary for compliance with the applicable law to which the controller (i.e., the employer) is subject.

Further legal bases may be relevant in the context of an investigation into any alleged wrongdoing by the employee.

For the processing of special categories of personal data, the most generally relevant legal bases would be that the processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of a controller or a data subject in the context of the data subject's employment, including but not limited to recruitment, visa or work permit processing, the performance of an employment contract, termination of employment, the conduct of proceedings relating to employment and the administration of a pension, retirement or employee money purchase benefit scheme.

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

*Last review date: 23 December 2024*

Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

While it may be possible to rely on consent in the employment context, the DIFC Commissioner of Data Protection is known to take into account guidance published by the European Commission, the European Data Protection Board and its predecessor as well as the guidance published by the UK data protection regulator (the Information Commissioner's Office). Accordingly, reliance on consent in the employment context in DIFC could be difficult given the unequal bargaining power between the employer and employee meaning that the consent provided in such context is arguably not freely given.

## 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?

Yes

In September 2023, the DIFC enacted amendments to Regulations under the DIFC Data Protection Law. The new Regulation 10 concerning personal data processed through autonomous and semi-autonomous systems 10 is the first regulation of its kind in the Gulf region to impose specific obligations for controllers and processors with respect to the use of autonomous systems (such as AI systems).

# 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: 23 December 2024*

Yes.

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

right to information / transparency requirement

right to request human review of the automated decision making

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

*Last review date: 23 December 2024*

Yes.

The decision of a data subject to object to any decision based solely on automated processing, which includes profiling, shall not apply to a decision that is: (i) necessary for entering into, or performance of a contract between a data subject and a controller; (ii) authorized by applicable law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights; or (iii) based on the data subject's explicit consent.

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

*Last review date: 23 December 2024*

Yes.

In September 2023, the DIFC enacted amendments to Regulations under the DIFC Data Protection Law. The new Regulation 10 concerning personal data processed through autonomous and semi-autonomous systems 10 is the first regulation of its kind in the Gulf region to  impose specific obligations for controllers and processors with respect to the use of autonomous systems (such as AI systems).

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

*Last review date: 23 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: 23 December 2024*

Yes, laws in force

Regulation 10 introduced new obligations for users and operators aimed at developing a responsible and ethical approach with regard to the processing of personal data processed through autonomous and semi-autonomous systems. The Regulation emphasizes ensuring transparency (through the provision of a notice in clear and explicit terms upon the initial use of, or access to, the systems, alerting users to any underlying technology and processes comprising the systems that may undertake any processing activities which is not human-initiated, controlled, or directed), fairness, ethics, security and accountability (e.g. a system must have mechanisms in place to ensure responsibility and accountability for enabling its systems and outcomes), and require implementing robust risk management and governance frameworks for AI-powered systems.

# 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: 23 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: 23 December 2024*

Unclear

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

*Last review date: 23 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: 23 December 2024*

Unclear

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

*Last review date: 23 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: 23 December 2024*

Yes.

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

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

*Last review date: 23 December 2024*

There are no such DIFC-specific regulations or laws. Please see the UAE chapter for information on obligations applicable to the UAE as a whole.

## 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?

Data privacy

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

*Last review date: 23 December 2024*

Yes.

Data breaches that compromise a data subject's confidentiality, security or privacy must be notified to the Commissioner as soon as practicable in the circumstances. No specific time-frame is specified in the law and no further written guidance has been offered on how the requirement 'as soon as practicable in the circumstances' should be interpreted. In practice, the Commissioner of Data Protection has confirmed that they will not hold companies to a 72-hour reporting timeframe. However, equally it is a safe assumption that reporting within 72-hours, even if only to make a preliminary notification, will be considered sufficient to satisfy the requirement.

Processors are also obliged to notify the Controller without undue delay after becoming aware of a breach. Again, there is no specific timeframe specified in the legislation. In the absence of further guidance as to what 'without undue delay' means we would recommend that the words are given their ordinary meaning in everyday language and that the term is interpreted on a case-by-case basis, taking into account the circumstances.

## Controllers/Owners have to notify:

*Last review date: 23 December 2024*

data protection authorities

Namely the DIFC Commissioner of Data Protection

affected individuals

Where a personal data breach is likely to result in a high risk to the security or rights of a data subject, the controller shall communicate the breach to the affected data subject(s) as soon as practicable in the circumstances. If there is an immediate risk of damage to the data subject, the controller shall promptly inform the affected data subject. No specific timeframe has been defined in the legislation, and no further written guidance has been offered on how these requirements should be interpreted in practice.

## Processors/Agents have to notify:

*Last review date: 23 December 2024*

controller/ owner

The processor must inform the relevant controller without undue delay after becoming aware of the personal data breach. There is no specific timeframe specified in the legislation. In the absence of further guidance as to what 'without undue delay' means we would recommend that the words are given their ordinary meaning in everyday language and that the term is interpreted on a case-by-case basis, taking into account the circumstances.

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

*Last review date: 23 December 2024*

Yes.

financial services requirements

Under the DFSA Rule Book, any entity regulated by the DFSA must advise the DFSA immediately if it becomes aware, or has reasonable grounds to believe, that any of the following matters may have occurred or may about to occur:

any matter which could have a significant adverse effect on the [regulated entity’s] reputation

any matter in relation to the [regulated entity] which could result in serious adverse financial consequences to the financial system or to other firms

a significant breach of a rule by the [regulated entity] or any of its employees, and

any significant failure in the [regulated entity’s] systems or controls, including a failure reported to the [regulated entity] by the firm’s auditor.

There are various other provisions that might be relevant here and we have only selected a few. Notably, due to the fact that the DIFC is a free zone, which caters to banks and financial services companies, amongst others, many DIFC entities will also be regulated by the DFSA.

# 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: 23 December 2024*

Yes.

tax or financial record laws

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

*Last review date: 23 December 2024*

No, there are no such DIFC-specific regulations or laws. Please see the UAE chapter for information on mandatory requirements applicable to the UAE as a whole.

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

*Last review date:23 December 2024*

N/A.

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.