DATA PROTECTION LAWS OF THE WORLD

UAE - Dubai (DIFC)

UAE - DUBAI (DIFC)

Last modified 9 January 2024

LAW

Note: Please also see UAE – General, UAE – ADGM, UAE – DHCC.

The Dubai International Financial Centre (“**DIFC**”) is a financial freezone in Dubai emirate. The DIFC has powers to issue laws regarding its governance. The DIFC Law No. 5 of 2020 on Data Protection Law (“**DPL**”) came into effect in July 2020.

In addition, alongside the DPL a new set of accompanying Data Protection Regulations (“**DPRs**”) were introduced. These were updated in 2023 to include regulations on processing via artificial intelligence systems.

DEFINITIONS

Definition of Data Subject

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

Definition of Personal Data

Any data referring to an “Identifiable Natural Person”.

Definition of Identifiable Natural Person

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 (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

Definition of Special Categories of Personal Data

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

Definition of Process, Processed, Processes and Processing

Any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of

stored Personal Data with the aim of limiting Processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on Personal Data by:

- a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or
- law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.

Definition of Substantial Public Interest

Includes, but is not limited to:

- administration of justice, including criminal and regulatory investigations; and
- exercise of a function conferred on a person by Applicable Law.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection (“**Commissioner**”) is essentially the regulating body in the DIFC from a data protection standpoint.

The Commissioner of Data Protection
Dubai International Financial Centre Authority
Level 14, The Gate
P.O. Box 74777
Dubai
United Arab Emirates

commissioner@dp.difc.ae

Tel: +971 4 362 2222

REGISTRATION

Controllers and Processors are required to submit a notification to the Commissioner via the DIFC’s online portal (the “**Notification**”) (Article 14 (7) DPL) and to keep that up Notification to date.

The Notification must contain the following information:

- a general description of the Personal Data Processing being carried out;
- an explanation of the purpose for the Personal Data Processing;
- the Data Subjects or class of Data Subjects whose Personal Data is being Processed;
- a description of the class of Personal Data being Processed; and
- a statement of jurisdictions to which Personal Data will be transferred by the Controller, along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection for the purposes of articles 26 and 27 of the DPL.

The information set out within the Notification will be available on the DIFC’s public register.

Where an organisation is required to appoint a Data Protection Officer (see DPO), the DPO must complete an “Annual Assessment” in the form prescribed by the Commissioner.

DATA PROTECTION OFFICERS

Data Protection Officers (“**DPOs**”) are mandatory for:

- DIFC Bodies (as defined under the DPL, other than courts acting in their judicial capacity); and
- a Controller or Processor performing high risk Processing activities on a systematic or regular basis.

A Controller or Processor could also be required to appoint a DPO by the Commissioner.

A Group (defined under DPL) may appoint a single DPO provided that he is easily accessible to each entity in the Group. The DPO must reside in the UAE unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis.

In addition, if a Controller or Processor is not required to appoint a DPO, it must still clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations and provide details to the Commissioner (i.e. the person appointed, pursuant to the DPL, to monitor, ensure and enforce compliance with the DPL).

(Article 16 DPL)

COLLECTION & PROCESSING

Data Controllers may collect and Process Personal Data when any of the following conditions are met (set out under Article 10 DPL):

- a Data Subject has given consent, which complies with the comprehensive consent requirements set out under Article 12 of the DPL, to the Processing of that Personal Data for specific purposes;
- Processing is necessary for the performance of a contract to which a Data Subject is a party, or in order to take steps at the request of a Data Subject prior to entering into such contract;
- Processing is necessary for compliance with applicable law that a Controller is subject to;
- Processing is necessary in order to protect the vital interests of a Data Subject or of another natural person;
- Processing is necessary for:
    - performance of a task carried out by a DIFC Body in the interests of the DIFC;
    - exercise of a DIFC Body’s powers and functions; or
    - the exercise of powers or functions vested by a DIFC Body in a Third Party to whom Personal Data is disclosed by the DIFC Body; or
- Processing is necessary for the purpose of legitimate interests pursued by a Controller (or a third party to whom the Personal Data has been made available, subject to Article 13 of the DPL which sets out certain restrictions on the ability to rely upon legitimate interests), except where such interests are overridden by the interests or rights of a Data Subject.

Data controllers may collect and Process Special Categories of Personal Data when any of the following conditions are met (as per Article 11 DPL), in addition to establishing one of the legal bases under Article 10, set out above:

- a Data Subject has given explicit consent, which complies with the comprehensive consent requirements set out under Article 12 of the DPL, to the Processing of those Special Categories of Personal Data for one (1) or more specified purposes;
- 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;

- Processing is necessary to protect the vital interests of a Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent;
- Processing is carried out by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities, subject to appropriate assurances and provided that the Processing relates:
    - solely to the members or former members of such an entity; or
    - to other persons who have regular contact with such a body in connection with its purpose,

    and the Personal Data is not disclosed to a Third Party without the consent of a Data Subject;
- Processing relates to Personal Data that has been made public by a Data Subject;
- Processing is necessary for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognised alternative dispute resolution procedures, such as mediation) or is performed by the Court acting in its judicial capacity;
- Processing is necessary for compliance with a specific requirement of Applicable Law to which a Controller is subject, and in such circumstances the Controller must provide a Data Subject with clear notice of such Processing as soon as reasonably practicable unless the obligation in question prohibits such notice being given;
- 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 the purposes of preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or the treatment or the management of health or social care systems and services, provided that the Personal Data is Processed by or under the responsibility of a health professional subject to an obligation of professional secrecy under applicable law or by another person also subject to an obligation of secrecy under applicable law;
- Processing is required for protecting members of the public against dishonesty, malpractice, incompetence or other improper 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; or
- 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.
- Processing is necessary for Substantial Public Interest reasons that are proportionate to the aim(s) pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the rights of the Data Subject.

Information Provision

Controllers are required to provide Data Subjects with certain information around how their Personal Data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information required to be provided is set out in detail under Part 5 of the DPL.

Where the Controller collects the Personal Data from the Data Subject, the information must be provided at the time of collection. (Article 29 DPL)

Where the Controller does not collect the Personal Data from the Data Subject, the Controller must provide the information:

- no longer than one (1) month from obtaining the Personal Data; or
- if the Personal Data is used for communicating with the Data Subject, no later than the first communication; or
- if a disclosure (including the making available for Processing) to a Processor or a third party is envisaged, no later than the time when the Personal Data is first disclosed.

(Article 30 DPL)

TRANSFER

As per Article 26 DPL, Personal Data may be transferred out of the DIFC:

- to a country or jurisdiction that has been determined to have adequate protections (available on the DIFC Commissioner for Data Protection website); or
- if it takes place in accordance with Article 27 DPL.

Article 27 DPL provides that:

A transfer or a set of transfers of Personal Data to a Third Country (i.e. Anywhere other than the DIFC, including onshore UAE) or an International Organisation (as defined within the DPL) may take place on condition that:

- the Controller or Processor in question has provided appropriate safeguards (as described in Article 27(2), set out below)), and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available;
- one of the specific derogations in Article 27(3) (set out below) applies; or
- the limited circumstances in Article 27(4) (set out below) apply.

Article 27 (2) DPL provides that the appropriate safeguards referred to at (a) above may be provided for by:

- a legally binding instrument between public authorities;
- Binding Corporate Rules (i.e. Personal Data protection policies and procedures, aggregated or incorporated in a single written document, which regulate the transfer of Personal Data between members of a Group, legally bind such members to comply, and which contain provisions for the protection of such Personal Data);
- standard data protection clauses adopted by the Commissioner (available on the DIFC website); The DIFC SCCs are a synthethised set of SCCs modelled on the EU Model Clauses and UK IDTA. They do not however take a modular approach;
- an approved code of conduct pursuant to Article 48 together with binding and enforceable commitments of the Controller or Processor in the third country or the International Organisation to apply the appropriate safeguards, including regarding a Data Subject’s rights; or
- an approved certification mechanism pursuant to Article 50 DPL together with binding and enforceable commitments of the Controller or Processor in the Third Country or the International Organisation to apply the appropriate safeguards, including regarding Data Subjects' rights.

Article 27 (3) DPL sets out the following derogations:

- a Data Subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;
- the transfer is necessary for the performance of a contract between a Data Subject and Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;
- the transfer is necessary for the conclusion or performance of a contract that is in the interest of a Data Subject between a Controller and a third party;
- the transfer is necessary for reasons of Substantial Public Interest;
- the transfer is necessary or legally required in the interests of the DIFC, including in the interests of the DIFC Bodies relating to the proper discharge of their functions;
- the transfer is necessary for the establishment, exercise or defence of a legal claim;
- the transfer is necessary in order 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;
- the transfer is made in compliance with applicable law and data minimisation principles from a register that is:
    - intended to provide information to the public; and
    - open for viewing either by the public in general or by any person who can demonstrate a legitimate interest;
- subject to Article 28 DPL (which sets out the requirements for data sharing with public authorities), the transfer is:
    - The transfer is necessary for compliance with any obligation under applicable law to which the Controller is subject;
    - The transfer is made at the reasonable request of a regulator, police or other government agency or competent authority;
- the transfer is subject to international financial standards, the transfer is necessary to uphold the legitimate interests of a Controller recognised in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
- the transfer is necessary to comply with applicable anti-money laundering or counter-terrorist financing obligations that apply to a Controller or Processor or for the prevention or detection of a crime.

Article 27(4) DPL provides that where a transfer could not be based on one of the aforementioned bases (including those at (a) –(k) (thereby making data transfers more flexible under the DPL), such transfer to a Third Country or an International Organisation may take place only if:

- the transfer is not repeating or part of a repetitive course of transfers;
- concerns only a limited number of Data Subjects;
- is necessary for the purposes of compelling legitimate interests pursued by the Controller that are not overridden by the interests or rights of the Data Subject; and
- the Controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

Under such circumstances the Controller is required to inform the Commissioner of any such transfer and to inform the Data Subject of the transfer and the compelling legitimate interests.

SECURITY

Controllers and Processors must implement appropriate technical and organisational measures to protect Personal Data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, taking into account:

- the nature, scope, context and purpose of the Processing;
- the risks presented by the Processing to a relevant Data Subject; and
- prevailing information security good industry practice.

They must also review and update such measures, where necessary, to reflect legal, operational and technical developments.

(Article 14 (2) DPL)

BREACH NOTIFICATION

If there is a Personal Data breach that compromises a Data Subject's confidentiality, security or privacy, the data Controller must, as soon as practicable in the circumstances (note that unlike the GDPR there is no hard deadline), notify the Personal Data breach to the Commissioner. Such notifications must include, at a minimum, the following information:

- description of the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate amount of Personal Data records concerned;
- the name and contact details of the DPO or other contact point where more information can be obtained;
- a description of the likely consequences of the Personal Data breach; and
- describe the measures taken or proposed to be taken by the Controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all of the information at (a) – (d) at the same time, the information may be provided in phases, as it becomes available.

In addition, Processors must notify Controllers without undue delay after becoming aware of a Personal Data breach.

Controllers and Processors must fully co-operate with any investigation of the Commissioner in relation to a Personal Data breach.

Controllers must also document in writing any Personal Data breaches, including the facts relating to the Personal Data breach, its effects and the remedial action taken. The information recorded must be sufficient to enable the Commissioner to verify compliance with the law and must be made available without delay on request.

(Article 41 DPL)

A Controller must make a notification to a Data Subject as soon as practicable in the circumstances (again, no hard deadline) where a Personal Data breach is likely to result in a high risk to the security or rights of a Data Subject. If there is an immediate risk of damage to the Data Subject, the Controller must promptly communicate with the affected Data Subject (for example, where his or her banking details are the subject of the breach).

Where a communication to the individual Data Subjects would involve disproportionate effort, a public communication or similar measure whereby the Data Subjects are informed in an “equally effective manner” will be sufficient.

Such notifications must include, at least, the information listed in (b) – (d) above, in clear and plain language. It must also, where possible, make recommendations for the Data Subject to mitigate against any potential adverse effects.

The Guidance to the DIFC DPL (“**Guidance**”) recommends that Controllers and Processors have in place an incident management policy which enables them to comply with the law in a timely fashion. It recommends clear incident classification as well as setting out the reporting requirements (including who to notify and when, with time being of the essence).

(Article 42 DPL)

ENFORCEMENT

The Commissioner has general powers to investigate and conduct inspections where it suspects that a Controller or Processor is not operating within the law.

Where it concludes that the Controller or Processor is not acting in compliance with the DPL, it has the power to:

- order it to do or refrain from doing any act or thing within such time as may be specified in the direction;
- order it to refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction;
- issue an administrative fine in an amount he considers appropriate but not exceeding the amount specified in Schedule 2 in respect of each contravention. The fines range from USD 10,000 to USD 100,000 and there are around 35 in total; and / or
- issue a general fine in an amount he considers appropriate and proportionate, taking into account the seriousness of the contravention and the risk of actual harm to any relevant Data Subject.

There is also a process built into the DPL and the DPRs for disputing any action taken by the Commissioner, with an ultimate right to challenge any action in court (Article 63 DPL).

Under the DPL Data Subjects also have the right to bring a claim for compensation where they suffer “material or non-material damage” by reason of any contravention of the law.

The DPL also contains provisions allowing Data Subjects to make compensation claims in relation to contraventions of the data protection law. Under the DPL, court proceedings can be initiated by the Commissioner as well as by Data Subjects.

The Commissioner has recently begun to publish certain limited information on its investigations and enforcement activities, including published decisions on infringements, which are available upon the DIFC website.

ELECTRONIC MARKETING

The DPL requires Controllers to provide Data Subjects with various pieces of information when they process their personal data (typically by way of a privacy notice, which must meet the detailed requirements set out Part 5 of the DPL), including whether the personal data will be used for direct marketing purposes.

Whilst consent is not expressly required (implying that one of the other legal bases can potentially be relied upon), Data Subjects do have 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 to be expressly offered the right to object to such disclosures or uses; and
- where Personal Data is Processed for direct marketing purposes, object at any time to such Processing, including Profiling to the extent that it is related to such direct marketing.

(Article 34 DPL)

The Controller should also make clear in its Notification to the Commissioner that one of the purposes for which it Processes Personal Data is that of direct marketing.

ONLINE PRIVACY

Where a Controller is offering online services through a platform, the default privacy preferences of the platform must be set such that no more than the minimum Personal Data necessary to deliver or receive the relevant services is obtained or collected, and a Data Subject should be:

- prompted to actively select his privacy preferences on first use; and
- able to easily change such preferences.

(Article 14(4) DPL)

In addition, Controllers are to make available a minimum of two methods (which may include, by way of example, post, telephone, email or an online form) by which a Data Subject can contact the Controller to request to exercise his rights under the DPL. If the Controller maintains a website, at least one method of contact must be made available without charge via the website, without the need to submit data to create an account of any sort. (Article 40 DPL)

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.