



DIFC

Data Protection Law 2007

DIFC Law No. 1 of 2007

DATA PROTECTION LAW 2007

TABLE OF CONTENTS

1.	Title	3
2.	Legislative Authority	3
3.	Date of Enactment	3
4.	Commencement	3
5.	Application of the Law	3
6.	Interpretation	3
7.	Administration of the Law	4
8.	General Requirements	4
9.	Requirements for Legitimate Processing	4
10.	Processing of Sensitive Personal Data	5
11.	Transfers out of the DIFC - Adequate Level of Protection	7
12.	Transfers out of the DIFC in the Absence of an Adequate Level of Protection	7
13.	Providing Information where Personal Data has been Obtained from the Data Subject	8
14.	Providing Information where Personal Data has not been Obtained from the Data Subject	9
15.	Confidentiality	10
16.	Security of Processing	10
17.	Right to Access to and Rectification, Erasure or Blocking of Personal Data	11
18.	Right to Object to Processing	11

19.	Requirement to Notify the Commissioner of Data Protection	11
20.	Register of Notifications	12
21.	Commissioner of Data Protection	12
22.	Appointment of the Commissioner of Data Protection	13
23.	Removal of the Commissioner of Data Protection	13
24.	Resignation of the Commissioner of Data Protection	13
25.	Powers and Functions of the Commissioner of Data Protection	13
26.	Production of Information	15
27.	Regulations	15
28.	Funding and Fees	17
29.	Annual Funding of the Commissioner of Data Protection	17
30.	Accounts	17
31.	Annual Report	17
32.	Directions	18
33.	Lodging Complaints and Mediation	18
34.	Application to the Court	19
35.	Compensation	19

SCHEDULE

1.	Rules of Interpretation	19
2.	Legislation in the DIFC	20
3.	Defined Terms	22

DATA PROTECTION LAW 2007

PART 1: GENERAL

1. Title

This Law may be cited as the “Data Protection Law 2007”.

2. Legislative Authority

This Law is made by the Ruler of Dubai.

3. Date of Enactment

This Law is enacted on the date specified in the Enactment Notice in respect of this Law.

4. Commencement

This Law comes into force on the date specified in the Enactment Notice in respect of this Law and replaces the DIFC Data Protection Law, being Law No. 9 of 2004. This Law abrogates the Data Protection Module (DAT) issued by the Dubai International Financial Services Authority (DFSA), which is replaced by the Data Protection Regulations 2007.

5. Application of the Law

This Law applies in the jurisdiction of the Dubai International Financial Centre.

6. Interpretation

The Schedule contains:

- (a) interpretative provisions which apply to this Law:
- (b) a list of defined terms used in this Law.

7. Administration of the Law

- (1) This Law and any legislation made for the purpose of this Law is administered by the Commissioner of Data Protection.
- (2) The President shall appoint the Commissioner of Data Protection.

PART 2: GENERAL REGULATIONS ON THE PROCESSING OF PERSONAL DATA

8. General Requirements

- (1) Data Controllers must ensure that Personal Data which they Process is:
 - (a) Processed fairly, lawfully and securely;
 - (b) Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights;
 - (c) adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further Processed;
 - (d) accurate and, where necessary, kept up to date; and
 - (e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which they are further Processed.
- (2) Every reasonable step must be taken by Data Controllers to ensure that Personal Data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further Processed, is erased or rectified.

9. Requirements for Legitimate Processing

- (1) Personal Data may only be Processed if:
 - (a) the Data Subject has given his written consent to the Processing of that Personal Data;
 - (b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

- (c) Processing is necessary for compliance with any legal obligation to which the Data Controller is subject;
- (d) Processing is necessary in order to protect the vital interests of the Data Subject;
- (e) Processing is necessary for the performance of a task carried out in the interests of the DIFC, the Dubai Financial Services Authority, the Court or in the exercise of the Commissioner of Data Protection's functions or powers vested in the Data Controller or in a Third Party to whom the Personal Data are disclosed; or
- (f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the Third Party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation.

10. Processing of Sensitive Personal Data

- (1) Sensitive Personal Data shall not be Processed unless:
 - (a) the Data Subject has given his written consent to the Processing of that Sensitive Personal Data;
 - (b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller;
 - (c) Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
 - (d) Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects;
 - (e) the Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims;
 - (f) Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;

- (g) Processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation;
 - (h) Processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller;
 - (i) Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Personal Data is Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;
 - (j) Processing is required for protecting members of the public against:
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, management consultancy, IT services, accounting or other commercial activities (either in person or indirectly by means of outsourcing);
 - (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, financial or other services; or
 - (k) authorised in writing by the Commissioner of Data Protection.
- (2) Article 10 (1) shall not apply if:
- (a) a permit has been obtained to Process Sensitive Personal Data from the Commissioner of Data Protection; and
 - (b) the Data Controller applies adequate safeguards with respect to the Processing of the Sensitive Personal Data.
- (3) The Court has jurisdiction to hear and determine any appeal in relation to a decision of the Commissioner of Data Protection to refuse to issue a permit to Process Sensitive Personal Data and its decision is final and binding upon the

Data Controller.

11. Transfers out of the DIFC - Adequate Level of Protection

- (1) A transfer of Personal Data to a Recipient located in a jurisdiction outside the DIFC may take place only if:
 - (a) an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable to the Recipient, as set out in Article 11 (2); or
 - (b) in accordance with Article 12.
- (2) For the purposes of Article 11(1), a jurisdiction has an adequate level of protection for that Personal Data if that jurisdiction is listed as an acceptable jurisdiction under the Regulations or with the written approval of the Commissioner of Data Protection.

12. Transfers out of the DIFC in the Absence of an Adequate Level of Protection

- (1) A transfer or a set of transfers of Personal Data to a Recipient which is not subject to laws and regulations which ensure an adequate level of protection within the meaning of Article 11 may take place on condition that:
 - (a) the Commissioner of Data Protection or his delegate has granted a permit or written authorisation for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of this Personal Data;
 - (b) the Data Subject has given his written consent to the proposed transfer;
 - (c) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of precontractual measures taken in response to the Data Subject's request;
 - (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a Third Party;
 - (e) the transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims;
 - (f) the transfer is necessary in order to protect the vital interests of the Data

Subject;

- (g) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;
 - (h) the transfer is necessary for compliance with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, police or other government agency;
 - (i) the transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
 - (j) the transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller.
- (2) The Court has jurisdiction to hear and determine any appeal in relation to a decision of the Commissioner of Data Protection to refuse to issue a permit referred to in Article 12 (1)(a) and his decision is final and binding upon the Data Controller.

13. Providing Information where Personal Data has been Obtained from the Data Subject

- (1) Data Controllers shall provide a Data Subject whose Personal Data it collects with at least the following information immediately upon commencing to collect Personal Data in respect of that Data Subject:
 - (a) the identity of the Data Controller;
 - (b) the purposes of the Processing for which the Personal Data are intended;
 - (c) any further information in so far as such is necessary, having regard to the specific circumstances in which the Personal Data are collected, to guarantee fair Processing in respect of the Data Subject, such as:
 - (d) the Recipients or categories of Recipients of the Personal Data;
 - (e) whether replies to questions are obligatory or voluntary, as well as the

- possible consequences of failure to reply;
 - (f) the existence of the right of access to and the right to rectify the Personal Data;
 - (g) whether the Personal Data will be used for direct marketing purposes; and
 - (h) whether the Personal Data will be Processed on the basis of Article 11 (1)(g) or Article 12 (1)(i).
- (2) A Data Controller need not provide that information otherwise required by Article 12 (1)(d) to the Data Subject if the Data Controller reasonably expects that the Data Subject is already aware of that information.

14. Providing Information where Personal Data has not been Obtained from the Data Subject

- (1) Where Personal Data has not been obtained from the Data Subject, a Data Controller or his representative must at the time of undertaking the Processing of Personal Data or if a disclosure to a Third Party is envisaged, no later than the time when the Personal Data is first Processed or disclosed provide the Data Subject with at least the following information:
- (a) the identity of the Data Controller;
 - (b) the purposes of the Processing;
 - (c) any further information in so far as such further information is necessary, having regard to the specific circumstances in which the Personal Data is Processed, to guarantee fair Processing in respect of the Data Subject, such as:
 - (i) the categories of Personal Data concerned;
 - (ii) the Recipients or categories of Recipients;
 - (iii) the existence of the right of access to and the right to rectify the Personal Data concerning him;
 - (iv) whether the Personal Data will be used for direct marketing purposes; and
 - (v) whether the Personal Data will be Processed on the basis of Article 11 (1)(g) or Article 12 (1)(i).

- (2) Article 15 (1) shall not apply to require:
 - (a) the Data Controller to provide information which the Data Controller reasonably expects that the Data Subject already has; or
 - (b) the provision of such information if it proves impossible or would involve a disproportionate effort.

15. Confidentiality

Any person acting under a Data Controller or a Data Processor, including the Data Processor himself, who has access to Personal Data must not Process it except on instructions from the Data Controller, unless he is required to do so by law.

16. Security of Processing

- (1) The Data Controller must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where the Processing of Personal Data is performed pursuant to Article 10 or Article 12 above.
- (2) Having regard to the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected.
- (3) The Data Controller must, where Processing is carried out on its behalf, choose a Data Processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, and must ensure compliance with those measures.
- (4) In the event of an unauthorised intrusion, either physical, electronic or otherwise, to any Personal Data database, the Data Controller or the Data Processor carrying out the Data Controller's function at the time of the intrusion, shall inform the Commissioner of Data Protection of the incident as soon as reasonably practicable.

PART 3: RIGHTS OF DATA SUBJECTS

17. Right to Access to and Rectification, Erasure or Blocking of Personal Data

- (1) A Data Subject has the right to require and obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense:
 - (a) confirmation as to whether or not Personal Data relating to him is being Processed and information at least as to the purposes of the Processing, the categories of Personal Data concerned, and the Recipients or categories of Recipients to whom the Personal Data are disclosed;
 - (b) communication to him in an intelligible form of the Personal Data undergoing Processing and of any available information as to its source; and
 - (c) as appropriate, the rectification, erasure or blocking of Personal Data the Processing of which does not comply with the provisions of the Law.

18. Right to Object to Processing

- (1) A Data Subject has the right:
 - (a) to object at any time on reasonable grounds relating to his particular situation to the Processing of Personal Data relating to him; and
 - (b) 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.
- (2) Where there is a justified objection, the Processing instigated by the Data Controller shall no longer include that Personal Data.

PART 4: NOTIFICATIONS TO THE COMMISSIONER OF DATA PROTECTION

19. Requirement to Notify the Commissioner of Data Protection

- (1) A Data Controller must establish and maintain records of any Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.

- (2) The Data Controller must file a notification with the Commissioner of Data Protection in accordance with the Regulations.
- (3) The Commissioner of Data Protection may make Regulations prescribing:
 - (a) the information in relation to Personal Data Processing operations that must be recorded for the purposes of Article 19 (1);
 - (b) the circumstances in which a Data Controller must notify the Commissioner of Data Protection of any operations referred to in Article 19 (1); and
 - (c) the content of any such notification.

20. Register of notifications

The Commissioner of Data Protection shall keep a register of Personal Data Processing operations notified in accordance with Article 19.

PART 5: COMMISSIONER OF DATA PROTECTION

21. Commissioner of Data Protection

- (1) The President shall appoint a person to be the Commissioner of Data Protection who is appropriately experienced and qualified.
- (2) The Commissioner of Data Protection is responsible for the administration of this Law and may appoint any appropriate person to discharge his duties and exercise his powers under this Law and any Regulations.
- (3) The Commissioner of Data Protection shall develop and carry out policies to promote greater awareness of this Law.
- (4) The Commissioner of Data Protection, by conditional or unconditional written authority, may delegate the Commissioner of Data Protection's powers and duties under this Law to any appropriate person employed under Article 21 (2).
- (5) A person to whom the Commissioner of Data Protection, by written authority under Article 21 (4), delegates powers and duties may exercise the powers and shall perform the duties in accordance with the written authority.

22. Appointment of the Commissioner of Data Protection

- (1) The President shall consult with the DIFCA Board of Directors prior to appointing, re-appointing or dismissing the Commissioner of Data Protection.
- (2) The Commissioner of Data Protection shall be appointed for a specified period of time not exceeding three (3) years, and may be re-appointed provided that such period may not extend beyond the day when the Commissioner of Data Protection turns seventy-five (75) years of age.
- (3) In exercising his powers and performing his functions the Commissioner of Data Protection shall act in an independent manner.

23. Removal of the Commissioner of Data Protection

The Commissioner of Data Protection may be removed from office by written notice issued by the President for reasons of inability, incapacity or misbehaviour,

24. Resignation of the Commissioner of Data Protection

The Commissioner of Data Protection may at any time resign as the Commissioner of Data Protection by giving three (3) months written notice addressed to the President.

25. Powers and Functions of the Commissioner of Data Protection

- (1) It is the duty of the Commissioner of Data Protection to promote good practices by the Data Controllers and, in particular, to perform his functions under this Law and any Regulation made under it as to promote the observance of the requirements of this Law and any Regulation made under it by Data Controllers.
- (2) The Commissioner of Data Protection has such powers, duties and functions as conferred on it under this Law and any Regulation made under it and shall exercise such powers and perform such functions in pursuit of the objectives of this Law and any Regulations.
- (3) Without limiting the generality of Article 25 (2), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable:
 - (a) access Personal Data Processed by Data Controllers or Data Processors;
 - (b) collect all the information necessary for the performance of its supervisory

duties;

- (c) issue warnings or admonishments and make recommendations to Data Controllers;
- (d) initiate proceedings for contraventions of the Law before the Court;
- (e) impose fines in the event of non-compliance with its direction;
- (f) impose fines for non-compliance with the Laws and any Regulations;
- (g) initiate a claim for compensation on behalf of a Data Subject before the Court where there has been a material contravention of the Law to the detriment of the Data Subject;
- (h) preparing or causing to be prepared in a timely and efficient manner:
 - (i) draft Regulations;
 - (ii) draft standards or codes of practice; and
 - (iii) guidance;

reasonably required to enable him to perform his statutory functions;
- (i) submitting such draft Regulations, draft standards, and draft codes of practice to the President and the DIFCA Board of Directors for approval and advising it of any guidance that is issued;
- (j) prescribing forms to be used for any of the purposes of this Law or any legislation administered by the Commissioner of Data Protection;
- (k) acquiring, holding and disposing of property of any description;
- (l) making contracts and other agreements;
- (m) with the prior consent of the President and DIFCA Board of Directors, borrowing monies and providing security for such borrowings;
- (n) employing and appointing persons on such terms as he considers appropriate to assist him in the exercise of his powers and performance of his functions;
- (o) where he considers it appropriate to do so, delegating such of his functions and powers as may more efficiently and effectively be performed by his officers or employees and, with the approval of the President either generally or in relation to any particular matter, by any other person; and

- (p) exercising and performing such other powers and functions as may be delegated to the Commissioner of Data Protection by the President pursuant to the provisions of this Law.
- (4) The Commissioner of Data Protection has power to do whatever he deems necessary, for or in connection with, or reasonably incidental to, the performance of his functions.

26. Production of Information

- (1) The Commissioner of Data Protection may require a Data Controller by written notice to:
 - (a) give specified information; or
 - (b) produce specified documentswhich relate to the Processing of Personal Data.
- (2) The Data Controller in respect of whom a requirement is made pursuant to Article 26(1) must comply with that requirement. Where the Data Controller fails to comply with the requirement, the Commissioner of Data Protection may impose a fine.

27. Regulations

- (1) The DIFC Authority, after consultation with the Commissioner, may make Regulations under the Law in respect of:
 - (a) any matters related to the application of the Law;
 - (b) as proposed by the Commissioner of Data Protection under Article 27 (2).
- (2) The Commissioner of Data Protection may propose Regulations to the DIFCA in respect of any matter that facilitates the administration and application of the Law or furthers the purposes of the Law, including but not limited to:
 - (a) the development and publication of information to DIFC entities and their employees concerning the application and interpretation of the Law and Regulations;
 - (b) procedures for initiating and filing complaints;
 - (c) procedures for appealing and reconsidering decisions or determinations of the Commissioner of Data Protection;

- (d) fines;
 - (e) forms, procedures and requirements under the Law;
 - (f) the keeping of the register of notifications; and
 - (g) the conduct of the Commissioner of Data Protection and his officers, employees and agents in relation to the exercise of powers and performance of functions.
- (3) Where the DIFCA issues a standard or code of practice, the DIFCA may incorporate such a standard or code into the Regulations by reference and in such circumstances, except to the extent that the Regulations otherwise provide, a person who is subject to the provisions of any such standard or code must comply with such provisions as if they were provisions of the Regulations.
- (4) Where any legislation made for the purpose of this Law purports to be made in exercise of a particular power or powers, it shall be taken also to be made in the exercise of all powers under which it may be made.
- (5) The DIFCA shall publish draft Regulations by means of a notice under Article 27 (6).
- (6) The notice of draft Regulations must include the following:
- (a) the draft text of the Regulations;
 - (b) a statement of the substance and purpose of the material provisions of the draft Regulations; and
 - (c) a summary of the draft Regulations.
- (7) Upon publication of a notice under Article 27 (6), the DIFCA shall invite Interested Persons to make representations with respect to the draft Regulations within a period of at least thirty (30) days after the publication, or within such period as the DIFCA Board of Directors may otherwise determine.
- (8) Article 27 (5), Article 27 (6) and Article 27 (7) shall not apply if the DIFCA concludes that any delay likely to arise under such Articles is prejudicial to the interests of the DIFC.
- (9) Any period of time during which the DIFCA invites Interested Persons to make representations with respect to draft Regulations prior to Article 27 coming into effect shall be deemed to count as part or all of the period referred to in Article 27 (7).

28. Funding and Fees

In respect of each financial year of the Commissioner of Data Protection, the President shall ensure that there is a provision of sufficient financial resources approved by the DIFCA to adequately perform its functions and exercise its powers in accordance with the Laws and the Regulations.

29. Annual Funding of the Commissioner of Data Protection

- (1) The Commissioner of Data Protection shall submit to the President for approval estimates of the annual income and expenditure of the Commissioner of Data Protection for the next financial year.
- (2) Such estimates shall include figures relating to levels of remuneration and entitlement to expenses of the Commissioner of Data Protection, officers, employees and agents of the Commissioner of Data Protection.
- (3) The Commissioner of Data Protection shall submit such estimates to the President for approval not later than forty-five (45) days before the end of the current financial year.
- (4) The President in consultation with the DIFCA may accept or reject such estimates within forty-five (45) days of receiving them, in writing to the Commissioner of Data Protection and where relevant state the reasons for rejection.

30. Accounts

- (1) The Commissioner of Data Protection shall keep proper accounts of its financial activities.
- (2) The Commissioner of Data Protection, shall before the end of the first quarter of the financial year, prepare financial statements for the previous financial year in accordance with accepted accounting standards.

31. Annual Report

- (1) As soon as practicable after 1 January in each year, the Commissioner of Data Protection shall deliver to the President, a report on the management of the administrative affairs of the Commissioner of Data Protection, for the previous year.
- (2) Such report shall give a true and fair view of the state of its regulatory operations in the DIFC, and financial statements of the Commissioner of Data Protection, as at the end of the relevant financial year.

PART 6: REMEDIES, LIABILITY AND SANCTIONS**32. Directions**

- (1) If the Commissioner is satisfied, after duly conducting all reasonable and necessary inspections and investigations, that a Data Controller has contravened or is contravening the Law or Regulations made for the purpose of the Law, he may issue a direction requiring him to do either or both of the following:
 - (a) to do or refrain from doing any act or thing within such time as may be specified in the direction; or
 - (b) 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.
- (2) The Commissioner of Data Protection shall carry out, as a minimum, due process by means of undertaking all the reasonable and necessary inspections and investigations to be adequately satisfied to establish the Data Controller's contravention with the Law or Regulations made for the purposes of this Law.
- (3) A direction issued under Article 32 (1) shall contain:
 - (a) a statement of the contravention of the Law or Regulations which the Commissioner of Data Protection is satisfied is being or has been committed; and
 - (b) a statement to the effect that the Data Controller may seek a review by the Court of the decision of the Commissioner of Data Protection to issue the direction.
- (4) A Data Controller who fails to comply with a direction of the Commissioner of Data Protection under this part of the Law contravenes this law and may be subject to fines and liable for payment of compensation.
- (5) A Data Controller may ask the Commissioner of Data Protection to review the direction within fourteen (14) days of receiving a direction under this part of the Law. The Commissioner of Data Protection may receive further submissions and amend or discontinue the direction.

33. Lodging Complaints and Mediation

- (1) A Data Subject who believes on reasonable grounds that he has been adversely affected by a contravention of the Law in respect of the Processing of his Personal Data and as regards the exercise of his rights under Articles 17 and 18

may lodge a complaint with the Commissioner of Data Protection.

- (2) The Commissioner of Data Protection may mediate between the affected Data Subject referred to in Article 33 (1) and the relevant Data Controller.
- (3) On the basis of the mediation referred to in Article 33 (2), the Commissioner of Data Protection may issue a direction requiring the Data Controller to do what he considers appropriate.
- (4) A Data Controller shall comply with any direction issued by the Commissioner of Data Protection under Article 33(3).

34. Application to the Court

- (1) Any Data Controller who is found to contravene this Law or a direction of the Commissioner of Data Protection may appeal to the Court within thirty (30) days.
- (2) The Court may make any orders that the Court may think just and appropriate in the circumstances, including remedies for damages, penalties or compensation.

35. Compensation

A Data Subject who suffers damage by reason of any contravention by a Data Controller of any requirement of this Law or the Regulations is entitled to compensation from the Data Controller for that damage.

SCHEDULE

1. Rules of Interpretation

- (1) In the Law, a reference to:
 - (a) a statutory provision includes a reference to the statutory provision as amended or re-enacted from time to time;
 - (b) a person includes any natural person, body corporate or body unincorporate, including a company, partnership, unincorporated association, government or state.
 - (c) an obligation to publish or cause to be published a particular document shall, unless expressly provided otherwise in the Law, include publishing or causing to be published in printed or electronic form;

- (d) a day shall refer to a business day, being a normal working day in the DIFC;
 - (e) a calendar year shall mean a year of the Gregorian calendar;
 - (f) a reference to the masculine gender includes the feminine and vice versa;
 - (g) where relevant the singular shall include the plural and vice versa.
- (2) The headings in the Law shall not affect its interpretation.
 - (3) References in this Law to a body corporate include a body corporate incorporated outside DIFC.
 - (4) A reference in this Law to a Part, Article or Schedule by number only, and without further identification, is a reference to the Part, Article or Schedule of that number in this Law.
 - (5) A reference in an Article or other division of this Law to a paragraph, sub-paragraph or Article by number or letter only, and without further identification, is a reference to the paragraph, sub-paragraph or Article of that number or letter contained in the Article or other division of this Law in which that reference occurs.
 - (6) Unless the context otherwise requires, where this Law refers to an enactment, the reference is to that enactment as amended from time to time, and includes a reference to that enactment as extended or applied by or under another enactment, including any other provision of that enactment.
 - (7) References in this Law to a writing, filing, instrument or certificate include any mode of communication that preserves a record of the information contained therein and is capable of being reproduced in tangible form, including electronic means.

2. Legislation in the DIFC

References to legislation and Guidance in the Law shall be construed in accordance with the following provisions:

- (a) Federal Law is law made by the federal government of the United Arab Emirates;
- (b) Dubai Law is law made by the Ruler, as applicable in the Emirate of Dubai;
- (c) DIFC Law is law made by the Ruler (including, by way of example, the Law), as applicable in the DIFC;

- (d) the Law is the Data Protection Law, DIFC Law No.1 of 2007 made by the Ruler;
- (e) the Regulations are legislation made by the DIFCA Board of Directors and are binding in nature; and
- (f) Guidance is indicative and non-binding and may comprise (i) guidance made and issued by the Commissioner of Data Protection for the purposes of this Law; and (ii) any standard or code of practice issued by the DIFCA Board of Directors.

3. Defined Terms

In the Law, unless the context indicates otherwise, the defined terms listed below shall have the corresponding meanings.

Terms	Definitions
Commissioner of Data Protection	the person appointed by the President pursuant to Article 7 (2) of the Law to administer the Law.
Court	the DIFC Court as established under Dubai Law.
Data Controller	any person in the DIFC who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Processor	any person who Processes Personal Data on behalf of a Data Controller.
Data Subject	the individual to whom Personal Data relates.
DIFC	the Dubai International Financial Centre.
DIFCA	the Dubai International Financial Centre Authority.
DIFCA Board of Directors	the governing body of the DIFCA established under Law No. 9 of 2004.
President	the President of the DIFC.
Identifiable Natural Person	is a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.
Interested Person	includes any person(s) who may be invited by the DIFCA Board of Directors to make representations

Terms	Definitions
	with respect to the notice of draft Regulations.
Law	the Data Protection Law 2007.
Personal Data	any information relating to an Identifiable Natural Person.
Process, Processed, Processes and Processing	Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Recipient	Any person to whom Personal Data is disclosed, whether a Third Party or not; however, authorities which may receive Personal Data in the framework of a particular inquiry shall not be regarded as Recipients.
Regulations	has the meaning given in Article 2 of Schedule 1 to the Law.
Ruler	the Ruler of the Emirate of Dubai.
Schedule	a schedule to the Law.
Sensitive 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.
Third Party	any person other than the Data Subject, the Data Controller, the Data Processor and the persons who, under the direct control of the Data Controller or the Data Processor, is authorized to Process the Personal Data.