DATA PROTECTION LAW

DIFC LAW NO. 1 OF 2007

Consolidated Version
(December 2012)

Amended by

Data Protection Law Amendment Law
DIFC Law No. 5 of 2012

CONTENTS

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

Schedule 1 contains:

(a) interpretative provisions which apply to this Law:

(b) a list of defined terms used in this Law.

7. Administration of the Law

This Law and any legislation made for the purpose of this Law is administered by the Commissioner of Data Protection.

PART 2: GENERAL REGULATIONS ON THE PROCESSING OF PERSONAL DATA

8. General Requirements

(1) Data Controllers shall 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 shall 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

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 for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFCA, the DFSA, the Court and the Registrar's functions or powers vested in the Data Controller or in a Third Party to whom the Personal Data are disclosed; or

(e) 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 any other jurisdiction as approved by 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 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;

(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 from the Data Subject with at least the following information as soon as possible 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:

(i) the Recipients or categories of Recipients of the Personal Data;

(ii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply

(iii) the existence of the right of access to and the right to rectify the Personal Data;

(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 12(1)(i) or Article 10(1)(g).

(2) A Data Controller need not provide that information otherwise required by Article 13(1) 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 shall 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 10(1)(g) or Article 12 (1)(i).

(2) Article 14 (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 shall 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 shall 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 shall, 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 shall 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

A Data Subject has the right to obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense:

(a) confirmation in writing 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 shall 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 shall file a notification with the Commissioner of Data Protection in accordance with the Regulations.

(3) The notification shall be accompanied by such fee as may be prescribed in the Regulations.

(4) The DIFCA Board of Directors, after consultation with the Commissioner of Data Protection, shall make Regulations prescribing:

(a) the information in relation to Personal Data Processing operations that shall be recorded for the purposes of Article 19 (1);

(b) the circumstances in which a Data Controller shall 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

(1) The Commissioner of Data Protection shall keep a register relating to the Personal Data Processing operations notified in accordance with Article 19 available for inspection by any person.

(2) Each entry in the register shall consist of:

(a) the registrable particulars notified in accordance with Article 19 or, as the case requires, those particulars as amended in accordance with Article 21; and

(b) such other information as the Commissioner of Data Protection deems appropriate.

(3) Any entry in the register shall be valid for a period of twelve (12) months and renewed annually upon payment of the relevant fee as prescribed in the Regulations.

21. Duty to notify changes

The Data Controller shall notify the Commissioner of Data Protection of any changes related to the registrable particulars notified under Article 19 in the manner prescribed in the Regulations.

PART 5: COMMISSIONER OF DATA PROTECTION

22. Appointment of the 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 President shall consult with the DIFCA Board of Directors prior to appointing, re-appointing or removal the Commissioner of Data Protection.

(3) 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.

23. Delegation powers of the Commissioner of Data Protection

The Commissioner of Data Protection, where he considers it appropriate to do so, may delegate such of his functions and powers as may more efficiently and effectively be performed by officers and employees of the Commissioner of Data Protection, and with the approval of the DIFCA Board of Directors, either generally or in relation to any particular matter, to any other person.

24. 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.

25. 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.

26. Powers, Functions and Objectives of the Commissioner of Data Protection

(1) The Commissioner of Data Protection has such powers, duties and functions as conferred on him under this Law and any Regulation made under this Law and shall exercise such powers and perform such functions in pursuit of the objectives of this Law and the Regulations.

(2) In performing his functions and exercising his powers, the Commissioner of Data Protections shall pursue the following objectives:

(a) to promote good practices and observance of the requirements of this Law and the Regulations by the Data Controllers; and

(b) to promote greater awareness and public understanding of data protection and the requirements of this Law and the Regulations in the DIFC.

(3) Without limiting the generality of Article 26(1), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable:

(a) accessing Personal Data Processed by Data Controllers or Data Processors;

(b) collecting all the information necessary for the performance of its supervisory;

(c) issuing warnings or admonishments and make recommendations to Data Controllers;

(d) initiating proceedings for contraventions of the Law before the Court;

(e) imposing fines in the event of non-compliance with its direction;

(f) imposing fines for non-compliance with the Law~~s~~ and any Regulations;

(g) initiating 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 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, 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.

(5) In exercising his powers and performing his functions the Commissioner of Data Protection shall act in an independent manner.

27. 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 documents which relate to the Processing of Personal Data.

(2) The Data Controller in respect of whom a requirement is made pursuant to Article 27(1) shall comply with that requirement. Where the Data Controller fails to comply with the requirement, the Commissioner of Data Protection may impose a fine.

28. Regulations

(1) The DIFCA Board of Directors, after consultation with the Commissioner of Data Protection, 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 28(2).

(2) The Commissioner of Data Protection may propose Regulations to the DIFCA Board of Directors 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) fees;

(f) forms, procedures and requirements under the Law;

(g) the keeping of the register of notifications; and

(h) 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 Board of Directors issues a standard or code of practice, it 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 shall 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 Commissioner of Data Protection shall publish draft Regulations by means of a notice under Article 28(6).

(6) The notice of draft Regulations shall 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 28(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 28(5), Article 28(6) and Article 28(7) shall not apply if the Commissioner of Data Protection 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 28 coming into effect shall be deemed to count as part or all of the period referred to in Article 28(7).

29. Funding

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

30. 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 as approved by the DIFCA Board of Directors no later than forty five (45) days before the end of the current 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 President in consultation with the DIFCA Board of Directors 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.

31. 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.

(3) The accounts prepared under Article 31(1) shall be submitted for the approval of the DIFCA Board of Directors.

31A. Audit

(1) The DIFCA Board of Directors shall appoint auditors to conduct an audit in relation to each financial year of the Commissioner of Data Protection.

(2) The DIFCA Board of Directors shall, as soon as reasonably practicable after the preparation and approval of the financial statements of the Commissioner of Data Protection, provide such statements to the relevant auditors for audit.

(3) The auditors shall prepare a report on the financial statements and send the

report to the DIFCA Board of Directors.

(4) Such report shall, where appropriate, include a statement by the auditors as to whether or not, in their opinion, the financial statements to which the report relates give a true and fair view of the state of the financial activities of the Commissioner of Data Protection as at the end of the financial year to which the financial statements relate and of the results of his operations and cash flows in the financial year.

(5) The auditors shall have a right of access at all reasonable times to all information which is reasonably required by them for the purposes of preparing the report and which is held or controlled by any officer, employee or agent of the Commissioner of Data Protection.

(6) The auditors shall be entitled reasonably to require from the officers, employees and agents of the Commissioner of Data Protection such information and explanations they consider necessary for the performance of their duties as auditors.

(7) A person shall not without reasonable excuse intentionally engage in conduct that results in the obstruction of a person appointed under Article 31A(1) in the exercise of his powers under Article 31A.

32. 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

33. Directions

(1) If the Commissioner of Data Protection 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 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 33(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) If the Commissioner of Data Protection considers that the Data Controller or any officer of it has failed to comply with the direction, he may apply to the Court for one or more of the following orders;

(a) an order directing the Data Controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the Commissioner of Data Protection relevant to the issue of the direction;

(b) an order directing the Data Controller or officer to pay any costs incurred by the Commissioner of Data Protection or other person relating to the issue of the direction by the Commissioner of Data Protection or the contravention of such Law, Regulations or legislation relevant to the issue of the direction; or

(c) any other order that the Court considers appropriate.

(6) 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.

34. 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 34(1) and the relevant Data Controller.

(3) On the basis of the mediation referred to in Article 34(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 34(3).

35. General contravention

A Data Controller who:

(a) does an act or thing that the Data Controller is prohibited from doing by or under this Law and the Regulations;

(b) does not do an act or thing that the Data Controller is required or directed to do under this Law and the Regulations; or

(c) otherwise contravenes a provision of this Law and the Regulations;

commits a contravention of this Law.

36. Administrative imposition of fines

(1) The DIFCA Board of Directors shall make Regulations on the procedures relating to the imposition and recovery of fines under this Article.

(2) Where the Commissioner of Data Protection considers that a Data Controller has contravened a provision of the Law referred to in Schedule 2 and in relation to which a fine is stipulated in that Schedule, he may impose by written notice given to the Data Controller a fine in respect of the contravention, of such amount as he considers appropriate but not exceeding the amount of the maximum fine specified in Schedule 2 in respect of each contravention.

(3) If, within the period specified in the notice:

(a) the Data Controller pays the prescribed fine to the Commissioner of Data Protection, then no proceedings may be commenced by the Commissioner of Data Protection against the person in respect of the relevant contravention, however the Commissioner of Data Protection may take action in relation to any continuing contravention to do or refrain from doing any act or thing; or

(b) the Data Controller takes such action as is prescribed in the Regulations to object to the imposition of the fine or has not paid the prescribed fine to the Commissioner of Data Protection, then the Commissioner of Data Protection may apply to the Court for, and the Court may so order, the payment of the fine or so much of the fine as is not paid and make any further order as the Court sees fit for recovery of the fine including any order for costs.

(4) A certificate that purports to be signed by the Commissioner of Data Protection and states that a written notice was given to a person pursuant to Article 36(2) imposing a fine on the basis of specific facts is:

(a) conclusive evidence of the giving of the notice to the person; and

(b) prima facie evidence of the facts contained in the notice;

in any proceedings commenced under Article 36(3).

37. 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.

38. 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 may apply to the Court for compensation from the Data Controller for that damage.

PART 7: GENERAL EXEMPTIONS

39. General exemptions

(1) The DIFCA Board of Directors may make Regulations exempting Data Controllers from compliance with this Law or any parts of this Law.

(2) Without limiting the generality of Article 39(1), Articles 11,12 13, 14 and 17 and 18 shall not apply to the DFSA, DIFCA and the Registrar if the application of these Articles would be likely to prejudice the proper discharge by those entities of their powers and functions under any laws administered by the DFSA, DIFCA and the Registrar, including any delegated powers and functions insofar as such powers and functions are designed for protecting members of the public against:

(a) 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 or other banking and financial activities and services, including insurance and reinsurance services, financial markets and financial and monetary brokerage services; or

(b) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services.

PART 8: MISCELLANEOUS

40. Fees

The fees applicable to a Data Controller shall be prescribed in the Regulations.

SCHEDULE 1

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) unless stated otherwise, a day means a calendar day. If an obligation falls on a calendar day which is either a Friday or Saturday or an official UAE holiday in the DIFC, the obligation shall take place on the next calendar day which is a business day;

(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) 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 22(1) of the Law to administer the Law.
Court	The DIFC Court as established under Dubai Law.
Data	Any information which: (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; or (c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System.
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.
DFSA	the Dubai Financial Services Authority established under Dubai law.

DIFCA	the DIFC Authority established under Dubai law.
DIFC	The Dubai International Financial Centre.
DIFCA Board of Directors	The governing body of the DIFCA established under Law No. 9 of 2004.
Government of Dubai	The Government of Dubai
Identifiable Natural Person	Is a natural living 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.
Law	The Data Protection Law 2007.
Personal Data	Any Data referring to an Identifiable Natural Person.
President	The President of the DIFC.
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.
Registrar	The Registrar of Companies appointed pursuant to Article 7 of the Companies Law, DIFC Law No.2 of 2009.
Regulations	Has the meaning given in Article 2 of Schedule 1 to the Law.
Relevant Filing System	Any set of information relating to an Identifiable Natural Person to the extent that, although the information is not Processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
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.
UAE	the United Arab Emirates

SCHEDULE 2 *CONTRAVENTIONS WITH FINES STIPULATED*		
Article of Law creating contravention	General nature of contravention	Maximum Fine
8	Failing to comply with general requirements specified under Article 8 of the Law made for the purpose of this Law	$15,000
9	Failure to comply with requirements for legitimate processing specified under Article 9 of the Law made for the purpose of this Law	$15,000
10(2)	Data Controller processing Sensitive Personal Data in accordance with Article 10(2) of the Law and failing to obtain a permit from the Commissioner of Data Protection	$10,000
12(1)(a)	Data Controller transferring Personal Data outside the DIFC in accordance with Article 12(1)(a) of the Law and failing to obtain a permit from the Commissioner of Data Protection	$20,000
16(1), 16(2)	Failing to implement and maintain technical and organisational measures to protect Personal Data in accordance with Articles 16(1) and 16(2) of the Law made for the purpose of this Law	$10,000
16(4)	Failing to report an unauthorised intrusion in accordance with Article 16(4) of the Law made for the purpose of this Law	$5,000
19(1)	Failing to maintain records of any Personal Data Processing operations	$5,000
19(2)	Failing to register with the Office of the Commissioner of Data Protection	$25,000
22(1)	Failure to notify the Commissioner of Data Protections of any amendments in personal data operations	$5,000