DATA PROTECTION LAW

DIFC LAW No.9 of 2004

CONTENTS

PART 1: GENERAL

1. **Title**

This Law may be cited as the “Data Protection Law 2004".

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.

5. **Application of the Law**

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

6. **Administration of the Law**

This Law and any legislation made for the purpose of this Law is administered by the DFSA.

PART 2: GENERAL RULES ON THE PROCESSING OF PERSONAL DATA

7. **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.

8. **Requirements for legitimate Processing**

Personal Data may only be processed if:

(a) the Data Subject has unambiguously given his consent;

(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 or in the exercise of DFSA 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.

9. **Processing of Sensitive Personal Data**

(1) Sensitive Personal Data shall not be processed unless:

(a) the Data Subject has given his explicit consent to the Processing of that Personal Data;

(b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment law;

(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 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 auditing, accounting or anti-money laundering obligations that apply to a Data Controller; or

(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 are processed by a health professional subject under national laws or Rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

(2) Article 9(1) shall not apply if:

(a) a permit has been obtained to process Sensitive Personal Data from the DFSA; and

(b) Data Controller applies adequate safeguards with respect to the processing of the Personal Data.

(3) The Regulatory Appeals Committee has jurisdiction to hear and determine any appeal in relation to a decision of the DFSA to refuse to issue a permit to process Sensitive Personal Data.

10. **Transfers out of the DIFC - adequate level of protection**

(1) Subject to Article 11, a transfer of Personal Data to a Recipient located in a jurisdiction outside the DIFC may take place only if an adequate level of protection for that Personal Data is ensured by laws and Rules that are applicable to the Recipient.

(2) The adequacy of the level of protection ensured by laws and regulations to which the Recipient is subject as referred to in Article 10(1) shall be assessed in the light of all the circumstances surrounding a Personal Data transfer operation or set of Personal Data transfer operations, including, but not limited to:

(a) the nature of the data;

(b) the purpose and duration of the proposed Processing operation or operations;

(c) if the data does not emanate from the DIFC, the country of origin and country of final destination of the personal data; and

(d) any relevant laws to which the recipient is subject, including professional rules and security measures.

11. **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 10 (1) may take place on condition that:

(a) the DFSA has granted a permit 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 unambiguous 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;

(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 auditing, accounting or anti-money laundering obligations that apply to a Data Controller which is established in the DIFC.

(2) The Regulatory Appeals Committee has jurisdiction to hear and determine any appeal in relation to a decision by the DFSA to refuse to issue a permit referred to in Article 11(1)(a).

12. **Providing information where 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 9(1)(g) or Article 11(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.

13. **Providing information where 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 recording of Personal Data or if a disclosure to a Third Party is envisaged, no later than the time when the Personal Data is first recorded 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 9(1)(g) or Article 11(1)(i).

(2) Article 13(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.

14. **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.

15. **Security of Processing**

(1) The Data Controller must implement appropriate technical and organisational measures to protect Personal Data against 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 9 or Article 11 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.

PART 3: RIGHTS OF DATA SUBJECTS

16. **Right to access to and rectification, erasure or blocking of Personal Data**

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.

17. **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 DFSA

18. **Requirement to notify to the DFSA**

(1) A Data Controller must establish and maintain a record of all wholly or partly automatic Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.

(2) The Council of the DFSA may make Rules prescribing:

(a) the information in relation to Personal Data Processing operations that must be recorded for the purposes of Article 18(1);

(b) the circumstances in which a Data Controller must notify the DFSA of any operations referred to in Article 18(1); and

(c) the content of any such notification.

19. **Register of notifications**

The DFSA shall keep a register of Personal Data Processing operations notified in accordance with Article 18.

PART 5: THE DFSA

20. **General Powers of the DFSA**

(1) The DFSA has such functions and powers as may be conferred or expressed to be conferred on it, by or under this Law.

(2) Without limiting the generality of Article 20(1), such powers and functions of the DFSA include the powers and functions, so far as are reasonably practicable, to:

(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) prescribe forms to be used for any of the purposes of this Law;

(d) to issue warnings or admonishments and make recommendations to Data Controllers; and

(e) bring contraventions of the Law to the attention of the Court.

21. **Production of information**

(1) The DFSA 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 21(1) shall comply with that requirement.

PART 6: COUNCIL OF THE DFSA

22. Power to make Rules

(1) The Council of the DFSA may make Rules in respect of any matters related to the Processing of Personal Data.

(2) In particular, the Council of the DFSA when exercising the power in Article 22(1) may make Rules in respect of:

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

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

(c) the conduct of the DFSA and his officers, employees and agents in relation to the exercise of powers and performance of functions.

(3) Where the Council of the DFSA issues a standard or code of practice, the Council of the DFSA may incorporate such a standard or code into the Rules by reference and in such circumstances, except to the extent that the Rules 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 Rules.

(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 Council of the DFSA shall publish draft Rules by means of a notice under Article 22(6).

(6) The notice of draft Rules must include the following:

(a) the draft text of the Rules;

(b) a statement of the substance and purpose of the material provisions of the draft Rules; and

(c) a summary of the draft Rules.

(7) Upon publication of a notice under Article 22(6), the Council of the DFSA shall invite interested persons to make representations with respect to the draft Rules within a period of at least 30 days after the publication, or within such period as the Council may otherwise determine.

(8) Articles 22(5), (6) and (7) shall not apply if the Council of the DFSA 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 Council of the DFSA invites interested persons to make representations with respect to draft Rules prior to Article 22 coming into effect shall be deemed to count as part or all of the period referred to in Article 22(7).

PART 7: REMEDIES, LIABILITY AND SANCTIONS

23. Directions

(1) If the DFSA is satisfied that a Data Controller has contravened or is contravening the Law or Rules made for the purpose of the Law, the DFSA may issue a direction to the Data Controller 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) A direction issued under Article 23(1) shall contain:

(a) a statement of the contravention of the Law or Rules which the DFSA 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 DFSA to issue the direction.

24. Lodging claims and mediation

(1) A person who believes on reasonable grounds that he has been adversely affected by a contravention of the Law in respect of the Processing of their Personal Data and as

regards the exercise of their rights under Articles 16 and 17 may lodge a claim with the DFSA.

(2) The DFSA may mediate between the affected Data Subject referred to in Article 24(1) and the relevant Data Controller.

(3) On the basis of the mediation referred to in Article 24(2), the DFSA may issue a direction requiring the Data Controller to do any act or thing.

(4) A Data Controller shall comply with any direction issued by the DFSA under Article 24(3).

PART 8: GENERAL EXEMPTIONS

25. General exemptions

(1) The Council of the DFSA may make Rules exempting Data Controllers from compliance with this Law or any parts of this Law.

(2) Without prejudice to Article 25(1), Articles 12 and 13 shall not apply to the DFSA or Company Registrar if the application of these Articles would be likely to prejudice the proper discharge by those entities of their functions insofar as such 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 financial 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.

SCHEDULE 1

INTERPRETATION

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.

(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.9 of 2004 made by the Ruler;

(e) the Rules are legislation made by the Council of the DFSA for the purposes of this Law and are binding in nature; and

(f) Guidance is indicative and non-binding and may comprise (i) guidance made and issued by the Registrar for the purposes of this Law; and (ii) any standard or code of practice issued by the Council of the DFSA which has not been incorporated into the Rules.

3. **Defined Terms**

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

Terms	Definitions
Council of the DFSA	the governing body of the DFSA established under Chapter 2 of Part 2 of the Regulatory Law and as constituted from time to time under that Law.
Court	the DIFC Court as established under Dubai Law.

Terms	Definitions
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	shall mean the individual to whom Personal Data relates.
DFSA	the DIFC Financial Services Authority.
DIFC	the Dubai International Financial Centre.
Filing System	any structured set of Personal Data which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
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 physical, physiological, mental, economic, cultural or social identity.
Law	the Data Protection Law 2004.
Personal Data	any information relating to an identified natural person or Identifiable Natural Person.
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.

Terms	Definitions
Regulatory Appeals Committee	a standing committee of the Council, established under and governed by Chapter 4 of Part 2 of the Regulatory Law 2004 and includes a sub-committee constituted under Article 29 of the Regulatory Law 2004.
Rules	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, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life.
Third Party	shall mean 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.

SCHEDULE 2

THIS LAW HAS BEEN DRAFTED TAKING INTO CONSIDERATION:

(A) the Recommendation of the Council of the Organisation for Economic Co-operation and Development (OECD) concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980;

(B) the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 by the member States of the Council of Europe signatory thereto (ETS No. 108) and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder Personal Data flows of 8 November 2001 (ETS No.: 181); and

(C) the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such Personal Data (Official Journal L 281, 23/11/1995 p. 0031-0050);

(D) the right to privacy as provided for in (i) Article 12 of the Universal Declaration of Human Rights, adopted and proclaimed by resolution 217 A (III) of the General Assembly of the United Nations of 10 December 1948, (ii) Article 17 of the International Covenant on Civil and Political Rights adopted and opened for signature, ratification and accession by resolution 2200A (XXI) of the General Assembly of the United Nations of 16 December 1966 and (iii) Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe of 20 March 1952;

AND CONSIDERING:

(1) it is desirable to adopt rules on the fair and lawful Processing of Personal Data by regulated entities, public authorities, agencies and other bodies and legal entities falling under the jurisdiction of the Dubai International Financial Centre as created under Dubai Law and

(2) the rules on the fair and lawful Processing of Personal Data are principally intended to govern the Processing of Personal Data of natural persons who are clients of natural persons, companies, organisations, partnerships, unincorporated associations, trusts, public authorities, agencies and other bodies and legal entities which fall under the jurisdiction of the Dubai International Financial Centre, but should also cover the Processing of Personal Data of employees of such natural persons, companies, organisations, partnerships, unincorporated associations, trusts, public authorities, agencies and other bodies and legal entities.