DATA PROTECTION LAW

DIFC LAW NO. 5 OF 2020

CONTENTS

PART 1: INTRODUCTION AND SCOPE

1. Title and repeal

(1) This Law may be cited as the "Data Protection Law 2020".

(2) This Law repeals and replaces the Data Protection Law, being Law No. 1 of 2007, as it was in force immediately prior to the commencement of this Law ("the Previous Law"), and all Regulations made under the Previous Law from commencement of this Law.

(3) Except where otherwise provided in this Law, anything done or omitted to be done pursuant to or for the purposes of the Previous Law is deemed to be done or omitted to be done pursuant to or for the purposes of this Law.

(4) Without limiting the generality of Article 1(3) and Article 4, and subject only to Article 1(5), such repeal and replacement shall not affect:

(a) any right, privilege, remedy, obligation or liability accrued to or incurred by any person; or

(b) any investigation, legal or administrative proceeding commenced, or to be commenced, in respect of any such right, remedy, obligation or liability,

under the Previous Law, and any such legal proceeding shall be instituted, continued or enforced, including any penalty, fine or forfeiture, under this Law.

(5) Where there is no equivalent provision in this Law to a provision in the Previous Law, a relevant provision of the previous Law is deemed to survive the repeal and replacement under this Article 1 until such time as necessary for the purpose of any investigation, legal or administrative proceedings specified in Article 1(4)(b).

(6) Unless otherwise provided, any reference to the Previous Law includes Regulations made under the Previous Law.

2. Legislative authority

This Law is made by the Ruler.

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 1 July 2020.

5. Purpose of this Law

The purpose of this Law is to:

(a) provide standards and controls for the Processing and free movement of Personal Data by a Controller or Processor; and

(b) protect the fundamental rights of Data Subjects, including how such rights apply to the protection of Personal Data in emerging technologies.

6. Application of the Law

(1) This Law applies in the jurisdiction of the DIFC.

(2) This Law applies to the Processing of Personal Data:

(a) by automated means; and

(b) other than by automated means where the Personal Data forms part of a Filing System or is intended to form part of a Filing System.

(3) This Law applies as follows:

(a) This Law applies to the Processing of Personal Data by a Controller or Processor incorporated in the DIFC, regardless of whether the Processing takes place in the DIFC or not.

(b) This Law applies to a Controller or Processor, regardless of its place of incorporation, that Processes Personal Data in the DIFC as part of stable arrangements, other than on an occasional basis. This Law applies to such Controller or Processor in the context of its Processing activity in the DIFC (and not in a Third Country), including transfers of Personal Data out of the DIFC.

(c) For the purposes of this Article 6(3), Processing "in the DIFC" occurs when the means or personnel used to conduct the Processing activity are physically located in the DIFC, and Processing "outside the DIFC" is to be interpreted accordingly.

(4) This Law does not apply to the Processing of Personal Data by natural persons in the course of a purely personal or household activity that has no connection to a commercial purpose.

(5) This Law is without prejudice to agreements entered into between one (1) or more DIFC Bodies and:

(a) Third Country governments or governmental authorities;

(b) regulatory bodies or public authorities established under the law of a Third Country; or

(c) International Organisations,

that address regulating the transfer of Personal Data and include appropriate safeguards for the relevant Data Subjects.

7. Schedules

Schedule 1 contains:

(a) interpretative provisions that apply to this Law; and

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

8. Administration of the Law

This Law and any Regulations made under it are administered by the Commissioner.

PART 2: GENERAL REQUIREMENTS

Part 2A: Requirements for legitimate and lawful Processing

9. General requirements

(1) Personal Data shall be:

(a) Processed in accordance with Article 10;

(b) Processed lawfully, fairly and in a transparent manner in relation to a Data Subject;

(c) Processed for specified, explicit and legitimate purposes determined at the time of collection of Personal Data;

(d) Processed in a way that is not incompatible with the purposes described in Article 9(1)(c);

(e) relevant and limited to what is necessary in relation to the purposes described in Article 9(1)(c);

(f) Processed in accordance with the application of Data Subject rights under this Law;

(g) accurate and, where necessary, kept up to date, including via erasure or rectification, without undue delay;

(h) kept in a form that permits identification of a Data Subject for no longer than is necessary for the purposes described in Article 9(1)(c); and

(i) kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) A Controller or Processor shall be responsible for, and must be able to demonstrate to the Commissioner its compliance with, Article 9(1).

10. Lawfulness of Processing

(1) Any one (1) or more of the following shall constitute a lawful basis for Processing Personal Data:

(a) a Data Subject has given consent, which complies with Article 12, to the Processing of that Personal Data for specific purposes;

(b) Processing is necessary for the performance of a contract to which a Data Subject is a party, or in order to take steps at the request of a Data Subject prior to entering into such contract;

(c) Processing is necessary for compliance with Applicable Law that a Controller is subject to;

(d) Processing is necessary in order to protect the vital interests of a Data Subject or of another natural person;

(e) Processing is necessary for:

(i) performance of a task carried out by a DIFC Body in the interests of the DIFC;

(ii) exercise of a DIFC Body's powers and functions; or

(iii) the exercise of powers or functions vested by a DIFC Body in a Third Party to whom Personal Data is disclosed by the DIFC Body; or

(f) Processing is necessary for the purpose of legitimate interests pursued by a Controller or a Third Party to whom the Personal Data has been made available, subject to Article 13, except where such interests are overridden by the interests or rights of a Data Subject.

Part 2B: Processing of Special Categories of Personal Data

11. Processing of Special Categories of Personal Data

In addition to general obligations set out in Article 9 and lawful Processing in accordance with a basis set out in Article 10, and regardless of the Controller's other Processing obligations, Special Categories of Personal Data shall not be Processed unless one (1) or more of the following applies:

(a) a Data Subject has given explicit consent that complies with Article 12, to the Processing of those Special Categories of Personal Data for one (1) or more specified purposes;

(b) Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of a Controller or a Data Subject in the context of the Data Subject's employment, including but not limited to recruitment, visa or work permit processing, the performance of an employment contract, termination of employment, the conduct of proceedings relating to employment and the administration of a pension, retirement or employee money purchase benefit scheme;

(c) Processing is necessary to protect the vital interests of a Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent;

(d) Processing is carried out by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities, subject to appropriate assurances and provided that the Processing relates:

(i) solely to the members or former members of such an entity; or

(ii) to other persons who have regular contact with such a body in connection with its purpose,

and the Personal Data is not disclosed to a Third Party without the consent of a Data Subject;

(e) Processing relates to Personal Data that has been made public by a Data Subject;

(f) Processing is necessary for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognised alternative dispute resolution procedures, such as mediation) or is performed by the Court acting in its judicial capacity;

(g) Processing is necessary for compliance with a specific requirement of Applicable Law to which a Controller is subject, and in such circumstances the Controller must provide a Data Subject with clear notice of such Processing as soon as reasonably practicable unless the obligation in question prohibits such notice being given;

(h) Processing is necessary to comply with Applicable Law that applies to a Controller in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime;

(i) Processing is required for the purposes of preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or the treatment or the management of health or social care systems and services, provided that the Personal Data is processed by or under the responsibility of a health professional subject to an obligation of professional secrecy under Applicable Law or by another person also subject to an obligation of secrecy under Applicable Law;

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

(k) Processing is proportional and necessary to protect a Data Subject from potential bias or inaccurate decision making, where such risk would be increased regardless of whether Special Category Personal Data is Processed.

(l) Processing is necessary for Substantial Public Interest reasons that are proportionate to the aim(s) pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the rights of the Data Subject.

Part 2C: Conditions of consent and reliance on legitimate interests

12. Consent

(1) Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent if it is to be relied on as a basis for Processing under Article 10(1)(a) or under Article 11(1)(a). If the performance of an act by a Controller, a Data Subject or any other party, (including the performance of contractual obligations), is conditional on the provision of consent to Process Personal Data, then such consent will not be considered to be freely given with respect to any Processing that is not reasonably necessary for the performance of such act or where the consent relates to excessive categories of Personal Data.

(2) Where Processing is based on consent, a Controller must be able to demonstrate that consent has been freely given.

(3) If the Processing is intended to cover multiple purposes, consent must be obtained for each purpose in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language.

(4) If a Controller seeks to obtain consent for one (1) or more other matters not expressly concerned with the Processing of Personal Data, the request for consent for the Processing of Personal Data must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(5) A Data Subject may withdraw consent at any time in accordance with the right afforded to Data Subjects under Article 32. A Data Subject must be informed of this right and how to exercise it as set out in Article 40 at the time consent is obtained. Withdrawing consent should not require undue effort on the part of the Data Subject and should be at least as easy as the process of giving consent. Withdrawal of consent does not affect the lawfulness of Processing carried out before the date of withdrawal. Where consent is withdrawn a Controller must comply with Article 3232(3).

(6) Other than for the purpose of a Single Discrete Incident, where a Controller relies on a Data Subject's consent for Processing, the Controller should implement appropriate and proportionate measures to assess the ongoing validity of the consent. This includes considering whether the Data Subject, acting reasonably, would expect Processing to continue based on the consent given, taking into account the circumstances and the terms of such consent.

(7) Where such ongoing assessment conducted in accordance with Article 12(6) concludes that a Data Subject would no longer reasonably expect the Processing to be continuing, he must be contacted without delay and asked to re-affirm consent.

(8) In the circumstances referred to in Article 12(7), consent shall be deemed to be withdrawn if there is no positive act of re-affirmation of consent within a reasonable period after a Data Subject has been contacted.

(9) A Controller must be able to demonstrate to the Commissioner that appropriate methods and procedures are in place to manage the recording of consent and the withdrawal of consent, and that periodic evaluations of the same are conducted.

(10) Where Processing is not a Single Discrete Incident and continues on the basis of consent, a Data Subject should be given the opportunity to re-affirm or withdraw consent on a periodic basis.

(11) A "Single Discrete Incident" means a Processing operation or a collection of Processing operations that relate to a:

(a) single, non-recurring transaction; or

(b) non-recurring and clearly defined purpose that a Data Subject is seeking to achieve,

in each case, with a definable end point.

(12) For the avoidance of doubt, consent given for Processing to perform a Single Discrete Incident remains subject to all foregoing provisions of this Article except for Article 12(6) and Article 12(10).

13. Legitimate interests

(1) A public authority subject to DIFC law may not rely on the basis of legitimate interests under Article 10(1)(f) to Process Personal Data.

(2) A Controller that is part of a Group may have a legitimate interest in transferring Personal Data within its Group for internal administrative purposes.

(3) Processing of Personal Data shall be considered a legitimate interest of a Controller if it is necessary and proportionate to prevent fraud or ensure network and information security.

Part 2D: General requirements

14. Accountability and notification

(1) A Controller or Processor is required to establish a program to demonstrate compliance with this Law, the level and detail of which will depend on the scale and resources of the Controller or the Processor, the categories of Personal Data being Processed and the risks to the Data Subjects.

(2) A Controller or Processor is required to implement appropriate technical and organisational measures to demonstrate that Processing is performed in accordance with this Law, including:

(a) taking into account:

(i) the nature, scope, context and purpose of the Processing;

(ii) the risks presented by the Processing to a relevant Data Subject; and

(iii) prevailing information security good industry practice.

(b) ensuring a level of security:

(i) appropriate to the risks associated with Processing, taking account of any wilful, negligent, accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of or access to Personal Data; and

(ii) against all other unlawful forms of Processing;

(c) ensuring that, by default, only Personal Data necessary for each specific purpose is Processed. This obligation applies to the amount and type of Personal Data collected, the extent of the Processing, the period of storage and accessibility; and

(d) reviewing and updating such measures where necessary to reflect legal, operational and technical developments.

(3) A Controller or Processor shall integrate necessary measures into the Processing in order to meet the requirements of this Law, protect a Data Subject's rights and follow the principle of "data protection by design and by default", which shall at least require assurances that:

(i) Processing is designed to reinforce data protection principles such as data minimisation at the time of determining the means for Processing and at the time of Processing itself; and

(ii) by default, only Personal Data that is necessary for each specific purpose is Processed, and that Personal Data is not made accessible to an indefinite number of persons without the Data Subject's intervention.

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

(a) prompted to actively select his privacy preferences on first use; and

(b) able to easily change such preferences.

(5) A Controller or Processor that collects or Processes Personal Data shall implement and maintain a data protection policy in writing that is:

(a) proportionate to the extent and type of Processing of Personal Data undertaken; and

(b) consistent with this Law.

(6) Notwithstanding Article 14(5), any person that can demonstrate adherence to approved codes of conduct under Article 48 or approved certification schemes under Article 50 has complied with the obligations in this Article 14.

(7) A Controller or Processor shall register with the Commissioner by filing a notification of Processing operations, which shall be kept up to date through amended notifications.

(8) Notifications referred to in Article 14(7) shall be:

(a) kept on a publicly available register maintained by the Commissioner; and

(b) accompanied by such fee as may be prescribed in Regulations made by the DIFCA Board of Directors.

15. Records of Processing activities

(1) A Controller shall maintain a written record, which may be in electronic form, of Processing activities under its responsibility, which shall contain at least the following information:

(a) name and contact details of the Controller, its appointed DPO, where applicable, and Joint Controller, if any;

(b) the purpose(s) of the Processing;

(c) a description of the categories of Data Subjects;

(d) a description of the categories of Personal Data;

(e) categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in Third Countries and International Organisations;

(f) where applicable, the identification of the Third Country or International Organisation that the Personal Data has or will be transferred to and, in the case of transfers under Article 27, the documentation of suitable safeguards;

(g) where possible, the time limits for erasure of the different categories of Personal Data; and

(h) where possible, a general description of the technical and organisational security measures referred to in Article 14(2).

(2) A Processor shall maintain a written record of all categories of Processing activities carried out on behalf of a Controller containing the information specified in Article 15(1).

(3) The DIFCA Board of Directors may make Regulations on the procedures relating to recording of Processing activities under this Article 15.

16. Designation of the DPO

(1) A Controller or Processor may elect to appoint a DPO that meets the requirements of Article 17.

(2) Notwithstanding Article 16(1), a DPO shall be appointed by:

(a) DIFC Bodies, other than the Courts acting in their judicial capacity; and

(b) a Controller or Processor performing High Risk Processing Activities on a systematic or regular basis.

(3) A Controller or Processor to which Article 16(2)(b) does not apply may be required to designate a DPO by the Commissioner.

(4) If a Controller or Processor is not required to appoint a DPO, it shall clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations under this Law, or any other applicable data protection law, within its organisation and be able to provide details of the persons with such responsibility to the Commissioner upon request.

(5) The role of a DPO may be performed by a member of a Controller's or Processor's staff, an individual employed within a Controller's or Processor's Group in accordance with Article 16(6) or by a third party under a service contract.

(6) A Group may appoint a single DPO provided that he is easily accessible from each entity in the Group.

(7) A DPO must reside in the UAE unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis.

(8) A Controller or Processor shall publish the contact details of its DPO in a manner that is readily accessible to third parties, such that a third party could determine how to contact the DPO without disproportionate effort. On request, a Controller or Processor shall confirm identity of its DPO to the Commissioner in writing.

17. The DPO: competencies and status

(1) A DPO must have knowledge of this Law and its requirements and shall ensure a Controller or Processor monitors compliance with this Law.

(2) A DPO must:

(a) have the ability to fulfil the tasks in Article 18;

(b) be able to perform his duties and tasks in an independent manner, and be able to act on his own authority;

(c) have direct access and report to senior management of the Controller or Processor;

(d) have sufficient resources to perform his duties in an effective, objective and independent manner; and

(e) have timely and unrestricted access to information within the Controller or Processor organisation to carry out his duties and responsibilities under this Law.

(3) Without prejudice to the mandatory notification requirements under this Law, a DPO shall be transparent and cooperative with the Commissioner and shall notify the Commissioner of all relevant information within the Controller or Processor organisation, other than information that is subject to legal privilege or a conflicting obligation of non-disclosure under Applicable Law.

(4) Subject to Article 18(1)(c), a DPO may hold other roles or titles within a Controller or Processor or within each such Group, and may fulfil additional tasks and duties other than those described in this Law.

18. Role and tasks of the DPO

(1) A Controller or Processor shall ensure that:

(a) its DPO is properly involved in a timely manner, on all issues relating to the protection of Personal Data and is given sufficient resources necessary to carry out the role;

(b) its DPO is free to act independently; and

(c) any additional tasks and duties fulfilled by its DPO, other than those required under this Law, do not result in a conflict of interest or otherwise prevent the proper performance of the role of the DPO.

(2) A Data Subject may contact the DPO of a Controller or Processor with regard to all issues related to Processing of his Personal Data and to the exercise of his rights under this Law.

(3) A DPO shall perform at least the following tasks:

(a) monitor a Controller or Processor's compliance with:

(i) this Law;

(ii) any other data protection or privacy-related laws or regulations to which the organisation is subject within the DIFC; and

(iii) any policies relating to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in Processing operations, and the related audits;

(b) inform and advise a Controller or Processor and its employees who carry out Processing of its obligations pursuant to this Law and to other data protection provisions, including where the organisation is subject to overseas provisions with extra-territorial effect;

(c) provide advice where requested in relation to data protection impact assessments undertaken pursuant to Article 20;

(d) cooperate with the Commissioner in accordance with Article 17(3);

(e) act as the contact point for the Commissioner on issues relating to Processing; and

(f) receive and act upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued or made by the Commissioner.

19. DPO Controller assessment

(1) Where a Controller is required to appoint a DPO under Articles 16(2) or 16(3), the DPO shall undertake an assessment of the Controller's Processing activities, at least once per year ("the Annual Assessment"), which shall be submitted to the Commissioner.

(2) A Controller shall report on its Processing activities in the Annual Assessment and indicate whether it intends to perform High Risk Processing Activities in the following annual period.

(3) The Commissioner shall prescribe and make publically available the format, required content and deadline for submission of Annual Assessments.

20. Data protection impact assessment

(1) Prior to undertaking High Risk Processing Activities a Controller shall carry out an assessment of the impact of the proposed Processing operations on the protection of Personal Data, considering the risks to the rights of the Data Subjects concerned. A Controller may also elect to carry out such assessment in relation to the Processing of Personal Data that is not a High Risk Processing Activity.

(2) A single assessment may address a set of similar Processing operations that present similar risks. If another member of a Controller's Group has conducted a data protection impact assessment, complying with the requirements of Article 20(6), in relation to substantially the same Processing that remains current and accurate, the Controller may rely on such data protection impact assessment for the purpose of this Article 20.

(3) A DPO, where appointed, shall be responsible for overseeing data protection impact assessments.

(4) The Commissioner may at his discretion publish a non-exhaustive list of types or categories of Processing operations that are considered to be High Risk Processing Activities. Such a list is not intended to be exhaustive and does not absolve a Controller from responsibility for complying with this Law in all respects with regard to High Risk Processing Activities.

(5) The Commissioner may also publish a list of the types or categories of Processing operations for which no data protection impact assessment is required.

(6) A data protection impact assessment shall contain at least:

(a) a systematic description of the foreseen Processing operations and the purpose(s) of the Processing, including, where applicable, the legitimate interest pursued by a Controller;

(b) an assessment of the necessity and proportionality of the Processing operations in relation to the purpose(s);

(c) identification and consideration of the lawful basis for the Processing, including:

(i) where legitimate interests are the basis for Processing, an analysis and explanation of why a Controller believes the interests or rights of a Data Subject do not override its interests; and

(ii) where consent is the basis for Processing, validation that such consent is validly obtained, consideration of the impact of the withdrawal of consent to such

Processing and of how a Controller will ensure compliance with the exercise of a Data Subject's right to withdraw consent;

(d) an assessment of the risks to the rights of Data Subjects; and

(e) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Law, taking into account the rights and legitimate interests of Data Subjects and other concerned persons.

(7) In assessing the impact of the Processing operations, compliance with approved codes of conduct referred to in Article 48 by a Controller or Processor shall be taken into account.

(8) Taking into account protection of commercial or public interests or the security of Processing operations, a Controller shall seek the input of Data Subjects or their representatives on the intended Processing, where appropriate.

(9) A new data protection impact assessment is not required unless Applicable Law requires that it is necessary to carry out such an assessment prior to undertaking Processing activities, where:

(a) Processing pursuant to Articles 10(1)(c) or 10(1)(e) has a lawful basis in Applicable Law to which a Controller is subject;

(b) Applicable Law regulates the specific Processing operation or set of operations in question; and

(c) a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that lawful basis.

(10) A Controller shall carry out a review to assess if Processing is performed in accordance with a data protection impact assessment:

(a) on a regular basis, proportionate to the extent and type of Processing the Controller conducts; or

(b) when there is a change in the risk related to the Processing operations.

(11) A Processor appointed, or in the process of being appointed, by a Controller to carry out a Processing activity shall assist the Controller by providing all information reasonably requested by the Controller in connection with the relevant data protection impact assessment.

21. Prior consultation

(1) A Controller shall consult the Commissioner where a data protection impact assessment under Article 20 indicates that, despite taking the measures referred to in Article 20(6)(e), the risks to the rights of Data Subjects remain particularly high and the Controller has already carried out or wishes to commence or continue carrying out a Processing activity.

(2) Where the Commissioner determines that a Processing activity referred to in Article 21(1) would or does breach this Law, the Commissioner shall provide written confirmation to the Controller and, where applicable, to the Processor, and may also use any of the powers referred to in Article 46.

(3) A Controller may consult with the Commissioner before commencing a Processing activity. A Controller is not prohibited from commencing a Processing activity before or during a consultation period where there is insufficient time to complete such consultation in advance and there is a pressing business need to commence Processing, provided it is not likely to override the vital interests of Data Subjects whose Personal Data is being Processed. Such Processing shall comply

with the Law at all times and the Controller shall remain liable for breaches of the Law prior to or during the consultation period.

(4) If the Commissioner makes a direction with respect to a Processing activity as a result of a consultation then a Controller shall implement such directions without delay including, if so directed, discontinuing the Processing activity.

(5) A Controller's decision regarding a consultation will be taken into account by the Commissioner when considering any applicable sanctions under this Law. Where Processing is determined to be in violation of the Law, a failure to consult with the Commissioner may result in the application of more severe penalties.

(6) A Controller may complete a data protection impact assessment or carry out prior consultation with other Controllers or Joint Controllers (as applicable), including where multiple Controllers wish to use a new technology or platform, or where there is an innovation in a particular industry that changes the way Personal Data is Processed.

(7) The Commissioner shall endeavour to provide its written confirmation within four (4) weeks of the beginning of the consultation period, but may notify a relevant Controller that the time period is being extended by up to a further four (4) weeks where the Processing in question is particularly complex.

(8) Where the Commissioner determines that the Processing is unlawful, a relevant Controller or Processor shall cease all such Processing immediately, unless otherwise directed by the Commissioner.

(9) When consulting with the Commissioner pursuant to Article 21(1), a Controller shall provide the Commissioner with:

(a) where applicable, its respective responsibilities and those of any Joint Controllers and Processors involved in the Processing, in particular for Processing within a Group;

(b) the purposes and means of the intended Processing;

(c) the measures and safeguards provided to protect the rights of Data Subjects pursuant to this Law;

(d) where applicable, the contact details of its DPO;

(e) the relevant data protection impact assessment; and

(f) any other information requested by the Commissioner.

(10) A Processor appointed, or in the process of being appointed, by a Controller to carry out a Processing activity shall assist the Controller in any prior consultation process with the Commissioner.

22. Cessation of Processing

(1) Where the basis for Processing changes, ceases to exist or a Controller is required to cease Processing due to the exercise of a Data Subject's rights, the Controller shall ensure that all Personal Data, including Personal Data held by Processors is:

(a) securely and permanently deleted;

(b) anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released;

(c) pseudonymised;

(d) securely encrypted; or

(2) Where a Controller is unable to ensure that Personal Data is securely and permanently deleted, anonymised, pseudonynmised or securely encrypted, the Personal Data must be archived in a manner that ensures the data is put beyond further use.

(3) "Put beyond further use" in Article 22(2) means that:

(a) a Controller and a relevant Processor is unable to use the Personal Data to inform any decision with respect of the Data Subject or in a manner that affects the Data Subject in any way, other than where such Personal Data needs to be cross-checked by automated means solely in order to prevent further Processing of Personal Data related to the Data Subject;

(b) no party has access to the Personal Data other than the Controller and any relevant Processor;

(c) Personal Data is protected by appropriate technical and organisational security measures that are equivalent to those afforded to live Personal Data; and

(d) a Controller and any relevant Processor have in place and must comply with a strategy for the permanent deletion, anonymisation, pseudonymisation or secure encryption of the Personal Data, complies and can demonstrate compliance with such policy.

(4) Notwithstanding Article 22(1), a Controller and any relevant Processor is not required to securely and permanently delete, anonymise, pseudonymise or encrypt Personal Data or put it beyond further use, where such Personal Data:

(a) is necessary for the establishment or defence of legal claims or must be retained for compliance with Applicable Law; or

(b) is being used in scientific research activity conducted in the public interest or in the interests of the DIFC in accordance with all Applicable Laws, in a manner that does not present risks to the rights of Data Subjects; or

(c) is part of a dataset used to lawfully train or refine an artificial intelligence system in a manner that does not present risks to a Data Subject's rights.

(5) A Controller or Processor seeking to rely on Articles 22(4)(b) or 22(4)(c) shall conduct a data protection impact assessment in accordance with Article 20 before doing so. Any Processing of Personal Data in accordance with Article 22(4) must be limited to the extent necessary for such purposes.

(6) A Controller or Processor shall have a policy and process for managing Personal Data that is subject to Article 22(4) when the grounds for retention no longer apply, and shall securely and permanently delete, anonymise, pseudonymise, encrypt Personal Data or to put it beyond further use when such grounds no longer apply.

PART 3: JOINT CONTROLLERS AND PROCESSORS

Part 3A: Joint Controllers

23. Joint Controllers

(1) Where two (2) or more persons jointly determine the purposes and means of Processing Personal Data, they shall be Joint Controllers.

(2) Joint Controllers shall, by way of legally binding written agreement, define their respective responsibilities for ensuring compliance with the obligations under this Law. Such agreement shall clarify the process for ensuring that a Data Subject can exercise his rights under this Law and for providing a Data Subject with the information referred to in Articles 29 and 30.

(3) The written agreement referred to in Article 23(2) or an appropriate summary shall be made available to an affected Data Subject.

(4) Notwithstanding the terms of any written agreement between the Joint Controllers, they shall remain responsible for all Controller obligations under this Law and the Data Subject's rights may be exercised under this Law in respect of and against each of the Joint Controllers.

Part 3B: Processors

24. Processors and Sub-processors

(1) Where Processing is to be carried out on behalf of a Controller by a Processor, the Processing shall be governed by a legally binding written agreement between the Controller and the Processor. A Controller shall only enter into agreements with Processors that provide sufficient assurances to implement appropriate technical and organisational measures that ensure the Processing meets the requirements of this Law and protects a Data Subject's rights.

(2) A Processor may not engage another Processor to act as a Sub-processor without the prior written authorisation of a Controller. A Controller may only give a general written authorisation where it has ensured that conditions are in place to enable appointed Sub-processors (present or future) to provide the assurances under Article 24(1). If a general written authorisation has been given, a Processor shall inform a Controller of any intended changes concerning the addition or replacement of a Sub-processor. A Processor shall take into account any good faith objection raised by a Controller to such intended changes.

(3) Subject to Article 24(2), a Processor may not engage a Sub-processor for carrying out specific Processing activities on behalf of the Controller, unless a legally binding written agreement containing the requirements set out in Article 24(5) is in place with such Sub-processor that ensures a full delegation of the obligations that the Processor owes to the Controller under the agreement with the Controller in respect of such specific Processing activities.

(4) Where a Sub-processor fails to fulfil its data protection obligations under an agreement or Applicable Law, the Processor that engaged it shall remain fully liable to a relevant Controller for the performance of the Sub-processor's obligations.

(5) Each agreement referred to in Articles 24(1) and 24(3):

(a) shall set out the:

(i) subject-matter and duration of the Processing;

(ii) nature and purpose of the Processing;

(iii) type of Personal Data and categories of Data Subjects; and

(iv) obligations and rights of the Controller; and

(b) must include commitments that each Processor and Sub-processor (if any) shall:

(i) Process Personal Data based on documented instructions from a Controller, including sharing of Personal Data in response to a request made by a Requesting Authority (as described in Article 28), or transfers of Personal Data to a Third Country or an International Organisation, unless required to do so by Applicable Law to which the Processor is subject;

(ii) where Applicable Law, as referred to in Article 24(5)(b)(i), applies:

(A) inform any relevant counterparty; or

(B) where there is a chain of Processors and Sub-processors, ensure that the Controller is notified, unless the Applicable Law in question prohibits such information being provided on grounds of Substantial Public Interest;

(iii) ensure that persons authorised to Process relevant Personal Data are under legally binding written agreements or duties of confidentiality;

(iv) take all measures required pursuant to Article 14;

(v) comply with the conditions referred to in Articles 24(2) and (3) for engaging any Sub-processor;

(vi) assist a relevant counterparty by providing appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights, having taken into account the nature of the Processing;

(vii) assist a relevant counterparty in ensuring the Controller's compliance with the obligations pursuant to Articles 14, 20, 21, 41 and 42, taking into account the nature of Processing and the information available to the Processor;

(viii) delete or return all Personal Data to the Controller, at the Controller’s option, or make the same available for return to a relevant counterparty after the end of the provision of services relating to Processing, and delete existing copies unless Applicable Law requires storage of the Personal Data;

(ix) make available to the Controller, relevant counterparty or the Commissioner (upon request) all necessary information to demonstrate compliance with the obligations in this Article 24; and

(x) permit and provide reasonable assistance with audits, including inspections, conducted by:

(A) a relevant counterparty;

(B) another auditor mandated by a relevant counterparty; or

(C) the Commissioner.

(6) A Processor or Sub-processor shall immediately inform the Controller or Processor (as applicable) whether, in its opinion, the Processing activity infringes this Law.

(7) Adherence by a Processor or Sub-processor to an approved code of conduct referred to in Article 48, or an approved certification mechanism referred to in Article 50, may demonstrate the sufficiency of the measures referred to in Articles 24(1) and 24(2).

(8) The Commissioner may publish standard contractual clauses for the matters referred to in Articles 24(1) and (3). The incorporation of such clauses in an applicable written agreement shall be sufficient to discharge the obligations in Articles 24(5)(b)(i) to 24(5)(b)(x) inclusive.

(9) If a Processor infringes this Law by determining the purposes and means of Processing, the Processor shall be considered to be a Controller in respect of that Processing and will assume all the responsibilities and obligations of a Controller.

(10) Both a Controller and Processor are in breach of this Law if they commence mutually agreed Processing activity without a written agreement referred to in Articles 24(1) and 24(3).

25. Confidentiality

A Controller or Processor, and where applicable, a Joint Controller or a Sub-processor, shall take steps to ensure that any person acting under its respective authority that has access to Personal Data shall not Process it except on the instructions of the Controller, unless it is required to do so under Applicable Law.

PART 4: DATA EXPORT AND SHARING

26. Transfers out of the DIFC: adequate level of protection

(1) Processing of Personal Data that involves the transfer of Personal Data from the DIFC to a Third Country or to an International Organisation may take place only if:

(a) an adequate level of protection for that Personal Data is ensured by Applicable Law, as set out in Articles 26(2) and (3), including with respect to onward transfers of Personal Data; or

(b) it takes place in accordance with Article 27.

(2) For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection, taking into account factors including:

(a) the rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights via administrative or judicial redress;

(b) the access of a public authority to Personal Data;

(c) the existence of effective data protection law, including rules on the onward transfer of Personal Data to a Third Country or International Organisation;

(d) the existence and functioning of one (1) or more independent, competent data protection or similar supervisory authorities with adequate enforcement powers; and

(e) international commitments and conventions binding on such Third Country or International Organisation and its membership of any multilateral or regional organisations.

(3) The Commissioner may, at his discretion, make such a determination that any Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection based on adequacy decisions made by other competent data protection authorities where such decisions have taken into account the same factors listed at Article 26(2)(a) to (e) above.

(4) The Commissioner shall pass Regulations to provide details of his determinations under Article 26(2) and 26(3).

(5) The Commissioner may repeal, amend or suspend the adequacy status of any Third Country, territory or one (1) or more specified sectors within a Third Country, or International Organisation determined under Article 26(2). In such circumstances, the Commissioner will issue amended Regulations if necessary.

(6) Processing in accordance with this Article 26 does not require any specific authorisation or notification to the Commissioner other than as required under any other provision of this Law which may apply to such Processing.

27. 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 Third Country or an International Organisation may take place on condition that:

(a) the Controller or Processor in question has provided appropriate safeguards (as described in Article 27(2)), and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available;

(b) one of the specific derogations in Article 27(3) applies; or

(c) the limited circumstances in Article 27(4) apply.

(2) The appropriate safeguards referred to in Article 27(1)(a) may be provided for by:

(a) a legally binding instrument between public authorities;

(b) Binding Corporate Rules, subject to Article 27(6);

(c) standard data protection clauses as adopted by the Commissioner in accordance with Regulations setting out a procedure for developing such clauses;

(d) an approved code of conduct pursuant to Article 48 together with binding and enforceable commitments of the Controller or Processor in the Third Country or the International Organisation to apply the appropriate safeguards, including regarding a Data Subject's rights; or

(e) an approved certification mechanism pursuant to Article 50 together with binding and enforceable commitments of the Controller or Processor in the Third Country or the International Organisation to apply the appropriate safeguards, including regarding Data Subjects' rights.

(3) The derogations referred to in Article 27(1)(b) are:

(a) a Data Subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between a Data Subject and Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract that is in the interest of a Data Subject between a Controller and a Third Party;

(d) the transfer is necessary for reasons of Substantial Public Interest;

(e) the transfer is necessary or legally required in the interests of the DIFC, including in the interests of the DIFC Bodies relating to the proper discharge of their functions;

(f) the transfer is necessary for the establishment, exercise or defence of a legal claim;

(g) the transfer is necessary in order to protect the vital interests of a Data Subject or of other persons where a Data Subject is physically or legally incapable of giving consent;

(h) the transfer is made in compliance with Applicable Law and data minimisation principles, set out in Article 9(1)(e), from a register that is:

(i) intended to provide information to the public; and

(ii) open for viewing either by the public in general or by any person who can demonstrate a legitimate interest;

(i) subject to Article 28, the transfer is:

(i) necessary for compliance with any obligation under Applicable Law to which the Controller is subject; or

(ii) made at the reasonable request of a regulator, police or other government agency or competent authority;

(j) subject to international financial standards, the transfer is necessary to uphold the legitimate interests of a Controller recognised in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subject's particular situation; or

(k) the transfer is necessary to comply with applicable anti-money laundering or counter-terrorist financing obligations that apply to a Controller or Processor or for the prevention or detection of a crime.

(4) Where a transfer could not be based on one of the provisions in this Article 27(1) to (3) or Article 26, such transfer to a Third Country or an International Organisation may take place only if:

(a) the transfer is not repeating or part of a repetitive course of transfers;

(b) concerns only a limited number of Data Subjects;

(c) is necessary for the purposes of compelling legitimate interests pursued by the Controller that are not overridden by the interests or rights of the Data Subject; and

(d) the Controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

(5) A Controller shall inform the Commissioner of any transfer made pursuant to Article 27(4) and shall, in addition to providing the information referred to in Articles 29 or 30, as applicable, inform the Data Subject of the transfer and the compelling legitimate interests.

(6) A public authority subject to DIFC law may not rely on Articles 27(3)(a), (b) and (c), or on Article 27(4).

(7) A Controller or Processor may rely on its existing Binding Corporate Rules subject to the following:

(a) relevant Binding Corporate Rules may only be used for lawful transfers within the Controller's or the Processor's respective Group (and, in the case of the Processor, only where permitted by the Controller); and

(b) relevant Binding Corporate Rules must have been reviewed and approved by the Commissioner.

(8) A Controller or Processor may make a request to the Commissioner for approval of its Binding Corporate Rules that have been approved by a competent data protection or similar supervisory authority in any jurisdiction to which Article 26(2) applies, and the Commissioner shall approve or reject such request, which shall include:

(i) a full copy of its Binding Corporate Rules and confirmation as to whether such Binding Corporate Rules have been approved by any competent data protection authority;

(ii) details of the transfers it intends to make or receive in reliance on the Binding Corporate Rules; and

(iii) where the Binding Corporate Rules operate on the basis that members of the Controller's or Processor's Group (including the Controller or Processor) will bind other members of the Group, such as by way of power of attorney, full evidence of all valid instruments necessary to create such powers to bind should also be provided.

(9) If a set of Binding Corporate Rules is amended at any time, a Controller or Processor shall provide a revised copy to the Commissioner without delay, in a form that clearly shows all edits. The Commissioner may approve or reject the revised Binding Corporate Rules. If the revised Binding Corporate Rules are rejected then the Controller or Processor may no longer rely on them.

(10) A Controller or Processor shall confirm in writing annually to the Commissioner that an approved set of Binding Corporate Rules remains in the same form and is used to facilitate the same transfers as approved.

(11) The Commissioner may provide guidance or make Regulations regarding the procedure for approving or rejecting and suggested contents of Binding Corporate Rules, and may require a Controller or Processor to provide evidence of any matter relating to Binding Corporate Rules.

28. Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

PART 5: INFORMATION PROVISION

29. Providing information where Personal Data has been obtained from the Data Subject

(1) A Controller shall provide a Data Subject from whom it collects Personal Data with at least the following information, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, at the time of collecting the Personal Data to enable the Data Subject to assess the implications of providing his Personal Data:

(a) the identity and contact details of the Controller;

(b) the contact details of the DPO, if applicable;

(c) the purposes of the Processing, as well as its lawful basis under this Law;

(d) if the Controller's lawful basis for the Processing is legitimate interests or compliance with any Applicable Law to which the Controller is subject, the Controller shall state clearly what those legitimate interests or compliance obligations are;

(e) the categories of Personal Data relating to the Data Subject that are being processed;

(f) the recipients or categories of recipients of the Personal Data;

(g) where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or International Organisation, or in the case of transfers referred to in Articles 27(1)(a), 27(2)(b) or 27(3)(b), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; and

(h) any further information in so far as such is necessary, having regard to the specific circumstances in which the Personal Data is collected, to ensure fair and transparent Processing in respect of the Data Subject, including:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(ii) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;

(iii) where the Processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

(iv) the right to lodge a complaint with the Commissioner;

(v) whether the Personal Data is obtained pursuant to a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data;

(vi) if applicable, the existence of automated decision-making, including Profiling, and meaningful information about the logic involved, as well as the significance and the possible outcomes of such Processing for the Data Subject;

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

(viii) whether the Personal Data will be used for direct marketing purposes; and

(ix) if the Controller intends to Process Personal Data in a manner that will restrict or prevent the Data Subject from exercising his rights to request rectification or erasure of Personal Data in accordance with Article 33, or to object to the Processing of the Personal Data in accordance with Article 34. In such cases, the Controller shall:

(1) include a clear and explicit explanation of the expected impact on such rights; and

(2) satisfy itself that the Data Subject understands and acknowledges the extent of any such restrictions.

(2) Article 29(1) shall not require a Controller to provide information the Data Subject already has.

30. 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 Controller shall provide the Data Subject with at least the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language:

(a) the identity and contact details of the Controller;

(b) the contact details of the DPO, if applicable;

(c) the purposes of the Processing, as well as its lawful basis under this Law;

(d) the categories of Personal Data relating to the Data Subject that are being processed;

(e) the recipients or categories of recipients of the Personal Data;

(f) where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or International Organisation, or in the case of transfers referred to in Articles 27(1)(a), 27(2)(b) or 27(3)(b), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; and

(g) any necessary information regarding the specific circumstances in which the Personal Data is Processed, to ensure fair and transparent Processing in respect of the Data Subject, including:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(ii) if the Controller's lawful basis for the Processing is legitimate interests or compliance with any Applicable Law to which the Controller is subject, the Controller shall state clearly what those legitimate interests or compliance obligations are;

(iii) notice of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;

(iv) where the Processing is based on the Data Subject's consent, notice of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

(v) the right to lodge a complaint with the Commissioner;

(vi) the source from which the Personal Data was obtained; and

(vii) if applicable, the existence of automated decision-making, including Profiling, and meaningful information about the logic involved, as well as the significance and the possible outcomes of such Processing for the Data Subject.

(2) The Controller must provide the information referred to in Article 30(1):

(a) no longer than one (1) month from obtaining the Personal Data; or

(b) if the Personal Data is used for communicating with the Data Subject, no later than the first communication; or

(c) if a disclosure (including the making available for Processing) to a Processor or a Third Party is envisaged, no later than the time when the Personal Data is first disclosed.

(3) Article 30(1) shall not apply:

(a) to require the Controller to provide information the Data Subject already has;

(b) to require the provision of such information if it proves impossible or would involve a disproportionate effort.

(c) where disclosure is expressly required by a Requesting Authority or an Applicable Law and which provides appropriate measures to protect the Data Subject's legitimate interests; or

(d) where the Personal Data must remain confidential subject to an obligation of professional secrecy in accordance with Applicable Law to which the Controller is subject, including a statutory obligation of secrecy.

31. Nature of Processing information

(1) Subject to Article 31(2), the information to be provided under Articles 29 and 30 shall be provided in writing, including, where appropriate, by electronic means.

(2) The information to be provided under Articles 29 and 30 may be provided orally upon a Data Subject's request, including where the Personal Data is being collected by means of a telephone conversation between the Controller and the Data Subject, on the condition that the identity of the Data Subject has been verified at the time of the request.

(3) A Controller may comply with the requirements under Articles 29 and 30, to the extent that the required information is contained within publicly available policies maintained by the Controller, by clearly directing the Data Subject to such policies. Such policies must be written in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Controller may include within such policies links directing the Data Subject to additional information about the Processing.

PART 6: RIGHTS OF DATA SUBJECTS

32. Right to withdraw consent

(1) Where the basis for the Processing of Personal Data is consent under Article 10(1)(a) or under Article 11(1)(a), the Data Subject may withdraw consent at any time by notifying the Controller in accordance with Article 12(5). Where a Controller has not complied with Article 12(5) a Data Subject may notify the Controller by any reasonable means.

(2) The right to withdraw consent is an absolute right available to a Data Subject if the basis for the Processing of the Data Subject's Personal Data is consent under Article 10(1)(a) or Article 11(1)(a).

(3) Upon the exercise of a Data Subject's right to withdraw consent, a Controller must comply with Article 22 and must cease Processing the Personal Data as soon as reasonably practicable, and ensure that any Processors do the same.

33. Rights to access, rectification and erasure of Personal Data

(1) Upon request, a Data Subject has the right to obtain from a Controller without charge and within one (1) month of the request:

(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) a copy of the Personal Data undergoing Processing in electronic form and of any available information as to its source, including up-to-date information corresponding with the information requirements set out in Articles 29 and 30; and

(c) subject to Article 33(4), the rectification of Personal Data unless it is not technically feasible to do so.

(2) Subject to Article 33(3), the Data Subject has the right to require the Controller to erase the Data Subject's Personal Data where:

(a) the Processing of the Personal Data is no longer necessary in relation to the purposes for which it was collected;

(b) a Data Subject has withdrawn consent to the Processing where consent was the lawful basis for Processing and there is no other lawful basis, provided that in such circumstances the Controller must comply with Article 22;

(c) the Processing is unlawful or the Personal Data is required to be deleted to comply with Applicable Law to which the Controller is subject; or

(d) the Data Subject objects to the Processing and there is no overriding legitimate grounds for the Controller to continue with the Processing.

(3) The Controller is only required to comply with a request by a Data Subject to erase Personal Data where:

(a) one of the conditions in Article 33(2) applies; and

(b) subject to Article 33(4), the Controller is not required to retain the Personal Data in compliance with Applicable Law to which it is subject or for the establishment or defence of legal claims.

(4) Where rectification or erasure of Personal Data is not feasible for technical reasons, then the Controller is not in violation of this Law for failing to comply with a request for rectification or erasure of the Personal Data, in accordance with Articles 33(1)(c), 33(2)(a) or Article 33(2)(d) as applicable, if:

(a) the Controller collected the Personal Data from the Data Subject; and

(b) the information provided to the Data Subject under Article 29(1)(h)(ix) was explicit, clear and prominent with respect to the manner of Processing the Personal Data and expressly stated that rectification or erasure (as the case may be) of the Personal Data at the request of the Data Subject would not be feasible.

(5) Where a Data Subject suffers adverse effects as a result of the inability of a Controller to rectify Personal Data and where the need for rectification was not caused by the Data Subject's own provision of inaccurate data, the Controller shall provide all reasonable assistance to the Data Subject to enable the Data Subject to take steps to mitigate the adverse effects.

(6) A Controller shall direct all recipients and Processors to rectify or erase Personal Data where the respective right is properly exercised or to cease Processing and return or erase the Personal Data where the right to object is validly exercised. In such circumstances, Article 22 applies to the erasure of the Personal Data by both the Controller and the Processor.

(7) If a Data Subject request under Article 33(1) is particularly complex, or requests are numerous, the Controller may send notice to the Data Subject, within one (1) month, to increase the period for compliance by a further two (2) months citing the reasons for the delay.

(8) Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request, providing written confirmation to the Data Subject reasons for the refusal.

(9) A Controller must be able to demonstrate to the Commissioner upon request that a Data Subject's request made in accordance with Article 33(8) is manifestly unfounded or excessive.

(10) If a Controller has reasonable doubts as to the identity of a Data Subject asserting a right under this Article 33, it may require the Data Subject to provide additional information sufficient to confirm the individual's identity. In such cases, the time period for complying with the Data Subject request does not begin until the Controller has received information or evidence sufficient to reasonably identify that the person making the request is the Data Subject.

(11) Where a Controller complies with a request under Article 33(1)(b) it shall not disclose the Personal Data of other individuals in a way that may infringe their rights under Applicable Law and the Controller may redact or otherwise obscure Personal Data relating to such other individuals. Where the Data Subject's request is received by electronic means, and unless otherwise requested by the Data Subject, the information may be provided in a commonly used electronic form.

(12) The information to be supplied pursuant to a request under this Article 33 must be supplied by reference to the data in question at the time the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(13) Without derogating from the requirements on DIFC Bodies as set out in Article 65(2), a Controller may restrict, wholly or partly, the provision of information to the Data Subject under Article 33(1)

to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the Data Subject, a necessary and proportionate measure to:

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security; or

(e) protect the rights of others.

(14) Where the provision of information to a Data Subject under Article 33(1) is restricted in accordance with Article 33(13), a Controller must inform the Data Subject in writing without undue delay:

(a) that the provision of information has been restricted;

(b) of the reasons for the restriction;

(c) of the Data Subject's right to lodge a complaint with the Commissioner under Article 60; and

(d) of the Data Subject's right to apply to the Court under Article 63.

(15) Article 33(14)(a) and (b) do not apply to the extent that complying with them would undermine the purpose of the restriction.

34. Right to object to Processing

(1) A Data Subject has the right to:

(a) object at any time on reasonable grounds relating to his particular situation to Processing of Personal Data relating to him where such Processing is carried out on the basis that:

(i) it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Controller; or

(ii) it is necessary for the purposes of the legitimate interests, where applicable, of a Controller or of a Third Party; and

(b) 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, subject to any provision of this Law that does not permit disclosure; and

(c) where Personal Data is Processed for direct marketing purposes, object at any time to such Processing, including Profiling to the extent that it is related to such direct marketing.

(2) Where there is a justified objection, Processing initiated by a Controller shall no longer include that Personal Data, and Article 22 shall apply with respect to such Personal Data. An objection under Article 34(1)(a) is deemed justified unless the Controller can demonstrate compelling grounds for such Processing that overrides the interests, rights of a Data Subject or that the circumstances in Article 34(3) apply.

(3) If a Controller collected Personal Data from a Data Subject and the Controller can demonstrate that the information provided to the Data Subject under Article 29(1)(h)(ix) was explicit, clear and prominent with respect to the manner of Processing the Personal Data and expressly stated that it

would not be possible to implement an objection to the Processing at the request of the Data Subject, then the Controller may continue Processing the Personal Data in the same manner, subject to this Law in all other respects.

(4) A Controller shall, no later than its first communication to a Data Subject, explicitly bring to the attention of the Data Subject in clear language that is prominent and separate from other communications or information, the rights referred to in Article 34(1).

35. Right to restriction of Processing

(1) Subject to Article 35(3), a Data Subject shall have the right to require a Controller to restrict Processing to the extent that any of the following circumstances apply:

(a) the accuracy of the Personal Data is contested by the Data Subject, for a period allowing the Controller to verify the accuracy of the Personal Data;

(b) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;

(c) the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

(d) the Data Subject has objected to Processing pursuant to Article 34 pending verification of whether the legitimate grounds of the Controller override those of the Data Subject.

(2) If a Controller lifts the period of restriction it shall inform the Data Subject in writing.

(3) Where Article 35(1) applies, the only Processing that may continue to be conducted without the consent of the Data Subject is:

(a) storage of the Personal Data concerned;

(b) Processing of the Personal Data for the establishment, exercise or defence of legal claims;

(c) Processing for the protection of the rights of another person; and

(d) Processing for reasons of Substantial Public Interest.

36. Controller's obligation to notify

The Controller shall communicate any rectification or erasure of Personal Data or Processing restriction carried out in accordance with Articles 33, 34 and 35 to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. A Controller shall inform the Data Subject about those recipients if a Data Subject requests it.

37. Right to data portability

(1) A Data Subject shall have the right to receive Personal Data that he has provided to a Controller in a structured, commonly used and machine-readable format where the Processing is:

(a) based on the Data Subject's consent or the performance of a contract; and

(b) carried out by automated means.

(2) The purpose of Article 37(1) is to enable ready portability between Controllers if so required by the Data Subject, and the Data Subject shall have the right to have the Personal Data transmitted directly from the Controller to whom the request is made to any other person, where technically feasible.

(3) A Controller is not required to provide or transmit any Personal Data where doing so would infringe the rights of any other natural person.

38. Automated individual decision-making, including Profiling

(1) A Data Subject shall have the right to object to any decision based solely on automated Processing, including Profiling, which produces legal consequences concerning him or other seriously impactful consequences and to require such decision to be reviewed manually.

(2) Article 38(1) shall not apply if the decision is:

(a) necessary for entering into, or performance of, a contract between a Data Subject and a Controller;

(b) authorised by Applicable Law to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights; or

(c) based on the Data Subject's explicit consent.

(3) DIFC law concerning fraud, counter-terrorism, money laundering, and tax-evasion monitoring and prevention which requires Processing of Personal Data that produces legal consequences concerning a Data Subject is regarded as falling within Article 38(2)(b).

(4) Article 38(2) does not apply if the Data Subject in question is a minor (by reference to the legal age of majority in the United Arab Emirates from time to time).

(5) A Controller may only rely on Articles 38(2)(a) and 38(2)(c) if it has implemented suitable measures to safeguard a Data Subject's rights which includes, at least, the ability for the Processing to be reviewed manually.

(6) Decisions affecting a Data Subject may not be based solely on the automated Processing, including Profiling, of Special Categories of Personal Data unless:

(a) the Data Subject has given explicit consent to the Processing of those Personal Data for such specific purposes; or

(b) the Processing is necessary for reasons of Substantial Public Interest, on the basis of Applicable Law, is proportionate to the aim pursued, respects the principles of data protection and provides for suitable measures to safeguard the rights and interests of the Data Subject.

39. Non-discrimination

(1) A Controller may not discriminate against a Data Subject who exercises any rights under this Part 6, including by:

(a) denying any goods or services to the Data Subject;

(b) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(c) providing a less favourable level or quality of goods or services to the Data Subject; or

(d) suggesting that the Data Subject will receive a less favourable price or rate for goods or services or a less favourable level or quality of goods or services.

(2) Nothing in this Article 39 prohibits a Controller from charging a Data Subject a different price or rate, or from providing a different level or quality of goods or services, if that difference is objectively and reasonably directly related to the value provided by the Data Subject’s data.

(3) Notwithstanding Article 39(1), a Controller may offer financial or non-financial incentives for the Processing of Personal Data provided that:

(a) the terms of the incentive are clearly communicated;

(b) the process for receiving the benefit of the incentive is clearly communicated, is transparent and does not require material additional effort or expense on the part of the Data Subject;

(c) the nature of the Processing involved is clearly communicated;

(d) the Processing complies in all respects with this Law; and

(e) it complies with Article 39(4).

(4) A Data Subject shall have the right to withdraw without penalty from, and require the cessation of Processing carried out under, any incentive scheme at any time. Incentive schemes must not be coercive or unreasonable in nature with respect to the Processing of Personal Data, including where the incentive is based on probability or a competition where the chance of receiving the incentive is disproportionately low compared to the value of the Personal Data and the impact on the Data Subject's rights.

40. Methods of exercising Data Subject rights

A Controller shall make available a minimum of two (2) methods (which may include but shall not be limited to post, telephone, email or an online form), which shall not be onerous, by which a Data Subject can contact the Controller to request to exercise his rights under this Part. If a Controller maintains a website, at least one (1) method of contact shall be available without charge via the website, without the need to submit data to create an account of any sort. At least one of the methods should correspond to the contact details provided under Article 29 or 30 as applicable.

PART 7: PERSONAL DATA BREACHES

41. Notification of Personal Data Breaches to the Commissioner

(1) If there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy, the Controller involved shall, as soon as practicable in the circumstances, notify the Personal Data Breach to the Commissioner.

(2) A Processor shall notify a relevant Controller without undue delay after becoming aware of a Personal Data Breach.

(3) A Controller or Processor shall fully co-operate with any investigation of the Commissioner in relation to a Personal Data Breach.

(4) The notification referred to in Article 41(1) shall at least:

(a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate amount of Personal Data records concerned;

(b) communicate the name and contact details of the DPO or other contact point where more information can be obtained;

(c) describe the likely consequences of the Personal Data Breach; and

(d) describe the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases when available.

(6) A Controller shall document in writing any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. The information recorded shall be sufficient to enable the Commissioner to verify compliance with this Article and shall be made available without delay on request.

42. Notification of Personal Data Breaches to a Data Subject

(1) When a Personal Data Breach is likely to result in a high risk to the security or rights of a Data Subject, the Controller shall communicate the Personal Data Breach to an affected Data Subject as soon as practicable in the circumstances. If there is an immediate risk of damage to the Data Subject, the Controller shall promptly communicate with the affected Data Subject.

(2) The communication to the Data Subject referred to in Article 42(1) shall describe in clear and plain language the nature of the Personal Data Breach and contain at least the information provided for in Articles 41(4)(b) to (d). Such communication shall, where possible, make recommendations for the Data Subject to mitigate potential adverse effects.

(3) Where a communication to the individual Data Subjects referred to in Article 42(1) will involve disproportionate effort, a public communication or similar measure by the Controller whereby the Data Subjects are informed in an equally effective manner shall be sufficient.

(4) If a Controller has not already communicated the Personal Data Breach to all relevant Data Subjects, the Commissioner may require it to do so, including where the Commissioner considers that there is a high risk to the security or rights of the Data Subjects involved, or otherwise direct it to make a public communication under Article 42(3).

PART 8: THE COMMISSIONER

43. Appointment of the Commissioner

(1) The President shall appoint a person to be the Commissioner who is appropriately experienced and qualified.

(2) The President shall consult with the DIFCA Board of Directors prior to appointing, re-appointing or removal of the Commissioner.

(3) The Commissioner shall be appointed for a specified period of time not exceeding five (5) years, and may be re-appointed provided that such period may not extend beyond the day when the Commissioner turns seventy-five (75) years of age.

(4) The Commissioner shall not be held personally liable for any act or omission committed by him under or in relation to this Law or in relation to his duties and functions as Commissioner, save for where the Commissioner has acted in bad faith. The DIFCA will indemnify and hold harmless the Commissioner with respect to all Liabilities whatsoever that may be incurred by or suffered by the Commissioner in relation to the discharge of the Commissioner's duties and functions under or in relation to this Law and his duties and functions as Commissioner.

(5) "Liabilities" as used in Article 43(4) includes, without limitation, the costs of settlements, judgments, damages and expenses including legal fees, costs and expenses, including legal fees, costs and expenses incurred in establishing a right to indemnity hereunder.

44. Removal of the Commissioner

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

45. Resignation of the Commissioner

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

46. Powers, functions and objectives of the Commissioner

(1) The Commissioner 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 shall pursue the following objectives:

(a) to monitor, ensure and enforce compliance with this Law;

(b) to promote good practices and observance of the requirements of this Law and the Regulations by a Controller or Processor; and

(c) 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 46(1), the Commissioner has the following powers, duties and functions:

(a) auditing a Controller or Processor, which includes having the right to obtain access to any premises and to any Processing equipment or means of a Controller or Processor who is subject to this Law, as well as having the right to require the production of information under Article 52. A Controller or Processor shall not be required to provide access to or

produce legally privileged material or material subject to a conflicting obligation of non-disclosure under Applicable Law. The Commissioner shall seek to minimise unreasonable interruption to the Controller or Processor in the exercise of its rights under this Article 46(3)(a) and shall give reasonable notice of its access requirements, in each case taking into account the purpose of the audit, the perceived risk to the rights of Data Subjects, the need to act urgently, the risk of loss or unavailability of information and the seriousness of any suspected contravention of this Law;

(b) conducting investigations and inspections to verify compliance with this Law;

(c) issuing directions in accordance with Article 59, and issuing warnings or admonishments and making recommendations to a Controller or Processor, including ordering the appointment of a DPO as described in Article 16(3);

(d) initiating proceedings for contraventions of the Law before the Court that may be self-initiated or initiated in response to an investigation of a complaint or a request from a Data Subject; for such purposes, the Commissioner shall be available for a Data Subject to contact in order to make complaints and shall take such action as he sees fit in furtherance of his primary objectives described in Article 46(1);

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

(f) imposing fines for non-compliance with the Law and any Regulations, including from time to time setting any limits or issuing schedules of fines applicable to specific breaches of the Law 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;

(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) promoting, as appropriate, and dealing with codes of conduct intended to contribute towards the application of this Law, as further described in Article 48;

(k) prescribing forms to be used for any of the purposes of this Law or any Applicable Law administered by the Commissioner;

(l) acquiring, holding and disposing of property of any description;

(m) making contracts and other agreements;

(n) with the prior consent of the President, borrowing monies and providing security for such borrowings;

(o) 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;

(p) 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;

(q) taking such steps as he deems appropriate in order to develop and participate in international cooperation mechanisms to facilitate data sharing and enforcement standards, including communicating with other competent data protection authorities with respect to breaches of this Law involving multi-jurisdictional organisations or Groups; and

(r) exercising and performing such other powers and functions as may be delegated to the Commissioner by the President pursuant to the provisions of this Law.

(4) The Commissioner 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 shall act in an independent and impartial manner and will not accept instructions from any other party.

47. Delegation of powers and establishment of advisory committee

(1) The Commissioner, 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, and with the approval of the DIFCA Board of Directors, either generally or in relation to any particular matter, to any other person.

(2) The Commissioner may establish an advisory committee. He may appoint a chairperson and a secretariat for the advisory committee.

(3) The scope and function of the advisory committee shall be confirmed in Regulations published by the Commissioner but may include:

(a) advising the Commissioner on any issue related to the protection of Personal Data and the application of this Law;

(b) assisting the Commissioner with the drafting of guidelines, recommendations, and best practices;

(c) assisting the Commissioner with respect to accreditation schemes, codes of conduct, mechanisms for data transfer;

(d) drafting Regulations;

(e) providing input, as requested by the Commissioner, regarding any question arising under this Law that the Commissioner is required to consider;

(f) preparing reports for the Commissioner; and

(g) liaising with other data protection committees and authorities as directed by the Commissioner.

(4) The advisory committee shall exercise its functions in an independent manner.

48. Codes of conduct

(1) A Controller, Processor, or any other body including any foundation, association, academic organisation, certification body or non-profit organisation representing categories of Controllers or Processors may prepare, amend or extend codes of conduct, for the purpose of specifying the application of and to contribute to the proper application of this Law. Specific codes may be developed that take account of the features of the various Processing sectors and the specific needs of different types of enterprises.

(2) Matters that such codes may cover include:

(a) fair and transparent Processing;

(b) legitimate interests pursued by a Controller in specific contexts;

(c) collection of Personal Data;

(d) pseudonymisation or anonymisation of Personal Data;

(e) information provided to a Data Subject or to the public;

(f) exercise of the Data Subject's rights;

(g) measures referred to in Article 14;

(h) notification of Personal Data Breaches to the Commissioner and the communication of such Personal Data Breaches to a Data Subject;

(i) transfer of Personal Data to Third Countries or International Organisations; and

(j) out-of-court proceedings and other dispute resolution procedures for resolving disputes between a Controller or Processor and a Data Subject with regard to Processing, without prejudice to a Data Subject's rights pursuant to Articles 60 and 64.

(3) Subject to the powers and functions of the Commissioner, a code of conduct referred to in Article 48(1) shall contain mechanisms that enable the relevant association or body to carry out the monitoring of compliance with its provisions by the Controllers or Processors that undertake to apply it.

(4) Persons or bodies referred to in Article 48(2) that intend to establish a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the Commissioner, who shall confirm whether or not the draft code is approved and may provide a process for approval by way of Regulations.

(5) Where the Commissioner approves a code under Article 48(4), it shall register and publish the code and designate a name by which the code is to be known.

(6) The Commissioner may also condition or withdraw approval of a code at any time, setting out the reason for such condition or withdrawal and any requirements that a Controllers or Processor must implement in place of any such code where relied upon in accordance with Article 14(6).

49. Monitoring of approved codes of conduct

(1) Subject to the powers and functions of the Commissioner, the monitoring of compliance with a code of conduct approved by the Commissioner pursuant to Article 48 may be carried out by a body that has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Commissioner.

(2) When deciding whether to accredit and maintain the accreditation of such a body, the Commissioner shall consider whether the body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code;

(b) established procedures that allow it to assess the eligibility of a Controller or Processor concerned to apply the code, to monitor compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a Controller or Processor, and to make those procedures and structures transparent to Data Subjects or the public; and

(d) demonstrated that its tasks and duties do not result in a conflict of interests.

(3) The Commissioner will revoke accreditation if he believes the above conditions are not met or if the body has infringed this Law.

(4) An accredited body shall, subject to appropriate safeguards, take appropriate action if the relevant code is infringed by a Controller or Processor, including suspension or exclusion of a Controller or Processor concerned from the code. It shall inform the Commissioner of such actions and the reasons for taking them.

50. Certification schemes

(1) A certification scheme may be established for the purposes of enabling a Controller or Processor to demonstrate compliance with this Law. Participation in a certification scheme shall be voluntary and available by a transparent process.

(2) Any certification achieved by a Controller or Processor does not relieve it of any responsibility for compliance with this Law.

(3) Certification may only be issued by a certification body approved under Article 51 or by the Commissioner (if he establishes a certification scheme).

(4) A certification issued under an approved scheme shall remain valid for a maximum period of three (3) years and may be renewed for equivalent periods, provided the relevant conditions continue to be met by the Controller or Processor in question. The approved body or Commissioner shall withdraw the certification of a Controller or Processor that is found to no longer meet the requirements for certification.

(5) The Commissioner shall maintain a public register of all approved certification bodies and relevant schemes.

51. Certification and Accreditation

(1) The Commissioner may receive applications for accreditation for the purposes of running a certification scheme referred to in Article 50.

(2) The Commissioner shall only award accreditation where a body has:

(a) demonstrated independence and expertise in relation to the subject-matter of the certification to the satisfaction of the Commissioner;

(b) undertaken in writing to respect the criteria of the proposed scheme;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks in connection with the proposed scheme, including establishing explicitly defined specific criteria for granting or not granting certification to an applicant;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by a Controller or Processor, and has made those procedures and structures transparent to Data Subjects and the public;

(e) demonstrated, to the satisfaction of the Commissioner, that its tasks and duties do not result in a conflict of interests; and

(f) demonstrated its compliance with any criteria for accreditation approved by the Commissioner and made public from time to time, whether via Regulations or otherwise.

(3) The Commissioner will revoke accreditation if he believes the above conditions are not met or if the body has infringed this Law.

(4) The body applying for accreditation shall make available all information in written form necessary or requested by the Commissioner, in order for him to make a determination for the purposes of Article 51(2).

(5) The maximum period of any accreditation shall be five (5) years, subject to renewal provided the body can demonstrate continuing compliance with all relevant requirements.

(6) When accredited, a certification body is responsible for the proper assessment of a Controller or Processor leading to the certification or the refusal or withdrawal of certification regardless of responsibility of the Controller or Processor for compliance with this Law.

52. Production of information

(1) The Commissioner may require a Controller or Processor by written notice to:

(a) give specified information;

(b) produce the Processing records, or copies thereof, required to be maintained under Article 15; or

(c) produce any other specified documents, including copies, that relate to the Processing of Personal Data.

(2) A Controller or Processor shall not be required to disclose legally privileged material or material subject to a conflicting obligation of non-disclosure under Applicable Law.

(3) The party in respect of whom a requirement is made pursuant to Article 52(1) shall comply with that requirement, unless the requested information is legally privileged material or material subject to a conflicting obligation of non-disclosure under Applicable Law. Where the party fails to comply with the requirement it shall be in breach of this Law. The Commissioner may issue a direction or impose a fine in accordance with Articles 59 or 62 of this Law or conduct further investigations.

53. Regulations

(1) The DIFCA Board of Directors, after consultation with the Commissioner, may make Regulations under the Law in respect of:

(a) any matters related to the application of the Law; and

(b) as proposed by the Commissioner under Article 53(2).

(2) The Commissioner 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) procedures for initiating and filing complaints;

(b) procedures for appealing and reconsidering decisions or determinations of the Commissioner;

(c) fines, including from time to time setting any limits or issuing schedules of fines applicable to specific breaches of the Law or otherwise setting out methodology to be used and the factors that will be taken into account by the Commissioner to determine the amount of any fine under this Law;

(d) fees;

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

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

(g) the conduct of the Commissioner 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 Applicable Law 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 shall publish draft Regulations by means of a notice including:

(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.

(6) Upon publication of a notice under Article 53(5), 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.

(7) Articles 53(5) and (6) shall not apply if the Commissioner concludes that any delay likely to arise under such Articles is prejudicial to the interests of the DIFC or to a Data Subject.

54. Funding

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

55. Annual budget of the Commissioner

(1) The DIFCA Board of Directors shall, before the end of each financial year, submit to the President for the President's approval estimates of the annual income and expenditure of the Commissioner for the next financial year.

(2) Such estimates shall include figures relating to levels of remuneration and entitlement to expenses of the officers, employees and agents of the Commissioner.

(3) The President may:

(a) approve the estimates submitted under Article 55(1); or

(b) on reasonable grounds reject such estimates within thirty (30) days of receiving them, where such rejection is to be advised in writing, with reasons, to the DIFCA Board of Directors.

(4) Unless the estimates have been expressly approved by the President under Article 55(3)(a) or rejected under Article 55(3)(b), they shall be deemed to have been approved on expiry of thirty (30) days from the date of submission referred to in Article 55(1).

56. Accounts

(1) The Commissioner shall keep proper accounts of his office's financial activities.

(2) The Commissioner, 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 this Article shall be submitted for the approval of the DIFCA Board of Directors.

57. Audit of Commissioner

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

(2) The DIFCA Board of Directors shall, as soon as reasonably practicable after the preparation and approval of the financial statements of the Commissioner, 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 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 that is reasonably required by them for the purposes of preparing the report and that is held or controlled by any officer, employee or agent of the Commissioner.

(6) The auditors shall be entitled reasonably to require from the officers, employees and agents of the Commissioner 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 57(1) in the exercise of his powers.

58. Annual report

(1) Upon request, the Commissioner shall deliver to the President, a report on the management of the administrative affairs of the Commissioner, for the previous year.

(2) Such report shall give a true and fair view of the state of the Commissioner's regulatory operations in the DIFC, and financial statements of the Commissioner, as at the end of the relevant financial year.

PART 9: REMEDIES, LIABILITY AND SANCTIONS

59. Directions

(1) If the Commissioner is satisfied, either on the basis of a complaint under Article 60(1) or on the basis of other information within his knowledge, that a Controller or Processor 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 may undertake reasonable and necessary inspections or investigations for the purposes of Article 59(1).

(3) A direction issued under Article 59(1) shall contain:

(a) a statement of the contravention of the Law or Regulations that the Commissioner is satisfied is being or has been committed; and

(b) a statement to the effect that the Controller or Processor may seek judicial review by the Court of:

(i) the decision of the Commissioner to issue the direction; or

(ii) the terms of the direction.

(4) A Controller or Processor that fails to comply with a direction of the Commissioner under this part of the Law contravenes this Law and may be:

(a) subject to fines; or

(b) liable for payment of damages and compensation to the Data Subject.

(5) If the Commissioner considers that a Controller or Processor or any officer of either has failed to comply with a direction, he may apply to the Court for one (1) or more of the following orders:

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

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

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

(6) Any affected party may make submissions to the Court in relation to the Commissioner's application for an order under Article 59(5).

(7) Any affected party may ask the Commissioner to review the direction within fourteen (14) days of receiving a direction under this part of the Law. The Commissioner may receive further submissions and amend or discontinue the direction.

(8) The Commissioner may, but is not obliged to, issue warnings to a Controller or Processor that its intended Processing operations are likely to infringe this Law.

(9) The Commissioner may, but is not obliged to, issue public reprimands to a Controller or Processor where its Processing operations have infringed this Law (in addition to imposing any other sanction provided for under this Law).

(10) The issuing of any direction by the Commissioner is without prejudice to the Commissioner's ability to impose fines under Article 62.

60. Lodging complaints and mediation

(1) A Data Subject who contends that there has been a contravention of the Law or an alleged breach of his rights under the Law may lodge a complaint with the Commissioner.

(2) Multiple Data Subjects affected by the same alleged contravention or breach of rights referred to in Article 60(1) may raise such complaint collectively. The Commissioner may choose to deal collectively with multiple allegations which relate to the same contravention or breach of rights, whether not such allegations are brought collectively.

(3) The Commissioner may investigate the matters that are the subject of the complaint or mediate between the complainant and the relevant Controller or Processor.

(4) On the basis of the investigation or mediation referred to in Article 60(3), the Commissioner may issue a direction under Article 59(1) or make a declaration of no contravention of the Law.

(5) The DIFCA Board of Directors may make Regulations on the procedures relating to the conduct of mediation under this Article 60.

61. General contravention

A Controller or Processor commits a contravention of this Law if it:

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

(b) does not do an act or thing that the Controller or Processor (as applicable) is required or directed to do under this Law and the Regulations (including where the Commissioner has issued a direction); or

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

62. 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 62.

(2) Subject to Article 62(3), where the Commissioner considers that a Controller or Processor (including a Sub-processor) has contravened the Law, the Commissioner may issue an administrative fine to the Controller or Processor in respect of a contravention referred to in Schedule 2 in an amount he considers appropriate but not exceeding the amount specified in Schedule 2 in respect of each contravention, payable by the date specified in such notice.

(3) The Commissioner may issue a general fine for a contravention of the Law by a Controller or Processor (including a Sub-processor), in an amount he considers appropriate and proportionate, taking into account the seriousness of the contravention and the risk of actual harm to any relevant Data Subject. Such fine shall be issued by written notice and shall be payable by the date specified in such notice.

(4) If, within the period specified in the notice referred to in Article 62(2) or 62(3), the Controller or Processor (as applicable) pays the prescribed fine to the Commissioner, then he may commence no further proceedings against the person in respect of the relevant contravention, but he may take action in relation to any continuing contravention, including where, in addition to the fine, a direction to the relevant Controller or Processor has been issued and has not been complied with.

(5) Provided an objection instigated in accordance with Article 62(6) is not in progress, if a Controller or Processor (as applicable) has not paid the prescribed fine to the Commissioner's office within the period specified in the notice referred to in Article 62(2) or 62(3) or within ten (10) days following the determination of any objection instigated in accordance with Article 62(6) in such terms that a fine is payable, then the Commissioner 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 interest, costs of enforcement (including legal costs) and other expenses directly arising from the failure to pay.

(6) A Controller or Processor (as applicable) may object to the imposition of a fine in accordance with procedures specified in Regulations referred to in Article 62(1).

(7) A certificate that purports to be signed by the Commissioner and states that a written notice was given to a person pursuant to Article 62(2) or 62(3) 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 62(4).

(8) In addition to any fine, the Commissioner may request the Court to make an order for damages or compensation payable to a Data Subject, even if he has not made a claim in accordance with Article 64. The principles in Article 64 will be considered when making the request to the Court. The Commissioner shall not make such requests unless in his opinion the Data Subject in question has suffered material damage as a result of the breach in question and is disadvantaged in his ability to bring a claim to the Court in his own name.

63. Application to the Court

(1) Any Controller or Processor who is found to contravene this Law or a direction of the Commissioner may appeal to the Court against the finding within thirty (30) days.

(2) A Data Subject who disagrees with a finding by the Commissioner of contravention of the Law or of no contravention of the Law may appeal against the finding to the Court within thirty (30) days.

(3) The Court may make any orders that it may think just and appropriate in the circumstances, including remedies for damages or compensation, penalties and imposition of administrative fines and findings of fact or alternative findings of fact in relation to whether or not the Law has been contravened.

64. Compensation

(1) A Data Subject who suffers material or non-material damage by reason of any contravention of this Law or the Regulations may apply to the Court for compensation from the Controller or Processor in question, in addition to, and exclusive of, any fine imposed on the same parties under Article 62. The same measure of damage shall be taken into account in any Court proceeding initiated by the Commissioner under Article 46(3)(d). No person shall be required to pay compensation twice with respect to the same damage.

(2) Any Controller involved in Processing that infringes this Law shall be liable for the damage caused. A Processor shall be liable for the damage caused by Processing only where it has not complied

with obligations of this Law specifically directed to Processors or where it has acted outside or contrary to the lawful instructions of the Controller.

(3) Where more than one Controller or Processor, or both a Controller and a Processor, are involved in the same Processing and where they are responsible for any damage caused by Processing, each person shall be held jointly and severally liable for the entire damage in order to ensure effective compensation of the Data Subject.

(4) Proceedings for exercising the right to receive compensation shall be brought before the Court, but may be settled out of Court.

PART 10: GENERAL EXEMPTIONS

65. General exemptions

(1) The DIFCA Board of Directors may make Regulations exempting Controllers from compliance with this Law or any parts of this Law. Such Regulations shall be consistent with the principles contained within this Article.

(2) In any case, without limiting the generality of Article 65(1), and having regard to the fundamental rights and legitimate interests of the Data Subject, Articles 26, 29, 30, 32, 33, 34, 35, 37, 38, 39 and 42 shall not apply to a DIFC Body, where such DIFC Body acts as a Controller, if, and only to the extent that, compliance with such Article would be likely to cause material prejudice to the proper discharge by such DIFC Body of its powers and functions under any laws administered by it (including any delegated powers and functions), provided that such powers and functions:

(a) are designed for protecting members of the public against 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;

(b) are designed for protecting members of the public against 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

(c) are designed for the detection, investigation and prosecution of criminal or unlawful behaviour.

(3) A DIFC Body shall maintain a register of instances where it relies on an Article 65(2) exemption, setting out:

(a) the Article concerned, to the extent that the exemption is a necessary and proportionate measure to carry out the powers and functions described in Article 65(2)(a) to (c); and

(b) the reasons for reliance on the exemption in such case.

(4) The Commissioner may inspect the register referred to in Article 65(3) and may at any time request additional information, raise a query or an objection to the exemption or conduct an investigation into the Applicable Law, regulation or public policy that supports the exemption to determine whether the exercise of the exemption complies with this Law.

(5) A DIFC Body that contravenes Article 65(2) by invalidly relying on an exemption shall be subject to any of the remedies, liabilities and sanctions set out in Part 9.

SCHEDULE 1

1. Rules of interpretation

(1) In this Law, unless otherwise provided, 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 this Law, include publishing or causing to be published in printed or electronic form;

(d) a "day" means a calendar day, unless expressly stated otherwise. If an obligation falls on a calendar day which is either a Friday or Saturday, or an official public holiday, the obligation shall take place on the next calendar day which is a business day;

(e) a "week" shall mean a calendar week or seven (7) days, whichever is applicable in the circumstances;

(f) a "month" shall mean a period of thirty (30) days;

(g) a "year" shall mean a period of three hundred and sixty five (365) days and a "calendar year" shall mean a year of the Gregorian calendar;

(h) a reference to the masculine gender includes the feminine and vice versa;

(i) the singular shall include the plural and vice versa;

(j) "dollar" or "$" is a reference to United States Dollars unless the contrary intention appears; and

(2) The headings in this Law shall not affect its interpretation.

(3) References in this Law to a body corporate include a company incorporated outside the DIFC.

(4) A reference in this Law to a Part, Chapter, Article or Schedule by number only, and without further identification, is a reference to the Part, Chapter, Article or Schedule of that number in this Law.

(5) A reference in an Article or other division of this Law to an Article by number or letter only, and without further identification, is a reference to the 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 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 this 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. 5 of 2020 made by the Ruler;

(e) the Regulations are legislation made by the DIFCA Board of Directors under this Law and are binding in nature;

(f) the Enactment Notice is the enactment notice pursuant to which this Law is brought into force; and

(g) guidance is indicative and non-binding and may comprise (i) guidance made and issued by the Commissioner 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
Applicable Law	means all applicable laws, statutes, codes, ordinances, decrees, rules, regulations, municipal by-laws, judgments, orders, decisions, rulings or awards of any government, quasi-government, statutory or regulatory body, ministry, government agency or department, court, agency or association of competent jurisdiction.
Binding Corporate Rules	Personal Data protection policies and procedures, aggregated or incorporated in a single written document, which regulate the transfer of Personal Data between members of a Group, legally bind such members to comply, and which contain provisions for the protection of such Personal Data.
Commissioner	the person appointed by the President pursuant to Article 43(1) of the Law to administer the Law.
Controller	any person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Court	the DIFC Court as established under Dubai Law.
Data Subject	the identified or Identifiable Natural Person to whom Personal Data relates.
DFSA	the Dubai Financial Services Authority.
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.

Terms	Definitions
DIFC Body	includes the Commissioner, DIFCA, DFSA, DIFC Courts, and any other person, body, office, registry or tribunal established under DIFC Laws or established upon approval of the President that is not revoked by this Law or any other DIFC Law. "DIFC Bodies" shall have a corresponding meaning.
DPO	a data protection officer appointed by a Controller (including a Joint Controller), or Processor to independently oversee relevant data protection operations in the manner set out in Article 16, 17, 18 and 19.
Filing System	any structured set of Personal Data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.
Group	any group of entities that are related to each other by virtue of being Subsidiaries of the same Ultimate Holding Company or subsidiaries of any such Subsidiaries. Ultimate Holding Company and Subsidiary have the meaning given in the DIFC Companies Law, Law No. 5 of 2018 (as amended or updated).
High Risk Processing Activities	Processing of Personal Data where one (1) or more of the following applies: (a) Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights; (b) a considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data; (c) the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or (d) a material amount of Special Categories of Personal Data is to be Processed.
Identifiable Natural Person	means a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and "Identified Natural Person" is interpreted accordingly).
International Organisation	an organisation and its subordinate bodies governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two (2) or more countries.
Joint Controller	any Controller that jointly determines the purposes and means of Processing with another Controller.
Law	this Data Protection Law 2020, Law No. 5 of 2020 as may be amended.
Personal Data	any information referring to an identified or Identifiable Natural Person.

Terms	Definitions
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
President	the President of the DIFC.
Process, Processed, Processes and Processing (and other variants)	any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored Personal Data with the aim of limiting Processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on Personal Data by: (a) a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or (b) law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.
Processor	any person who Processes Personal Data on behalf of a Controller.
Profiling	the automated Processing of Personal Data to evaluate the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.
Registrar	the Registrar of Companies appointed pursuant to Article 6 of the Companies Law, DIFC Law No. 5 of 2018.
Regulations	has the meaning given in paragraph 2(e) of this Schedule 1.
Requesting Authority	has the meaning given in Article 28(1).
Ruler	the Ruler of the Emirate of Dubai.
Schedule	a schedule to the Law.
Special Categories of Personal Data	Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.
Single Discrete Incident	has the meaning given in Article 12(11).
Sub-processor	a processor appointed by the Processor as set out in Article 24(2).
Substantial Public Interest	includes, but is not limited to: (a) administration of justice, including criminal and regulatory investigations; and (b) exercise of a function conferred on a person by Applicable Law.

Terms	Definitions
Third Country	a jurisdiction other than the DIFC, whether in the UAE or elsewhere.
Third Party	any person authorised to Process Personal Data, other than the: (a) the Data Subject; (b) the Controller; (c) Joint Controller; (d) the Processor; or (e) Sub-processor.
UAE	the United Arab Emirates.

SCHEDULE 2

The following table sets out administrative fines that may be applied for the corresponding contraventions of this Law. This list is not exhaustive and may be updated from time to time.

Article	Contravention	Maximum Fine (USD)
9	Failing to comply with general requirements specified under Article 9 of the Law made for the purpose of this Law	$50,000
10	Failure to comply with requirements for lawful Processing specified under Article 10 of the Law made for the purpose of this Law	$50,000
11	Failure to comply with requirements for obtaining consent specified under Article 11 of the Law made for the purpose of this Law	$50,000
12	Failure to comply with requirements for lawful Processing specified under Article 12 of the Law made for the purpose of this Law	$50,000
14(1)	Failure to comply with the requirements for accountability specified under Article 14(1) of the Law made for the purpose of this Law	$25,000
14(2)	Failing to implement and maintain technical and organisational measures to protect Personal Data in accordance with Articles 14(2) of the Law made for the purpose of this Law	$50,000
14(3)	Failure to comply with the requirements for accountability specified under Article 14(3) of the Law made for the purpose of this Law	$25,000
14(4)	Failure to comply with the requirements for accountability specified under Article 14(4) of the Law made for the purpose of this Law	$25,000
14(5)	Failure to comply with the requirements for accountability specified under Article 14(5) of the Law made for the purpose of this Law	$25,000
14(7)	Failing to register with the Commissioner in accordance with Article 14(7)	$25,000
15	Failing to maintain records of any Personal Data Processing operations in accordance with Article 15	$25,000
16	Failing to appoint a DPO in accordance with Articles 16(2) and 16(3) of the Law made for the purpose of this Law	$50,000
20	Failing to carry out a data protection impact assessment prior High Risk Processing Activities in accordance with Article 20 of the Law made for the purposes of this Law.	$20,000
22	Failing to comply with the requirements specified under Article 22(1), 22(2), 22(5) or 22(6) of the Law made for the purpose of this Law	$25,000
23	Failing to comply with the requirements specified under Article 23 of the Law made for the purpose of this Law	$25,000
24	Failing to comply with the requirements specified under Article 24(1), 24(3) or 24(6) of the Law made for the purpose of this Law	$25,000
25	Failing to comply with the requirements specified under Article 25 of the Law made for the purpose of this Law	$25,000
26	Failing to comply with the requirements specified under Article 26 of the Law made for the purpose of this Law	$25,000

Article	Contravention	Maximum Fine (USD)
27	Failing to comply with the requirements specified under Article 27 of the Law made for the purpose of this Law	$50,000
28	Failing to comply with the requirements specified under Article 28 of the Law made for the purpose of this Law	$10,000
29	Failing to comply with the requirements specified under Article 29 of the Law made for the purpose of this Law	$75,000
30	Failing to comply with the requirements specified under Article 30 of the Law made for the purpose of this Law	$75,000
31	Failing to comply with the requirements specified under Article 31 of the Law made for the purpose of this Law	$75,000
32(3)	Failing to comply with the requirements specified under Article 32(3) of the Law made for the purpose of this Law	$75,000
33	Failing to comply with the requirements specified under Article 33 of the Law made for the purpose of this Law	$100,000
34	Failing to comply with the requirements specified under Article 34 of the Law made for the purpose of this Law	$100,000
35	Failing to comply with the requirements specified under Article 35 of the Law made for the purpose of this Law	$100,000
36	Failing to comply with the requirements specified under Article 36 of the Law made for the purpose of this Law	$100,000
37	Failing to comply with the requirements specified under Article 37 of the Law made for the purpose of this Law	$100,000
38	Failing to comply with the requirements specified under Article 38 of the Law made for the purpose of this Law	$100,000
39	Failing to comply with the requirements specified under Article 39 of the Law made for the purpose of this Law	$50,000
40	Failing to comply with the requirements specified under Article 40 of the Law made for the purpose of this Law	$25,000
41	Failing to report Personal Data Breach in accordance with Article 41 of the Law made for the purpose of this Law	$50,000
42	Failing to report Personal Data Breach in accordance with Article 42 of the Law made for the purpose of this Law	$50,000
65	Failing to comply with the requirements specified under Article 65 of the Law made for the purpose of this Law	$75,000