Annex A

DATA PROTECTION LAW

DIFC LAW NO. [●] OF [2019]

TABLE OF CONTENTS

PART 1: INTRODUCTION AND SCOPE		1
1	Title	1
2	Legislative authority	1
3	Date of enactment	1
4	Commencement	1
5	Application of the Law	1
6	Interpretation	1
7	Administration of the Law	1
8	Fees	1
PART 2: GENERAL REQUIREMENTS		2
CHAPTER 1 – REQUIREMENTS FOR LEGITIMATE AND LAWFUL PROCESSING		2
9	General requirements	2
10	Requirements for legitimate and lawful Processing	2
CHAPTER 2 – PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA		3
11	Processing of Special Categories of Personal Data	3
CHAPTER 3 – CONDITIONS OF CONSENT AND RELIANCE ON LEGITIMATE INTERESTS		4
12	Consent	4
13	Legitimate interests	4
CHAPTER 4 – GENERAL REQUIREMENTS		5
14	Processing responsibilities	5
15	Records of Processing activities	5
16	Designation of the DPO	6
17	The DPO: competencies and status	6
18	Position and tasks of the DPO	7
19	DPO Controller assessment	7
20	Data protection impact assessment	7
21	Prior consultation	9
22	Cessation of Processing	10
PART 3: JOINT CONTROLLERS AND PROCESSORS		11
CHAPTER 1 – JOINT CONTROLLERS		11
23	Joint Controllers	11
CHAPTER 2 – PROCESSORS		11
24	Processors	11
25	Confidentiality	12
PART 4: DATA EXPORT		13
26	Transfers out of the DIFC: adequate level of protection	13
27	Transfers out of the DIFC in the absence of an adequate level of protection	13
28	Data sharing	15
PART 5: INFORMATION PROVISION		17
29	Providing information where Personal Data has been obtained from the Data Subject	17
30	Providing Information where Personal Data has not been obtained from the Data Subject	18
31	Nature of processing information	19
PART 6: RIGHTS OF DATA SUBJECTS		20
32	Right to withdraw consent	20
33	Rights to: access, rectification and erasure of Personal Data	20
34	Right to object to Processing	21
35	Right to restriction of Processing	22
36	Controller's obligation to notify	22
37	Right to data portability	22
38	Automated individual decision-making, including Profiling	23
39	Non-discrimination	23
40	Methods of exercising Data Subject rights	24
PART 7: PERSONAL DATA BREACHES		25
41	Notification of Personal Data Breaches to the Commissioner of Data Protection	25
42	Notification of Personal Data Breaches to the Data Subject	25
PART 8: THE COMMISSIONER OF DATA PROTECTION		26
43	Appointment of the Commissioner of Data Protection	26
44	Removal of the Commissioner of Data Protection	26

45	Resignation of the Commissioner of Data Protection	26
46	Powers, functions and objectives of the Commissioner of Data Protection	26
47	Delegation of powers and establishment of advisory committee	27
48	Codes of conduct	28
49	Monitoring of approved codes of conduct	29
50	Certification schemes	29
51	Certification bodies	30
52	Production of information	30
53	Regulations	30
54	Funding	31
55	Annual funding of the Commissioner of Data Protection	31
56	Accounts	32
57	Audit of Commissioner of Data Protection	32
58	Annual report	32
PART 9: REMEDIES, LIABILITY AND SANCTIONS		33
59	Directions	33
60	Lodging complaints and mediation	33
61	General contravention	34
62	Administrative imposition of fines	34
63	Application to the Court	35
64	Compensation	35
PART 10: GENERAL EXEMPTIONS AND DATA SHARING		36
65	General exemptions	36
SCHEDULE 1		37
1.	Rules of interpretation	37
2.	Legislation in the DIFC	37
3.	Defined terms	38

PART 1: INTRODUCTION AND SCOPE

1 **Title**

This Law may be cited as the "Data Protection Law **[**2019**]**".

2 **Legislative authority**

This Law is made by the Ruler of Dubai.

3 **Date of enactment**

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

4 **Commencement**

This Law comes into force on the date specified in the Enactment Notice in respect of this Law and replaces and repeals the DIFC Data Protection Law, being Law No. 1 of 2007, as amended by Data Protection Law Amendment Law DIFC Law No. 5 of 2012 and Amendment Law No. 1 of 2018, and all Regulations made thereunder.

5 **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 form part of a Filing System or are intended to form part of a Filing System.

(3) This Law applies to the Processing of Personal Data in the context of the activities of a Controller or a Processor operating, conducting or attempting to conduct business in or from the DIFC, regardless of whether the processing takes place in the DIFC or not.

(4) To the extent that this Law or the Regulations apply to any person to whom any provision of the DFSA-administered Applicable Law also applies, this Law and the Regulations shall not exempt such person from any requirement applicable to that person under the DFSA-administered Applicable Law.

6 **Interpretation**

Schedule 1 contains:

(a) interpretative provisions which apply to this Law: and

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

7 **Administration of the Law**

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

8 **Fees**

Regulations may be made which prescribe fees applicable to Controllers.

PART 2: GENERAL REQUIREMENTS

CHAPTER 1 – REQUIREMENTS FOR LEGITIMATE AND LAWFUL PROCESSING

9 General requirements

(1) Personal Data must be:

(a) Processed in accordance with a lawful basis set out in Article 10;

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

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

(d) Processed in a way which 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) accurate and, where necessary, kept up to date via erasure or rectification without undue delay;

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

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

(2) Without prejudice to the obligations on Processors, a Controller remains responsible for ensuring Article 9(1) is complied with and must be able to demonstrate such compliance, including to the Commissioner of Data Protection.

10 Requirements for legitimate and lawful Processing

(1) A lawful basis for Processing Personal Data may only be one of the following:

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

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

(c) the Processing is necessary for compliance with Applicable Law to which the Controller is subject;

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

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

(f) the Processing is necessary for the purposes of the legitimate interests pursued by the Controller or parties to whom the Personal Data are lawfully disclosed, subject to Article 13, except where such interests are overridden by the interests or rights of the Data Subject.

CHAPTER 2 – PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

11 Processing of Special Categories of Personal Data

(1) In addition to being Processed under a lawful basis provided for in Article 10, and without prejudice to the Controller's other Processing obligations including those in Article 9, Special Categories of Personal Data shall not be Processed unless:

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

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

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

(d) the Processing is carried out by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities with appropriate guarantees on condition that the Processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects;

(e) the Processing relates to Personal Data which are manifestly made public by the Data Subject;

(f) the Processing is necessary for the establishment, exercise or defence of legal claims or is performed by the Court acting in its judicial capacity;

(g) the Processing is necessary for compliance with a specific requirement of Applicable Law to which the Controller is subject, provided that:

(i) the Data Subject is given adequate notice unless the obligation in question prohibits, or the time for compliance with it does not reasonably allow for, any notice to be given; and

(ii) where the ability to give notice is not restricted in accordance with Article 11(1)(g)(i), the Data Subject is given the opportunity to object;

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

(i) the Processing is necessary for reasons of substantial public interest, on the basis of Applicable Law which shall be proportionate to the aim pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

(j) the Processing is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment or the management of health or social care systems and services, and where those Personal Data are Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy; or

(k) the Processing is required for protecting members of the public against:

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, management consultancy, IT services, accounting or other commercial activities (either in person or indirectly by means of outsourcing); or

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

CHAPTER 3 – CONDITIONS OF CONSENT AND RELIANCE ON LEGITIMATE INTERESTS

12 Consent

(1) Consent under Article 10(1)(a) and under Article 11(1)(a) must be freely given and given by a clear affirmative act which shows an unambiguous indication of consent.

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

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

(4) If the Controller seeks to obtain consent in the context of written information which is concerned with one or more other matters (matters not expressly concerned with the obtaining of consent to Process Personal Data) then the request for consent must be clearly distinguishable, intelligible, in an easily accessible form and use clear and plain language. Consent obtained via written information which does not comply with the above is not valid.

(5) A Data Subject may withdraw consent at any time in accordance with the right afforded to Data Subjects under Article 32. The Data Subject must be informed of this right at the time consent is obtained and the methods for exercising it (which must comply with Article 40). 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 time of withdrawal. Where consent is withdrawn the Controller must comply with Article 32(3).

(6) Where a Controller relies on a Data Subject's consent for Processing other than for a Single Discrete Incident, the Controller should implement appropriate and proportionate measures to assess the ongoing validity of the consent, which must include at least an annual re-evaluation by the Controller which considers whether the Data Subject, acting reasonably, would expect Processing to be continuing based on the consent given (taking into account the circumstances and the terms of such consent). Where such re-evaluation concludes that the Data Subject would no longer reasonably expect the Processing to be continuing, the Data Subject must be contacted without delay and asked to re-affirm consent. Without a positive act of re-affirmation within a reasonable time period, such consent shall be deemed to be withdrawn.

(7) Where Processing continues on the basis of consent and is not a Single Discrete Incident, the Data Subject should be made aware periodically of opportunities to re-affirm or withdraw his consent (without prejudice to Article 12(5)).

(8) A Single Discrete Incident means a Processing operation or collection of operations which relates to:

(a) a single, non-recurring transaction; or

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

in each case, with a definable end point.

(9) For the avoidance of doubt, consent given for Processing to perform a Single Discrete Incident remains subject to all foregoing provisions of this Article, in particular Article12(5).

13 Legitimate interests

(1) Public authorities may not rely on the basis of legitimate interests under Article 10(1)(f) to Process Personal Data.

(2) Where a Controller wishes to rely on the basis of legitimate interests under Article 10(1)(f) to Process Personal Data, the Controller must conduct a careful assessment first, including considering

whether a Data Subject can reasonably expect at the time and in the context of the collection of the Personal Data that Processing for that purpose may take place.

(3) Without prejudice to the provisions of this Law covering transfer of Personal Data to Third Countries and International Organisations, Controllers that are part of a group of undertakings may have a legitimate interest in transferring Personal Data within their group for internal administrative purposes.

(4) The Processing of Personal Data to the extent strictly necessary and proportionate to ensure network and information security is a legitimate interest of a Controller, as is the Processing of Personal Data strictly necessary for the purposes of preventing fraud.

CHAPTER 4 – GENERAL REQUIREMENTS

14 Processing responsibilities

(1) Controllers and Processors must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that Processing is performed in accordance with this Law. Those measures shall:

(a) take into account the nature, scope, context (including the risks presented by the Processing to the relevant Data Subjects and prevailing information security good industry practice) and purposes of Processing on a case-by-case basis;

(b) protect Personal Data and ensure a level of security appropriate to the risk, including taking account of the risk of wilful, negligent, accidental or unlawful destruction or loss, alteration, unauthorised disclosure of or access to Personal Data transmitted stored or otherwise Processed and against all other unlawful forms of Processing; and

(c) be reviewed and updated where necessary to reflect legal, operational and technical developments.

(2) Controllers and Processors must integrate the necessary measures into the Processing in order to meet the requirements of this Law and protect the rights of Data Subjects and follow the principle of "data protection by default and by design".

(3) Where a Controller is offering online services through a platform, the privacy settings of the platform should not be set to obtain or collect Personal Data by default; the Data Subject should be required to select their settings actively on first use and should be able to easily change such settings.

(4) Controllers and Processors shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility.

(5) All Controllers must implement and maintain an appropriate written data protection policy. Where proportionate in relation to Processing activities, the measures referred to in Articles 14(1), 14(2), 14(3) and 14(4) shall include the implementation and maintenance of appropriate data protection policies by the Processor.

(6) Adherence to approved codes of conduct as referred to in Article 48 or approved certification mechanisms as referred to in Article 50 may be used as an element by which to demonstrate compliance with the obligations in this Article.

15 Records of Processing activities

(1) Each Controller shall maintain a written record in electronic form of Processing activities under its responsibility. That record shall contain all of the following information:

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

(b) the purposes of the Processing;

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

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

(e) where applicable, transfers of Personal Data to a Third Country or an International Organisation, including the identification of that Third Country or International Organisation and, in the case of transfers referred to in Article 27(1)(b), the documentation of suitable safeguards;

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

(g) where possible, a general description of the technical and organisational security measures referred to in Article 14(1).

(2) Each Processor engaged in a specific Processing activity shall maintain a record containing the information specified in paragraph (1) of this Article with respect to such Processing activity.

16 **Designation of the DPO**

(1) Each Controller and Processor shall designate a DPO, having the competencies and status described in Article 17, if it performs (or will commence performing) High Risk Processing Activities systematically, regularly or necessarily to carry out its business.

(2) A Group may appoint a single DPO provided that a DPO is easily accessible from each undertaking in the Group. The DPO must be resident in the UAE unless the DPO is an individual employed within the organisation's Group outside the UAE and performs a similar function for the Group on an international basis.

(3) Subject to Article 16(2), the DPO may be a staff member of the Controller or Processor, or fulfil the tasks on the basis of a service contract.

(4) In cases other than those referred to in Article 16(1), a Controller or Processor may designate a DPO. A Controller or Processor to which Article 16(1) does not apply may be required to designate a DPO by order of the Commissioner of Data Protection and must, if required, do so.

(5) Controllers and Processors must publish the contact details of their DPO. On request, Controllers and Processors shall confirm identity of their DPO to the Commissioner of Data Protection in writing.

17 **The DPO: competencies and status**

(1) The designated DPO must have knowledge of this Law and its requirements and must assist the Controller or Processor to monitor compliance with this Law. The DPO must have the ability to fulfil the tasks referred to in Article 18.

(2) The DPO must:

(a) be in a position to perform their duties and tasks in an independent manner, whether or not they are a staff member of the relevant organisation or group, and possess a level of seniority to enable him to act on his own authority;

(b) have direct access and a reporting line to senior management;

(c) have sufficient resources to assist in the performance of his duties in an effective, objective and independent manner; and

(d) have timely and unrestricted access to information sufficient to enable him to carry out his responsibilities.

(3) The DPO must deal with the Commissioner of Data Protection in an open and co-operative manner and must disclose appropriately any information of which the Commissioner of Data Protection would reasonably be expected to be notified (without prejudice to mandatory notification requirements under this Law).

18 **Position and tasks of the DPO**

(1) The Controller or Processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data and is given sufficient resources necessary to carry out the role.

(2) The Controller or Processor shall ensure that the DPO does not receive any instructions regarding the exercise of his/her tasks and is free to perform them independently. He or she shall not be dismissed or penalised for properly performing his/her tasks.

(3) The DPO may also fulfil additional tasks and duties but the Controller or Processor must ensure that such tasks and duties do not result in a conflict of interests and do not otherwise prevent the DPO from properly performing the DPO role.

(4) Data Subjects may contact the DPO with regard to all issues related to Processing of their Personal Data and to the exercise of their rights under this Law.

(5) The tasks of the DPO shall include at least the following:

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

(b) to monitor compliance with: i) this Law; and ii) any other data protection provisions to which the organisation is subject; and iii) the policies of the organisation in relation 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;

(c) to provide advice where requested as regards data protection impact assessments;

(d) to cooperate with the Commissioner of Data Protection;

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

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

19 **DPO Controller assessment**

(1) Where the Controller is required to appoint a DPO under Article 16(1), the DPO must perform an annual Controller data protection assessment ("Annual Assessment").

(2) The Annual Assessment must be submitted to the Commissioner of Data Protection. The Annual Assessment will require the Controller to report on its Processing activities and indicate whether it anticipates it will perform High Risk Processing Activities in the following annual period.

(3) The Commissioner of Data Protection shall prescribe the format, required content and deadline for submission of the Annual Assessment.

20 **Data protection impact assessment**

(1) Where High Risk Processing Activities are to take place the Controller shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data.

(2) A single assessment may address a set of similar Processing operations that present similar high risks. If another member of the 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, which remains current and accurate, then the Controller may rely on such data protection impact assessment for the purposes of this Article 20.

(3) The Controller shall seek the advice of the DPO, where designated (under Article 16), when carrying out a data protection impact assessment.

(4) The Commissioner of Data Protection may establish and make public a non-exhaustive list of types and categories of Processing operations which are considered to be High Risk Processing Activities. Such a list is not intended to be exhaustive and does not absolve Controllers from responsibility for complying with this Law in all respects with regard to High Risk Processing Activities which are not referred to on the list. The absence of such a list does not absolve Controllers from complying with this Law in all respects with regard to High Risk Processing Activities.

(5) The Commissioner of Data Protection may also establish and make public a list of the kind of Processing operations for which no data protection impact assessment is required.

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

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

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

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

(i) where legitimate interests are the basis for Processing, the reasoning comprising the assessment required by Article 13(2) and why the Controller believes the interests or rights of the Data Subject do not override its interests; and

(ii) where consent is the basis for Processing, validation that consents will be or have been validly obtained and consideration of the impact of the withdrawal of consent to such Processing and how the Controller will ensure it is able to comply with the exercise of the Data Subject's right to withdraw consent;

(d) an assessment of the risks to the rights and freedoms 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 persons concerned.

(7) Compliance with approved codes of conduct referred to in Article 48 by the relevant Controllers or Processors shall be taken into due account in assessing the impact of the Processing operations.

(8) Where appropriate, the Controller shall seek the views of Data Subjects or their representatives on the intended Processing, without prejudice to the protection of commercial or public interests or the security of Processing operations.

(9) Where:

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

(b) that 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 legal basis,

the need for a new data protection impact assessment shall not apply unless such Applicable Law deems it to be necessary to carry out such an assessment prior to Processing activities.

(10) Where necessary, the Controller shall carry out a review to assess if Processing is performed in accordance with the data protection impact assessment and at least when there is a change of the risk represented by Processing operations.

(11) Processors which have been appointed by a Controller or are in discussions with a Controller, which are not merely hypothetical, with a view to being so appointed to carry out identified Processing activity should assist the Controller by providing all reasonable information requested by the Controller in connection with any data protection impact assessment which the Controller carries out in relation to the Processing in question.

21 **Prior consultation**

(1) The Controller shall consult the Commissioner of Data Protection 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 and freedoms of Data Subjects remain particularly high and the Controller has already carried out or wishes to commence or continue with the Processing activity.

(2) Controllers may consult, where required, with the Commissioner of Data Protection before commencing the Processing activity in question. The Controller is not prohibited from commencing the Processing activity in question before or during the consultation period where there is insufficient time to complete consultation in advance and there is a pressing business need to commence Processing which is not overridden by the vital interests of the Data Subjects. Such Processing must comply with the Law at all times and the Controller will remain liable for breaches of the Law prior to or during the consultation period.

(3) If the Commissioner of Data Protection makes directions with respect to the Processing in question as a result of the consultation then the Controller must implement such determinations without delay or cease or not commence, as the case may be, the Processing activity.

(4) The Controller's decision to consult, or failure to consult, will be taken into account by the Commissioner when considering any applicable sanctions under this Law. A failure to consult with the Commissioner of Data Protection when required may result in the application of more severe penalties if the Processing in question is in violation of the Law.

(5) Controllers may act with other Controllers (which need not be Joint Controllers) in jointly completing data protection impact assessments and carrying out prior consultation (for example, where multiple Controllers wish to use a new technology or platform, or where there is an innovation in a particular industry which changes the way Personal Data are Processed).

(6) Where the Commissioner of Data Protection is of the opinion that the Processing referred to in Article21(1) would infringe this Law or does infringe this Law, in particular where the Controller has insufficiently identified or mitigated the risk, the Commissioner of Data Protection shall provide written confirmation to the Controller and, where applicable to the Processor, and may use any of its powers referred to in Article 46 The Controller and Processor must cease unlawful Processing. The Commissioner of Data Protection shall endeavour to provide its written confirmation within four weeks of the beginning of consultation but may notify the Controller that the time period is being extended by up to a further four weeks where the Processing in question is particularly complex.

(7) When consulting the Commissioner of Data Protection pursuant to Article 21(1), the Controller shall provide the Commissioner of Data Protection with:

(a) where applicable, the respective responsibilities of the Controller, Joint Controllers and Processors involved in the Processing, in particular for Processing within a group of undertakings;

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

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

(d) where applicable, the contact details of the DPO(s) of the relevant undertakings;

(e) the data protection impact assessment provided for in Article 20; and

(f) any other information requested by the Commissioner of Data Protection.

(8) Processors which have been appointed by a Controller or are in discussions with a Controller, which are not merely hypothetical, with a view to being so appointed to carry out identified Processing activity should provide reasonable assistance to the Controller in the prior consultation process.

22 **Cessation of Processing**

(1) Where the basis for Processing (in accordance with Article 10) ceases to exist or the Controller is required to cease Processing via the exercise of Data Subject rights, the Controller must ensure that all Personal Data (including Personal Data held by Processors) are securely and permanently deleted or, where the Controller is unable to ensure that the Personal Data are securely and permanently deleted, archived in a manner which ensures the data is put beyond further use.

(2) "put beyond further use" in Article 22(1), means that:

(a) the Controller is not able, and must not attempt, to use the Personal Data to inform any decision in respect of the Data Subject or in a manner that affects the Data Subject in any way;

(b) no party other than the Controller has access to the Personal Data;

(c) the Personal Data are protected by appropriate technical and organisational security which is no less than that afforded to live Personal Data in accordance with this Law; and

(d) the Controller has in place a strategy for the permanent deletion of the Personal Data if, or when, this becomes possible (which the Controller must comply with).

(3) Notwithstanding Article 22(1), the Controller is not required to securely and permanently delete Personal Data or to put them beyond further use, when such Personal Data are necessary for the establishment or defence of legal claims or must be retained for compliance with Applicable Law.

(4) The Controller must have a policy and process for securely and permanently deleting Personal Data which are subject to Article 22(3) when the grounds for retention under Article 22(3) no longer apply. The Controller must securely and permanently delete the Personal Data when such grounds no longer apply.

PART 3: JOINT CONTROLLERS AND PROCESSORS

CHAPTER 1 – JOINT CONTROLLERS

23 **Joint Controllers**

(1) Where two or more controllers jointly determine the purposes and means of processing, they shall be Joint Controllers.

(2) Joint Controllers must, in a clear manner and in a written agreement, determine their respective responsibilities for ensuring compliance with the obligations under this Law. Such agreement must be clear how attempts by Data Subjects to exercise their rights will be dealt with and how the duties to provide the information referred to in Articles 29 and 30 will be complied with.

(3) The essence of the written agreement shall be made available to the affected Data Subjects.

(4) Regardless of the terms of the written agreement, all Joint Controllers remain responsible for all Controller obligations under this Law and the Data Subject may exercise his or her rights under this Law in respect of and against each of the Joint Controllers.

CHAPTER 2 – PROCESSORS

24 **Processors**

(1) Where Processing is to be carried out on behalf of a Controller, the Controller shall use only Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Law and ensure the protection of the rights of the Data Subject.

(2) A Processor may not engage another Processor without the prior specific or general written authorisation of the Controller. The Controller must not give a general written authorisation unless the Controller has ensured that conditions are in place to ensure that appointed sub-Processors (present or future) adequately protect the Personal Data. If a general written authorisation has been given, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors.

(3) Subject to Article 24(2), a Processor may not engage another Processor for carrying out specific Processing activities on behalf of the Controller, unless it has in place with such other Processor a legally binding contract containing the requirements set out in Article 24(4). Where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.

(4) Processing by a Processor must be governed by a legally binding contract with the Controller, or where sub-Processors are engaged in accordance with Articles 24(2) and (3), governed by a legally binding contract in writing between the appropriate Processors in the chain to ensure a full flow-down of the Processor's obligations referred to in this Article 24(4). Each such contract must set out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller. Every Processor or sub-Processor (as applicable) must give commitments under such a contract that it shall:

(a) Process the Personal Data only on the documented instructions from the Controller (as reflected in flow-down agreements between Processors if applicable and permitted as described above), including with regard to 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;

(b) where Applicable Law, as referred to in Article 24(4)(a) above applies, the Processor subject to the Applicable Law must be under a commitment in the contract to inform the counterparty; where there is a chain of Processors, the obligations must ensure that the chain of contracts operates such that the Controller is notified; in each case, a Processor is not required to give such notification if the Applicable Law in question prohibits such information being provided on important grounds of public interest;

(c) ensure that persons authorised to Process the Personal Data are under legally binding commitments or duties of confidentiality;

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

(e) comply with the conditions referred to in Articles 24(2) and (3) for engaging another Processor;

(f) taking into account the nature of the Processing, assist the counterparty by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights;

(g) assist the counterparty in ensuring the Controller's compliance with the obligations pursuant to Articles 14 (Processing Responsibilities), 20 (Data Protection Impact Assessment), 21 (Prior Consultation), 41 (Notification of Personal Data Breaches to the Commissioner of Data Protection) and 42 (Notification of Personal Data Breaches to the Date Subject; taking into account the nature of Processing and the information available to the Processor;

(h) at the choice of the Controller, delete or return all the Personal Data to the Controller or make the same available for return by the 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; and

(i) make available to the counterparty or, if requested, the Commissioner of Data Protection, all information necessary to demonstrate compliance with the obligations laid down in this Article (on condition that where the counterparty is not the Controller, such information may be made available to the Controller) and permit and provide reasonable assistance with audits, including inspections, conducted by i) the counterparty, ii) another auditor mandated by the counterparty, or iii) the Commissioner of Data Protection.

(5) The Processor shall immediately inform the Controller or the Processor which has appointed it if, in its opinion, the Processing activity infringes this Law.

(6) Adherence of a Processor to an approved code of conduct as referred to in Article 48 or an approved certification mechanism as referred to in Article 50 may be used as an element by which to demonstrate sufficient guarantees as referred to in Article 24(1).

(7) The Commissioner of Data Protection may lay down or endorse standard contractual clauses for the matters referred to in Articles 24 (3) and (4). If it does so, then the incorporation of such clauses in an applicable written agreement shall be sufficient to discharge the obligations in Articles 24(4)(a) to (4)(i) (inclusive).

(8) Without prejudice to Articles 60 (Lodging Complaints and Mediation), 61 (General Contravention), 62 (Administrative Imposition of Fines), 63 (Application to the Court) and 64 (Compensation), 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 assume all the responsibilities and obligations of a Controller accordingly.

(9) Both the original Controller and the Processor in question are in breach of this Law if they commence mutually agreed Processing activity without the required written contract in place.

25 **Confidentiality**

The Controller and Processor should take steps to ensure that any person acting under their respective authority who has access to Personal Data shall not Process it except on instructions from the Controller, unless he is required to do so by Applicable Law in his personal capacity.

PART 4: DATA EXPORT

26 Transfers out of the DIFC: adequate level of protection

(1) Any Processing of Personal Data which 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 laws and regulations that are applicable, as set out in Articles 26(2) and (3), including with respect to onward transfers of Personal Data; or

(b) in accordance with Article 27.

(2) For the purposes of Article 26(1), the Commissioner of Data Protection shall determine which jurisdictions and International Organisations provide 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 public authorities to personal data;

(c) the existence of effective data protection law, including rules on the onward transfer of personal data to another jurisdiction or International Organisation;

(d) the existence and functioning of one or more independent supervisory authorities with adequate enforcement powers; and

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

The Commissioner of Data Protection may make such determination based on adequacy decisions made by other competent data protection authorities where such decisions have taken into account the same factors.

(3) The Commissioner of Data Protection shall pass Regulations to provide details of its determinations under Article 2426(2).

(4) A jurisdiction may lose adequacy status from time to time. In such circumstances, the Commissioner of Data Protection may issue amended Regulations if necessary.

(5) Processing in accordance with this Article 26 does not require any specific authorisation or notification to the Commissioner of Data Protection as a result (but is without prejudice to the other provisions 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 and enforceable instrument between public authorities or bodies;

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

(c) standard data protection clauses adopted by the Commissioner of Data Protection;

(e) an approved code of conduct pursuant to Article 48 together with binding and enforceable commitments of the Controller or Processor in the Third Country to apply the appropriate safeguards, including as regards Data Subjects' rights; or

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

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

(a) the Data Subject has given his explicit consent to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the Data Subject and the 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 concluded in the interest of the Data Subject between the Controller and a Third Party;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary or legally required on grounds important in the interests of the DIFC;

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

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

(h) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Applicable Law for consultation are fulfilled in the particular case (the content of the register to be transferred shall be minimised and limited as far as possible);

(i) subject to Article 28, the transfer is necessary for compliance with any obligation under Applicable Law to which the Controller is subject or the transfer is made at the request of a regulator, police or other government agency or competent authority;

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

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

(4) Where a transfer could not be based on one of the above provisions in this Article 27 or on Article 26, a 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; and

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

(c) is necessary for the purposes of compelling legitimate interests pursued by the Controller which are not overridden by the interests or rights and freedoms 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.

The Controller shall inform the Commissioner of Data Protection of the transfer. The Controller shall, in addition to providing the information referred to in Articles 29 and 30, as applicable, inform the Data Subject of the transfer and on the compelling legitimate interests pursued.

(5) Public authorities may not rely on Articles 27(3)(a), (b) and (c), or on Article 27(4).

(6) A Controller may rely on Binding Corporate Rules subject to the following:

(a) the Binding Corporate Rules may only be used for transfers within the Controller's Group and shall not permit transfers of Personal Data outside the Controller's Group unless such transfer would otherwise be lawful in accordance with this Law in all respects;

(b) the Binding Corporate Rules must have been approved by the Commissioner of Data Protection.

(7) Any Controller may make a request to the Commissioner of Data Protection for approval of Binding Corporate Rules. Such a request must include a full copy of the Binding Corporate Rules and confirmation as to whether such Binding Corporate Rules have been approved by any competent data protection authority. The Controller should also include details of the transfers it intends to make in reliance on the Binding Corporate Rules. Where the Binding Corporate Rules operate on the basis that members of the Controller's Group (including the Controller) purport to 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.

(8) The Commissioner of Data Protection shall typically, but does not guarantee to, approve Binding Corporate Rules which have been approved by a competent data protection authority in any jurisdiction to which Article 26(2) applies. Controllers must not assume such approval and must submit a request under Article 27(7) in any event.

(9) If any set of Binding Corporate Rules is amended the Controller must provide the revised copy to the Commissioner of Data Protection without delay, in a form which shows clearly the edits made. The Commissioner of Data Protection may approve or reject the revised Binding Corporate Rules. If the revised Binding Corporate Rules are rejected then the Controller may not rely on them under Article 27(2)(b).

(10 The Commissioner of Data Protection may request Controllers to confirm in writing from time to time that an approved set of Binding Corporate Rules remains in the same form as when approved and is used to facilitate the same transfers as when approved.

(11) The Commissioner of Data Protection may require a Controller to provide evidence of any matter relating to Binding Corporate Rules on request.

28 **Data sharing**

(1) Where a Controller receives a request from any governmental authority or competent authority, national enforcement agency or other person exercising statutory authority over the Controller of any part of its Group (a "Requesting Authority") for the disclosure and transfer outside the DIFC of any Personal Data, the Controller shall (without prejudice to any other obligations under this Law and, in particular, the Controller's obligations under Part 2 regarding its responsibility for ensuring compliance with the general data protection principles and Part 4 regarding transfers out of the DIFC):

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request (including that the Requesting Authority has the appropriate powers to make the request and is doing so in the performance of a function of the Requesting Authority) and 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 and freedoms of affected Data Subjects 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;

(c) wherever possible, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights and freedoms 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) To the extent that a Controller cannot satisfy itself that:

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

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

the Controller should not disclose or transfer Personal Data to the Requesting Authority.

(3) The Controller may consult with the Commissioner of Data Protection 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 or her Personal Data:

(a) the identity and contact details (which should be within the DIFC) of the Controller;

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

(c) the purposes of the Processing for which the Personal Data are intended, as well as the legal basis under this Law;

(d) if the Controller's lawful basis for the Processing is legitimate interests (including where necessary to uphold the legitimate interests of the Controller recognised in the international financial markets), compliance with any Applicable Law to which the Controller is subject or the Processing is necessary to comply with Applicable Law, auditing, accounting, anti-money laundering or counter terrorist financing obligations, the Controller must state clearly what those legitimate interests or compliance obligations are;

(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 further information in so far as such is necessary, having regard to the specific circumstances in which the Personal Data are collected, to guarantee fair and transparent Processing in respect of the Data Subject, which includes:

(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 of Data Protection;

(v) if the Personal Data is 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 or requests for Personal Data 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 which will restrict or prevent the Data Subject from exercising his or her 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, the

Controller must: (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) A Controller need not provide that information otherwise required by this Article 29 to the Data Subject if the Controller has already provided that information.

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 (which should be within the DIFC);

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

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

(d) the categories of Personal Data concerned;

(e) the recipients or categories of recipients;

(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 2627(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 further information in so far as such further information is necessary, having regard to the specific circumstances in which the Personal Data is Processed, to guarantee fair and transparent Processing in respect of the Data Subject, which includes:

(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 (including where necessary to uphold the legitimate interests of the Controller recognised in the international financial markets), compliance with any Applicable Law to which the Controller is subject or the Processing is necessary to comply with any Applicable Law, auditing, accounting, anti-money laundering or counter terrorist financing obligations, the Controller must state clearly what those legitimate interests or compliance obligations are;

(iii) 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;

(iv) 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;

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

(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) within a reasonable period of, and no longer than one month from, obtaining the Personal Data; or

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

(c) if a disclosure to a Third Party is envisaged no later than the time when the Personal Data is first Processed by such Third Party or disclosed to it.

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

(a) the Controller to provide information which the Controller reasonably expects that the Data Subject already has; or

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

31 **Nature of processing information**

(1) The information to be provided under Articles 29 and 30 shall be provided in writing, including, where appropriate, by electronic means. When requested by the Data Subject (which includes where the Personal Data is being collected by means of a telephone conversation between the Controller and the Data Subject), the information may be provided orally, provided that the identity of the Data Subject has been verified.

(2) The Controller may comply with the requirements, to the extent that the required information is contained within public 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 the information, links to where the Data Subject may find further information in relation to 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) (or where the Controller has not complied with Article 12(5) by providing compliant means for the withdrawal of consent, the Data Subject may notify the Controller by any reasonable means).

(2) The right to withdraw consent is an absolute right.

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

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

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

(a) without charge and within one month, 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) without charge and within one month, 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 Article 29; and

(c) without charge and within one month, the rectification of Personal Data unless it is not technically feasible to do so and subject to Article 33(4).

(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 they were collected or Processed;

(b) a Data Subject has withdrawn his or her 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 in any case;

(c) the Processing is unlawful or the Personal Data are 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) 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; and

(c) subject to Article 33(4).

(4) Where rectification or erasure of Personal Data is not feasible for technical reasons then the Controller is not in violation of this Law with respect to a failure to comply with a request for rectification or erasure of the Personal Data in accordance with Article 33(2)(a) or Article 33(2)(d) 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)(g)(ix) was explicit, clear and prominent with respect to the manner of Processing the Personal Data and expressly stated that rectification and/or erasure (as the case may be) of the Personal Data at the request of the Data Subject would not be feasible.

(5) Where the Data Subject suffers adverse effects as a result of the inability of the 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) The Controller must direct all recipients and Processors to rectify or erase the Personal Data where the corresponding right is properly exercised or to cease Processing and return or erase the Personal Data where the right to object is properly exercised. Article 22 applies to the erasure of the Personal Data by the Controller (and the Processor).

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

The Controller must be able to demonstrate that the request is manifestly unfounded or excessive.

(9) If the Controller has reasonable doubts as to the identity of a person purporting to exercise a right under this Article 33, it may require the person to provide additional information sufficient to confirm his or her identity. In such cases, the time period for complying with the Data Subject request does not begin until the Controller has verified that the person making the request is the Data Subject.

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

34 **Right to object to Processing**

(1) A Data Subject has the right:

(a) to object at any time on reasonable grounds relating to his particular situation to the Processing of Personal Data relating to him 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 the Controller; or

(ii) it is necessary for the purposes of the legitimate interests of the Controller or of a third party; and

(b) to be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses (without prejudice to any provision of this Law which would not permit such disclosure in any event); and

(c) where Personal Data are Processed for direct marketing purposes, the Data Subject shall have the right to object at any time to such Processing, which includes Profiling to the extent that it is related to such direct marketing.

(2) Where there is a justified objection, the Processing instigated by the 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 which override the interests, rights and freedoms of the Data Subject or the circumstances in Article 34(4) apply.

(3) Any objection under Articles 34(1)(b) or 34(1)(c) shall be deemed justified.

(4) If the Controller collected the Personal Data from the Data Subject and the Controller can demonstrate that the information provided to the Data Subject under Article 29(1)(g)(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).

(5) The Controller must, no later than its first communication with the 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) The Data Subject shall have the right to require the Controller to restrict Processing whilst one of the following applies:

(a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling 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 their 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 the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

If the Controller lifts the period of restriction it must inform the Data Subject in writing.

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

(a) the storage of the Personal Data concerned;

(b) the 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; or

(d) Processing for reasons of important public interest.

36 **Controller's obligation to notify**

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

37 **Right to data portability**

(1) The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format where the Processing:

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

(b) is carried out by automated means.

(2) The purpose of Article 37(1) is to enable ready portability between Controllers 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 another Controller, where technically feasible.

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

(4) Controllers within common industries, particularly data-heavy consumer-focussed industries, are encouraged to develop interoperable formats within their respective industries that enable data portability.

38 **Automated individual decision-making, including Profiling**

(1) The Data Subject shall have the right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Examples of such an automated decision may include online credit applications or online recruitment tools, where there is no element of human intervention.

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

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

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

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

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

(3) Article 38(2) does not apply if the Data Subject in question is a child.

(4) The Controller may only rely on Articles 38(2)(a) and (c) if it has implemented suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests which includes at the least, the right for the Processing to be revisited and considered by human intervention (rather than automatic means), the right for the Data Subject to express a point of view to the Controller and the right to contest the decision made due to the Processing.

(5) Decisions 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 because the Data Subject exercised any of the Data Subject's rights under this Part 6 of the Law, including, but not limited to, by:

(a) denying 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 different level or quality of goods or services to the Data Subject; or

(d) suggesting that the Data Subject will receive a different price or rate for goods or services or a different 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) Without prejudice to 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 and 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; and

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

(e) Article 39(4) is complied with.

(4) The Data Subject must 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 (for example, where the incentive is based on probability or a competition where the chance of receiving the incentive is disproportionately low compared to the value in the Personal Data and the impact on the rights and freedoms of the Data Subject).

40 **Methods of exercising Data Subject rights**

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

(2) Where a telephone method is offered, the number should be a toll-free line.

PART 7: PERSONAL DATA BREACHES

41 Notification of Personal Data Breaches to the Commissioner of Data Protection

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

(2) The Processor must notify the Controller without undue delay after becoming aware of a Personal Data Breach.

(3) Both Controllers and Processors shall fully co-operate with any investigation that the Commissioner of Data Protection wishes to conduct in relation to any 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 number 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;

(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 without undue further delay.

(6) The Controller shall document in writing in electronic form any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall enable the Commissioner of Data Protection to verify compliance with this Article and must be made available without delay on request.

42 Notification of Personal Data Breaches to the Data Subject

(1) When the Personal Data Breach is likely to result in a high risk to confidentiality, security or privacy of Data Subjects, the Controller shall communicate the Personal Data Breach to the Data Subjects as soon as feasible in the circumstances. An immediate risk of damage urgently requires prompt communication with Data Subjects whereas the need to implement appropriate measures against continuing or similar Personal Data Breaches without an immediate risk of damage may justify more time for communication.

(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 and the recommendations provided for in Articles 41(4)(b),(c) and (d). The communication should make recommendations for the Data Subject to mitigate potential adverse effects.

(3) The communication to the individual Data Subjects referred to in Article 42(1) shall not be required if it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

(4) If the Controller has not already communicated the Personal Data Breach to the Data Subject, the Commissioner of Data Protection, having considered the likelihood of the Personal Data Breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in Article 42(3) are met.

PART 8: THE COMMISSIONER OF DATA PROTECTION

43 Appointment of the Commissioner of Data Protection

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

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

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

(4) The Commissioner of Data Protection 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 of Data Protection, save for where the Commissioner of Data Protection has acted in bad faith. DIFCA will indemnify and hold harmless the Commissioner of Data Protection with respect to all Liabilities whatsoever that may be incurred by or suffered by the Commissioner of Data Protection in relation to the discharge of the Commissioner of Data Protection's duties and functions under or in relation to this Law and his duties and functions as Commissioner of Data Protection.

(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 of Data Protection

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

45 Resignation of the Commissioner of Data Protection

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

46 Powers, functions and objectives of the Commissioner of Data Protection

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

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

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

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

(3) Without limiting the generality of Article 46(1), the Commissioner of Data Protection has the following powers, duties and functions, so far as is reasonably practicable:

(a) accessing Personal Data Processed by Controllers or Processors, which includes having the right to obtain access to any premises of a Controller or Processor who is subject to this Law and to any Processing equipment, means and records;

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

(c) issuing warnings or admonishments and making recommendations to Controllers and Processors, including ordering the appointment of a DPO as described in Article 16(4);

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

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

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

(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) promote, as appropriate, and deal 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 of Data Protection;

(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 it 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 of Data Protection by the President pursuant to the provisions of this Law.

(4) The Commissioner of Data Protection has power to do whatever he deems necessary, for or in connection with, or reasonably incidental to, the performance of his functions.

(5) In exercising his powers and performing his functions the Commissioner of Data Protection shall act in an independent and impartial manner and will not accept instructions from any other party.

47 **Delegation of powers and establishment of advisory committee**

(1) The Commissioner of Data Protection, where he considers it appropriate to do so, may delegate such of his functions and powers as may more efficiently and effectively be performed by officers

and employees of the Commissioner of Data Protection, and with the approval of the DIFCA Board of Directors, either generally or in relation to any particular matter, to any other person.

(2) The Commissioner of Data Protection may establish an advisory committee. The Commissioner of Data Protection may appoint a chairperson and a secretariat.

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

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

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

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

(d) providing input, as requested by the Commissioner of Data Protection, into any question arising under this Law which the Commissioner of Data Protection is required to consider;

(e) preparing reports for the Commissioner of Data Protection; and

(f) liaising with other data protection committees and authorities as directed by the Commissioner of Data Protection.

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

48 **Codes of conduct**

(1) The Commissioner of Data Protection shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Law. Specific codes may be developed which take account of the features of the various Processing sectors and the specific needs of different types of enterprises.

(2) Associations and other bodies representing categories of Controllers or Processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Law. Matters which such codes may cover include:

(a) fair and transparent Processing;

(b) the legitimate interests pursued by Controllers in specific contexts;

(c) the collection of Personal Data;

(d) the pseudonymisation of Personal Data;

(e) the information provided to the public and to Data Subjects;

(f) the exercise of the rights of Data Subjects;

(g) the measures and procedures referred to in Article 14;

(h) the notification of Personal Data Breaches to the Commissioner of Data Protection and the communication of such Personal Data Breaches to Data Subjects;

(i) the transfer of Personal Data to third countries or International Organisations; or

(j) out-of-court proceedings and other dispute resolution procedures for resolving disputes between Controllers and Data Subjects with regard to Processing, without prejudice to the rights of Data Subjects pursuant to Articles 60 and 64.

(3) A code of conduct referred to in Article 48(2) shall contain mechanisms which enable the relevant association or representative body to carry out the monitoring of compliance with its provisions by the Controllers or Processors which undertake to apply it, without prejudice to the tasks and powers of the Commissioner of Data Protection.

(4) Associations and representative bodies referred to in Article 48(2) which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the Commissioner of Data Protection. The Commissioner of Data Protection shall confirm whether or not the draft code is approved.

(5) Where the Commissioner of Data Protection 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.

49 **Monitoring of approved codes of conduct**

(1) Without prejudice to the tasks and powers of the Commissioner of Data Protection, the monitoring of compliance with a code of conduct approved pursuant to Article 48 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Commissioner of Data Protection.

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

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

(b) established procedures which allow it to assess the eligibility of Controllers and Processors concerned to apply the code, to monitor their 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 and the public; and

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

The Commissioner of Data Protection will revoke accreditation if it believes the above conditions are not met or if the body has infringed this Law.

(3) Without prejudice to the tasks and powers of the Commissioner of Data Protection, 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 the Controller or Processor concerned from the code. It shall inform the Commissioner of Data Protection of such actions and the reasons for taking them.

50 **Certification schemes**

(1) Bodies may seek to establish certification schemes for the purposes of enabling Controllers and Processors to demonstrate compliance with this Law. Participation in certification schemes shall be voluntary and available by a transparent process.

(2) Any certification achieved by the Controller or Processor does not relieve them of any responsibility for compliance with this Law and is without prejudice to the tasks and powers of the Commissioner of Data Protection.

(3) Certification may be issued by a certification body approved under Article 51 or by the Commissioner of Data Protection (if it establishes its own certification scheme); no other body may issue certification concerned with compliance with this Law.

(4) Any certification issued under a scheme run by an approved body or the Commissioner of Data Protection shall be for a maximum period of three 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 of Data Protection must withdraw the certification of any Controller or Processor who is found to no longer meet the requirements for certification.

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

51 **Certification bodies**

(1) A body may apply to the Commissioner of Data Protection to be accredited for the purposes of running a certification scheme referred to in Article 50.

(2) The Commissioner of Data Protection shall only accredit a body which has:

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

(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;

(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 the Controller or Processor, and to make those procedures and structures transparent to Data Subjects and the public;

(e) demonstrated, to the satisfaction of the Commissioner of Data Protection, 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 of Data Protection and made public from time to time, whether via Regulations or otherwise.

The Commissioner of Data Protection will revoke accreditation if it believes the above conditions are not met or if the body has infringed this Law.

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

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

(5) When accredited, a certification body is responsible for the proper assessment of Controllers and Processors leading to the certification or the refusal or withdrawal of certification without prejudice to the responsibility of the Controller or Processor for compliance with this Law.

52 **Production of information**

(1) The Commissioner of Data Protection 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 which relate to the Processing of Personal Data.

(2) The party in respect of whom a requirement is made pursuant to Article 52(1) shall comply with that requirement. Where the party fails to comply with the requirement it shall be in breach of this Law. The Commissioner of Data Protection 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 of Data Protection, may make Regulations under the Law in respect of:

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

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

(2) The Commissioner of Data Protection may propose Regulations to the DIFCA Board of Directors in respect of any matter that facilitates the administration and application of the Law or furthers the purposes of the Law, including but not limited to:

(a) the development and publication of information to DIFC entities and their employees concerning the application and interpretation of the Law and Regulations;

(b) procedures for initiating and filing complaints;

(c) procedures for appealing and reconsidering decisions or determinations of the Commissioner of Data Protection;

(d) fines;

(e) fees;

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

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

(h) the conduct of the Commissioner of Data Protection and his officers, employees and agents in relation to the exercise of powers and performance of functions.

(3) Where the DIFCA Board of Directors issues a standard or code of practice, it may incorporate such a standard or code into the Regulations by reference and in such circumstances, except to the extent that the Regulations otherwise provide, a person who is subject to the provisions of any such standard or code shall comply with such provisions as if they were provisions of the Regulations.

(4) Where any 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 of Data Protection 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 of Data Protection concludes that any delay likely to arise under such Articles is prejudicial to the interests of the DIFC or to Data Subjects.

54 **Funding**

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

55 **Annual funding of the Commissioner of Data Protection**

(1) The Commissioner of Data Protection shall submit to the President for approval estimates of the annual income and expenditure of the Commissioner of Data Protection for the next financial year as approved by the DIFCA Board of Directors no later than forty five (45) days before the end of the current financial year.

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

(3) The President in consultation with the DIFCA Board of Directors may accept or reject such estimates within forty-five (45) days of receiving them, in writing to the Commissioner of Data Protection and where relevant state the reasons for rejection.

56 **Accounts**

(1) The Commissioner of Data Protection shall keep proper accounts of its financial activities.

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

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

57 **Audit of Commissioner of Data Protection**

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

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

(3) The auditors shall prepare a report on the financial statements and send the report to the DIFCA Board of Directors.

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

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

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

(7) A person shall not without reasonable excuse intentionally engage in conduct that results in the obstruction of a person appointed under Article 57(1) in the exercise of his powers.

58 **Annual report**

(1) As soon as practicable after 1 January in each year, the Commissioner of Data Protection shall deliver to the President, a report on the management of the administrative affairs of the Commissioner of Data Protection, for the previous year.

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

PART 9: REMEDIES, LIABILITY AND SANCTIONS

59 Directions

(1) If the Commissioner of Data Protection is satisfied, after duly conducting all reasonable and necessary inspections and investigations, 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 of Data Protection shall carry out, as a minimum, due process by means of undertaking all the reasonable and necessary inspections and investigations to be adequately satisfied to establish the Controller's or Processor's contravention with the Law or Regulations made for the purposes of this Law.

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

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

(b) a statement to the effect that the Controller or Processor may seek a review by the Court of the decision of the Commissioner of Data Protection to issue the direction.

(4) A Controller or Processor who fails to comply with a direction of the Commissioner of Data Protection under this part of the Law contravenes this Law and may be subject to fines and liable for payment of damages and compensation to the Data Subject.

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

(a) an order directing the 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 of Data Protection 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 of Data Protection or other person relating to the issue of the direction by the Commissioner of Data Protection or the contravention of such Law, Regulations or Applicable Law relevant to the issue of the direction; or

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

(6) A Controller or Processor may ask the Commissioner of Data Protection to review the direction within fourteen (14) days of receiving a direction under this part of the Law. The Commissioner of Data Protection may receive further submissions and amend or discontinue the direction.

(7) The Commissioner of Data Protection may, but is not obliged to, issue warnings to Controllers or Processors that their intended Processing operations are likely to infringe this Law.

(8) The Commissioner of Data Protection may, but is not obliged to, issue public reprimands to Controllers or Processors where their Processing operations have infringed this Law (in addition to imposing any other sanction provided for under this Law).

60 Lodging complaints and mediation

(1) A Data Subject who believes on reasonable grounds that he has been adversely affected by a contravention of the Law in respect of the Processing of his Personal Data or as regards the exercise of his rights under this Law may lodge a complaint with the Commissioner of Data Protection.

(2) Where multiple Data Subjects are affected by the same alleged contravention or breach of rights, they may raise such complaint collectively, including via a representative body or professional. The Commissioner may choose to deal collectively with multiple allegations which relate to the same contravention or breach of rights, whether or not such allegations are brought collectively or not.

(3) The Commissioner of Data Protection may mediate between the complainant and the relevant Controller and/or Processor.

(4) On the basis of the mediation referred to in Article 60(3), the Commissioner of Data Protection may issue a direction under Article 59.

61 **General contravention**

(1) A Controller or Processor commits a contravention of this Law if he:

(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 of Data Protection has issued a direction); or

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

62 **Administrative imposition of fines**

(1) Where the Commissioner of Data Protection considers that a Controller or Processor has contravened the Law, he may impose by written notice given to the Controller or Processor a fine in respect of the contravention, of such amount as he considers appropriate. The level of such fine will be determined by the Commissioner of Data Protection, taking into account the seriousness of the contravention and the risk and actual harm to Data Subjects.

(2) If, within the period specified in the notice referred to in Article 62(1):

(a) the Controller or Processor (as applicable) pays the prescribed fine to the Commissioner of Data Protection, then no further proceedings may be commenced by the Commissioner of Data Protection against the person in respect of the relevant contravention, however the Commissioner of Data Protection may take action in relation to any continuing contravention to do or refrain from doing any act or thing, including where a direction to the relevant Controller or Processor has been issued in addition to the fine;

(b) has not paid the prescribed fine to the Commissioner of Data Protection, then the Commissioner of Data Protection may apply to the Court for, and the Court may so order, the payment of the fine or so much of the fine as is not paid and make any further order as the Court sees fit for recovery of the fine including any order for interest, costs of enforcement (including legal costs) and other expenses directly arising from to the failure to pay; or

(c) the Controller or Processor (as applicable) takes such action as is prescribed in the Regulations to object to the imposition of the fine, or where no such Regulations have been passed, appeals directly to the Court, then Article 63 shall apply.

(3) A certificate that purports to be signed by the Commissioner of Data Protection and states that a written notice was given to a person pursuant to Article 62(1) if this Law 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(2).

(4) In addition to any administrative fine, the Commissioner of Data Protection may request the Court to make an order for damages or compensation payable to Data Subjects, even if the Data Subject 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 of Data Protection will not usually make such requests unless in its opinion the Data Subjects in question have suffered material damage as a result of the breach in question and are disadvantaged in their ability to bring a claim to the Court in their 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 of Data Protection may appeal to the Court within thirty (30) days.

(2) The Court may make any orders that the Court may think just and appropriate in the circumstances, including remedies for damages, penalties or compensation and imposition of administrative fines and 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 and Processor (if applicable) in question (which is in addition to, and without prejudice to, any fine imposed on the same parties under Article 62).

(2) Any Controller involved in Processing which 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 AND DATA SHARING

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) Without limiting the generality of Article 65(1), Articles 26, 32, 33, 34, 35, 37, 38, and 39 shall not apply to the DFSA, DIFCA and the Registrar ("DIFC Bodies") on a case-by-case basis with respect to each activity of each such DIFC Body, if the application of these Articles would be likely to cause material prejudice to the proper discharge by such body of its powers and functions under any laws administered by it (including any delegated powers and functions), insofar as such powers and functions are designed for protecting members of the public against:

(a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other banking and financial activities and services, including insurance and reinsurance services, financial markets and financial and monetary brokerage services; or

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

(3) The DIFC Bodies do not benefit from blanket exemptions and must take appropriate steps to confirm the exemption applies. To benefit from an exemption the body must inform the Commissioner of Data Protection that it believes it will need to benefit from the exemption, setting out why it requires the exemption, which Articles it requires exemption from, which activities the exemption should apply to, and describing the material prejudice it will suffer without the exemption. The Commissioner of Data Protection will then confirm in writing whether or not such exemption shall apply and publish details of the exemption publicly.

(4) The Commissioner of Data Protection may require any person or body who benefits from exemptions under Articles 65(1) or (2), to certify to him in writing at regular intervals that such person or body remains eligible for the exemption it holds, taking into account the applicable criteria for the exemption. A person or body who contravenes the Law, after becoming ineligible for an exemption which would have prevented such contravention, shall be treated in the same way as any never-exempt person would have been with respect to such contravention.

SCHEDULE 1

1. Rules of interpretation

(1) In the Law, a reference to:

(a) a statutory provision includes a reference to the statutory provision as amended or re-enacted from time to time;

(b) a person includes any natural person, body corporate or body unincorporate, including a company, partnership, unincorporated association, government or state.

(c) an obligation to publish or cause to be published a particular document shall, unless expressly provided otherwise in the Law, include publishing or causing to be published in printed or electronic form;

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

(e) a calendar year shall mean a year of the Gregorian calendar;

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

(g) where relevant the singular shall include the plural and vice versa.

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

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

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

(5) Reference in an Article or other division of this Law to a paragraph, sub-paragraph or Article by number or letter only, and without further identification, is a reference to the paragraph, sub-paragraph or Article of that number or letter contained in the Article or other division of this Law in which that reference occurs.

(6) Unless the context otherwise requires, where this Law refers to an enactment, the reference is to that enactment as amended from time to time, and includes a reference to that enactment as extended or applied by or under another enactment, including any other provision of that enactment.

(7) References in this Law to a writing, filing, instrument or certificate include any mode of communication that preserves a record of the information contained therein and is capable of being reproduced in tangible form, including electronic means.

2. Legislation in the DIFC

References to Applicable Law and guidance in the Law shall be construed in accordance with the following provisions:

(a) Federal Law is law made by the federal government of the United Arab Emirates;

(b) Dubai Law is law made by the Ruler, as applicable in the Emirate of Dubai;

(c) DIFC Law is law made by the Ruler (including, by way of example, the Law), as applicable in the DIFC;

(d) the Law is the Data Protection Law, DIFC Law No.[XX] of [2019] made by the Ruler;

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

(f) Guidance is indicative and non-binding and may comprise

(i) guidance made and issued by the Commissioner of Data Protection for the purposes of this Law; and

(ii) any standard or code of practice issued by the DIFCA Board of Directors.

3. Defined terms

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

Terms	Definitions
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 of Data Protection	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.
DIFC Body	has the meaning provided in Article 65(2)
DPO	a data protection officer, as further described in Articles 16 to 18.
Filing System	any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.
Government of Dubai	the Government of Dubai.
Group	any group of entities which 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 or more of the following applies: (a) new technologies are being deployed which may increase the risk to Data Subjects or render it more difficult for Data Subjects to exercise their rights; (b) a considerable amount of Personal Data will be Processed and where such Processing is likely to result in a high risk to the Data

	Subject, for example, on account of the sensitivity 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; (d) a non-trivial 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 or more factors specific to his / her 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 which is set up by, or on the basis of, an agreement between two or more countries.
Joint Controller	any Controller which jointly determines the purposes and means of Processing with another Controller.
Law	this Data Protection Law **[**2019**]**, as may be amended.
Personal Data	any information referring to an Identified or Identifiable Natural Person.
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 which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restricting (meaning the marking of stored Personal Data with the aim of limiting their Processing 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; and (b) competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of 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 7 of the Companies Law, DIFC Law No.2 of 2009.
Regulations	has the meaning given in Article 2 of Schedule 1 to the Law.
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(8).
Third Country	a jurisdiction other than DIFC, including any other free zone in the UAE.
Third Party	any person other than: (a) the Data Subject; (b) the Controller; (c) the Processor; and (d) the persons who, under the direct control of the Controller or the Processor, are authorized to Process Personal Data.
UAE	the United Arab Emirates.