DATA PROTECTION REGULATIONS

In force on ~~1 July 2020~~XXX 2023

CONTENTS

1. INTRODUCTION

These Regulations may be cited as the "Data Protection Regulations".

1.1 Application and interpretation

1.1.1 In these Regulations a reference to the Law is a reference to the Data Protection Law, DIFC Law No. 5 of 2020.

1.1.2 These Regulations apply to any person to whom the Law applies.

1.1.3 Defined terms are as set out in the Law and are identified throughout these Regulations by the capitalisation of the initial letter of a word or phrase. Where capitalisation of the initial letter is not used, an expression has its natural meaning.

1.1.4 Where reference is made in these Regulations to a statutory provision, it is a reference to the provision as amended, and includes a reference to that provision as extended or applied by or under any other provision, unless the contrary intention appears.

1.1.5 Unless the contrary intention appears:

(a) words in these Regulations importing the masculine gender include the feminine and words importing the feminine gender include the masculine; and

(b) words in these Regulations in the singular include the plural, and words in the plural include the singular; and

1.1.6 The Rules of interpretation in the Law apply to these Regulations.

1.2 References to writing

1.2.1 If a provision in these Regulations refers to a communication, notice, agreement of other document 'in writing' then, unless the contrary intention appears, it means in legible form and capable of being reproduced on paper, irrespective of the medium used. Expressions related to writing must be interpreted accordingly.

1.2.2 This does not affect any other legal requirements which may apply in relation to the form or manner of executing a document or agreement.

2. RECORDS

2.1 Records contents

For the purposes of Article 15(1) of the Law, a Controller must record at least the following information in relation to its Personal Data Processing operations:

(a) description of the Personal Data Processing being carried out;

(b) an explanation of the purpose for the Personal Data Processing;

(c) the Data Subjects or class of Data Subjects whose Personal Data is being processed;

(d) a description of the class of Personal Data being processed; and

(e) a list of the jurisdictions to which Personal Data may be transferred by the Controller, along with an indication as to whether the particular jurisdiction has been assessed as having adequate levels of protection for the purposes of Articles 26 and 27 of the Law.

2.2 Guidance on what constitutes purposes and categories of processing activities

2.2.1 With respect to Regulation 2.1.1(b) the purposes for which Personal Data may be Processed will vary but includes at least one (1) or more of the following:

(a) accounting and auditing;

(b) administration of justice;

(c) administration of membership records;

(d) advertising, marketing and public relations for the Controller itself;

(e) advertising, marketing and public relations for others;

(f) benefits, grants and loans administration;

(g) consultancy and advisory services;

(h) credit referencing;

(i) debt administration and factoring;

(j) education;

(k) information and data bank administration;

(l) insurance administration;

(m) legal services;

(n) licensing and registration;

(o) pastoral care;

(p) pensions administration;

(q) policing;

(r) private investigation;

(s) property management;

(t) provision of financial services;

(u) research; and

(v) staff administration.

2.2.2 With respect to Regulation 2.1.1(c), where Personal Data of multiple Data Subjects is being processed, a Controller may instead of listing individual Data Subjects, record the ~~class~~categories of Data Subject involved. In such a case, the Controller may use the following, or other similar, ~~classes~~categories:

(a) staff, including agents, temporary and casual workers;

(b) clients and customers;

(c) suppliers;

(d) members;

(e) complainants, correspondents and enquirers;

(f) relatives and associates of the Data Subject; and

(g) advisors, consultants and other professional experts.

3. NOTIFICATIONS

3.1 Notifying the Commissioner

3.1.1 For the purposes of Articles 14(7) and 14(8) of the Law, a Controller or Processor must notify the Commissioner of the following Personal Data Processing operations or set of such operations including but not limited to the Processing of:

(a) ~~the Processing of~~ Personal Data;

(b) Special Category Data; and

(c) the transfer of Personal Data to a recipient outside of the DIFC which is not subject to laws and Regulations ~~which~~that ensure an adequate level of protection.

3.1.2 When a Controller or Processor gives a notification to the Commissioner in accordance with Regulation 3.1.1, the notification must contain the following information:

(a) a general description of the Personal Data Processing being carried out;

(b) an explanation of the purpose for the Personal Data Processing;

(c) the Data Subjects or class of Data Subjects whose Personal Data is being processed;

(d) a description of the class of Personal Data being processed; and

(e) a statement of jurisdictions to which Personal Data will be transferred by the Controller, along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection for the purposes of Articles 26 and 27 of the Law.

3.2 Time for filing Notifications

~~3.1.3~~3.2.1 The notification required by Regulation 3.1.1 must be provided to the Commissioner:

(a) as soon as possible and in any event within fourteen (14) days of commencing the Personal Data Processing referred to in Regulation 3.1.1;

(b) on every anniversary of the initial notification, where the Personal Data Processing is to continue in the subsequent year; and

(c) as soon as possible and in any event within fourteen (14) days upon any Personal Data Processing being processed in a manner different to that described in the initial notification.

~~**3.2 Time for filing Notifications**~~

~~Where the Law requires a notification to be filed with the Commissioner, the notification must be filed, in the absence of a time limit being stated in the Law or these Regulations, within fourteen (14) days of the date of the happening of the event to which the notification relates.~~

3.3 Fees

For the purposes of Article 14(8)(b) of the Law, a Controller or Processor must pay any applicable fees in respect of matters set out in Appendix 1.

4. DPO ~~CONTROLLER ASSESSMENT~~CONTROLLER ASSESSMENT

For the purposes of Article 19(3), the Commissioner has approved and published, via the DIFC Client Portal, the format, required content and deadline for submission of Annual Assessments on the Data Protection section of the DIFC website (difc.ae), which may be updated from time to time.

5. ~~TRANSFERS OUT OF THE~~TRANSFERS OUT OF THE DIFC

For the purposes of Article 27(2)(c), the Commissioner has approved and published standard contractual clauses that may be used for transfers outside the DIFC to a non-adequate jurisdiction. These clauses may be updated from time to time, and are available on the Data Protection section of the DIFC website (difc.ae).

6. COMPLAINTS AND MEDIATION

6.1 Process of mediation

6.1.1 For the purposes of Article 60 of the Law, a person may file a complaint with the Commissioner by lodging a written notice providing the following information:

(a) full name and address of the person making the complaint;

(b) the Controller whom the person believes has contravened the Law;

(c) a detailed statement of facts which the person believes gives rise to contravention of the Law; and

(d) the relief sought by the person making the complaint.

6.1.2 Upon receiving a complaint lodged under Article 60 of the Law, the Commissioner may follow such practices and procedures in the mediation of the claim that will, in the view of the Commissioner, lead to the most timely, fair and effective resolution of the claim.

6.1.3 At the conclusion of the mediation process, should the Commissioner determine to issue a direction requiring a Controller to do any act or thing in accordance with Article 60(4) of the Law, he will do so by issuing a notice in writing setting out:

(a) the act or thing that the Controller is required to do; and

(b) the time within which, or before which, the Controller is required to do that act or thing.

7. FINES

7.1 Notice of fines

7.1.1 Where the Commissioner decides to impose a fine pursuant to Article 62(2) of the Law, he will give a Controller or Processor written notice in accordance with Notice 1 or 2, whichever is applicable in Appendix 2:

(a) alleging that reason that the Controller or Processor has committed the contravention and giving particulars of the facts alleged by the Commissioner to constitute a contravention;

(b) setting out the fine imposed by the Commissioner in respect of the contravention;

(c) specifying the period during which the fine may be paid; and

(d) providing an address for filing a notice of objection.

7.1.2 Where a fine is issued pursuant to Article 62(3), the Commissioner will give written notice in substantially the same format as Notice 1 in Appendix 2 and as described in Regulation 7.1.1.

7.2 Notice of Objection

7.2.1 Where a Controller or Processor wishes to file a notice of objection to an administrative fine issued pursuant to Article 62(2) directly to the Commissioner, it must be set out in accordance with Notice 2 of Appendix 2 and must detail every matter which the person believes ought to be taken into account by the Commissioner in determining whether to accept the objection in full or alter the fine amount.

7.2.2 Where a Controller or Processor wishes to file a notice of objection to an administrative fine issued pursuant to Article 62(3) directly to the Commissioner, it must be set out in accordance with Notice 2 of Appendix 2 and must detail every matter which the person believes ought to be taken into account by the Commissioner in determining whether to accept the objection in full or alter the fine amount.

7.2.3 The notice of objection filed under Regulation 7.2.1 or 7.2.2 shall constitute the representations of the relevant person and sets out every matter which the person believes ought to be taken into account by the Registrar in making its decision.

7.2.4 Where a fine is imposed under Article 62 of the Law and the person files a notice of objection within the period specified, the Commissioner may not recover the fine as a debt due until the objection is resolved.

7.2.5 If at the end of the period for payment specified in the notice imposing the fine, the Controller has not paid the full amount of the fine and has not filed a notice of objection, the Commissioner may apply to the Court for payment of the fine, or so much of the fine as is not paid, and any further orders the Court sees fit for recovery of the fine, including any orders for costs.

7.2.6 The Commissioner may withdraw a notice imposing a fine whenever he considers it appropriate.

7.2.7 The administrative fines are set out in Schedule 2 of the Law.

7.3 Application to the Court

7.3.1 Subject to Regulation 5.3.2, the Commissioner may recover the outstanding amount of the fine as a debt due if he has confirmed his decision to impose a fine and the fine remains unpaid, in full or in part.

7.3.2 The Registrar shall not recover the outstanding amount of the fine as a debt due under Regulation 7.3.1, where the person to whom a fine has been imposed makes an application to the Court within thirty (30) days of the date on which the Commissioner confirms his decision, and the Court subsequently determines that the fine should not be payable.

8. PERSONAL DATA BREACHES

8.1 Article 41 Breach – Report to Commissioner

8.1.1 A Controller or Processor shall report a Personal Data Breach to the Commissioner either by writing to commissioner@dp.difc.ae or submitting a form via the Data Protection section of the DIFC website without undue delay after becoming aware of a Personal Data Breach.

8.2 Fine for Failure to Notify an Article 41 or Article 42 Personal Data Breach

8.2.1 If the circumstances surrounding an alleged Personal Data Breach demonstrate to the Commissioner that a Controller or Processor should have notified the Commissioner or the Data Subject of such breach failed to do so, the Commissioner may impose fines or seek sanctions or remedies pursuant to Parts 9 and 10 of the Law.

8.3 Article 42 Breach – Report to Data Subject

8.3.1 The Commissioner may direct a Controller to communicate a Personal Data Breach to all affected Data Subjects, or otherwise direct it to make a public communication regarding a Personal Data Breach, by any reasonable means including but not limited to email, written letter or via media outlets.

8.3.2 Any such direction does not prejudice any other actions or directions that the Commissioner may undertake or provide in accordance with Parts 8, 9 or 10 of the Law.

8.4 Inadvertently Obtaining Personal Data

8.4.1 Where a person ("Party A") inadvertently comes into control or possession of data, documents, devices, computer hardware or software or other information ("Inadvertently Obtained Information") that may contain Personal Data, Party A must reasonably attempt to identify and notify the party/ies that previously were Controllers or Processors thereof (individually or collectively "Party B"), requesting that the same be removed or accepted by Party B by a specified future date.

8.4.2 Where it is apparent to Party A that the Inadvertently Obtained Information contains Personal Data, Party A must take reasonable steps to determine:

(a) the nature of the Personal Data;

(b) the sensitivity of the Personal Data;

(c) whether a Personal Data Breach may have occurred as a consequence of the Inadvertently Obtained Information being under the control or possession of Party A; and

(d) Party A's obligations under the Law as a consequence of it being a Controller or Processor of the Personal Data.

8.4.3 If it is determined pursuant to Regulation 8.4.2 that a Personal Data Breach may have occurred, it must be reported by Party A without undue delay to the Commissioner pursuant to the provisions of Article 41(1) of the Law and Regulation 8.1.1, provided that:

(a) Party A will only be required to provide the information or cooperation required under Article 41(1) of the Law to the extent that can reasonably expected from it as an inadvertent Controller or Processor of the Personal Data concerned; and

(b) such report to the Commissioner being accompanied with an explanation, as to how the Personal Date came into Party A's control or possession.

8.4.4 The Commissioner shall make a determination in respect of a potential Personal Data Breach reported under Regulation 8.4.3 and may:

(a) if there was a Personal Data Breach, impose or seek sanctions or remedies against any Controller or Processor involved in the Personal Data Breach in accordance with the provisions of Regulation 8.2;

(b) direct Party B, or any relevant Controller, to communicate in respect of such Personal Data Breach in the manner prescribed in Regulation 8.3; and

(c) direct or suggest actions to Party A, or any other relevant person, in terms of what needs to be done by it in respect of the Inadvertently Obtained Information.

8.4.5 Where Party B positively responds to a notice provided under Regulation 8.4.1 and removes the Inadvertently Obtained Information from Party A's control or possession, Party A shall take reasonable steps to ensure that the Inadvertently Obtained Information is completely expunged from its records. In such circumstances, any notification responsibility in relation to a Personal Data Breach under Article 41 of the Law shall be Party B.

8.4.6 Where Party A:

(a) cannot identify any party/ies that previously were Controllers or Processors of Inadvertently Obtained Information pursuant to Regulation 8.4.1;

(b) identified Party B but the latter does not positively respond to a request to remove or accept Inadvertently Obtained Information at a specified future date pursuant to Regulation 8.4.1;

(c) cannot establish whether is apparent that Inadvertently Obtained Information contains Personal Data pursuant to Regulation 8.4.2;

(d) cannot establish whether a Personal Data Breach may have occurred as a consequence of the Inadvertently Obtained Information being under the control or possession of Party A pursuant to Regulation 8.4(c); or

(e) any combination of the above occurs,

it shall notify the Commissioner of the same and request directions as to what should be done with the Inadvertently Obtained Information and any Personal Data contained therein.

8.4.7 Where Party A:

(a) fails to act in accordance with the provisions of this Regulation 8.4;

(b) in any way uses or disposes of Inadvertently Obtained Information; or

(c) fails to meet its obligations as a Controller or Processor of Inadvertently Obtained Information,

shall constitute a contravention under Article 61 of the Law and the Commissioner may impose fines or seek sanctions or remedies against Party A pursuant to Parts 9 and 10 of the Law.

9. COLLECTION AND USE OF PERSONAL DATA IN DIGITAL COMMUNICATIONS AND SERVICES

9.1 Digital Communications and Services

9.1.1 For the purposes of this Regulation 9, unless otherwise specified, the phrase "Digital Communications and Services" are comprised of electronic communication and are generally enabled through behavioural advertising, where:

(a) "electronic communications" include but are not limited to:

(i) text or short message service (SMS) messages;

(ii) multimedia messaging service (MMS), which includes media such as videos, pictures, audio clips and GIFs;

(iii) electronic mail (email);

(iv) in-app messaging services;

(v) any digital service that uses artificial intelligence or other technology to enable a messaging service; and

(b) "behavioural advertising" is a means of electronic communication, and includes but is not limited to:

(i) direct marketing;

(ii) use of cookies for personalization, analytics or advertising profile development.

9.2 Notice and Default Settings

9.2.1 In accordance with Article 31 and Article 29(1)(h)(viii) of the Law, a Controller must provide information whether Personal Data will be used for the purposes of enabling Digital Communications and Services in a concise, transparent, intelligible and easily accessible form, using clear and plain language, at the time of collecting the Personal Data.

9.2.2 The Data Subject must be provided an opportunity to refuse or opt out of receiving Digital Communications and Services the first time a Controller collects Personal Data for such purposes.

9.2.3 In accordance with Article 14(4) of the Law, privacy preferences must be set by default such that no more than the minimum Personal Data necessary to deliver or receive the relevant product or services are obtained or collected. The means of selecting privacy preferences available to a Data Subject on first use of a platform or application enabling Digital Communications and Services shall include:

(a) clear, colour-neutral selection boxes or buttons that neither promote nor discourage any particular setting selections;

(b) plain language text explaining the preference settings, that the Data Subject may change them, and how to change them; and

(c) an easily accessible means, such as a preferences link or dashboard, to further alter privacy preferences upon additional use of the platform or application.

9.3 Conditions for Consent in Digital Communications and Services

9.3.1 In accordance with Article 12 of the Law, a Controller who relies on consent for Processing Personal Data for purposes of Digital Communications and Services can only do so on the basis of a clear affirmative act that shows an unambiguous indication of freely given consent by a Data Subject.

9.3.2 Consent pursuant to Regulation 9.3.1 must be provided by a Data Subject in a manner that demonstrates that the Controller can rely on it as a legal basis under Article 10(a) or Article 11(a) of the Law, comprising of at least:

(a) an unticked selection box, or other easy to use method, that enables a positive indication of a Data Subject's understanding of the purpose of collection of Personal Data;

(b) language that clarifies the reason(s) for collecting the Personal Data and the purpose(s) for which it may be used; and

(c) a link to a privacy policy, notice, or other reasonably accessible information regarding how the Data Subject may exercise his rights in relation to his Personal Data that is collected for purposes of Digital Communications and Services, including withdrawal of consent in accordance with Article 32 of the Law.

9.3.3 The following methods are not acceptable means of collecting consent in accordance with the requirements of Regulation 9.3.1 and 9.3.2:

(a) pre-ticked selection boxes;

(b) silence; or

(c) inactivity.

9.3.4 Where a Data Subject has previously contacted a Controller or Processor, or a Data Subject has previously provided an opt-in or consent in accordance with Regulations 9.3.1 and 9.3.2, a Controller may continue to rely on information or the consent previously obtained from a Data Subject, provided that the following obligations are complied with:

(a) the Controller must have obtained any Personal Data included in the information directly from the Data Subject who will receive the Digital Communications and Services;

(b) the Controller must have obtained the Personal Data included in the information in the course of a sale or negotiation of a sale of the Controller's product or a service;

(c) the Digital Communications and Services directed at the Data Subject must pertain to products or services of the Controller similar to what the previous contact or previous consent was based on;

(d) the Controller shall provide the Data Subject with an opportunity to unsubscribe, change preferences, refuse or opt out when subsequent Digital Communications and Services are received by the Data Subject; and

(e) the Controller shall provide a reliable, straightforward means to the Data Subject to withdraw consent at any time, together with the information set out in Articles 22, 32 and 40 of the Law.

10. PERSONAL DATA PROCESSED THROUGH DIGITAL ENABLEMENT TECHNOLOGY SYSTEMS

10.1 Obligations of Controllers and Processors

10.1.1 Where Personal Data is Processed for any lawful purposes set out in the Law, either for use in, or to enable learning processes of, digital enablement technology, such as artificial intelligence and autonomous and automated systems ("Systems"), a Controller, Joint Controller, Processor or Sub-processor that is (a) engaged in, or directs the Systems involved in, such Processing; or (b) operates, supervises or in any way uses the output produced by, the Systems involved in such Processing, must in each case adhere to the general requirements for legitimate and lawful Processing set out in Article 9 of the Law.

10.1.2 In accordance with Regulation 10.1.1, where an application or website service employing Systems to Process Personal Data is used, the following actions must be undertaken by any person that acts (or is deemed under Regulation 10.2.2 to act) as a Controller, Joint Controller, Processor or Sub-processor in respect of such Processing:

(a) notice must be provided in clear and explicit terms upon the initial use of, or access to, the System, alerting users to any underlying technology and processes comprising the System that may undertake further Processing of Personal Data by the System that is not human-initiated or directed, as well as indicating the impact of the use of the System on the exercise of individual rights as provided under the Law in Article 29(1)(h)(ix);

(b) the notice referred to in the previous sub-paragraph must also include a comprehensive, true and plain description of:

(i) the purposes for which Personal Data is Processed by the System;

(ii) the output which the System produces on the basis of such Processing and the manner in which such output is used;

(iii) the principles on the basis of which the System has been developed and designed to operate, including a description of any safeguards built into the System by design to ensure compliance of the Processing of Personal Data by the System with the Law; and

(iv) the codes, certifications or principles that the System complies with, including those promulgated by the Dubai Digital Authority, the Organisation for Economic Cooperation and Development (OECD), the United Nations Educational, Scientific and Cultural Organisation (UNESCO), or the Guidelines for Financial Institutions adopting Enabling Technologies published by the Central Bank of the UAE, Securities and Commodities Authority, Dubai Financial Services Authority, the Financial Services Regulatory Authority and such other codes, certifications and/or principles established by national or international regulatory authorities or bodies as the Commissioner may designate from time to time;

(c) evidence, to be provided upon request by any affected party, of the System's compliance with any applicable audit and/or certification requirements that may be established by the Commissioner from time to time;

(d) evidence, to be provided upon request by any affected party, of any algorithm(s) that instructs the System to seek human intervention that includes a risk and impact assessment of access by the System or information made available to the System that may result in unjust bias;

(e) evidence, to be provided upon request by any relevant party, of an algorithm or algorithms that instruct the Systems to seek human intervention that includes a risk and impact assessment of access

by, or on behalf of, competent government authorities, including law enforcement, for the purposes of prevention or prosecution of alleged or confirmed criminal offenses; and

(f) provide upon request by any relevant party a register listing the following information, including but not limited to:

(i) use cases, Processing activities or categories in which such Systems are used;

(ii) how information in the system can be accessed by Data Subjects in accordance with Articles 32 to 40;

(iii) with which third parties or, to the extent permitting by applicable laws, Requesting Authorities any Personal Data used in the systems is Processed as part of stable arrangements, other than on an occasional basis;

(iv) where such third parties or Regulatory Authorities are based, if known; and

(v) any other information the Commissioner requests to demonstrate compliance with the Law, these Regulations or other applicable laws.

10.2 General Digital Enablement Technology Concepts

10.2.1 A System developed and utilised in products, services, or other use cases that may impact a Data Subject, negatively or positively, must be designed in accordance with the following concepts:

(a) **Fairness:** Systems should be designed to treat all individuals equally and fairly, regardless of race, gender, or other specifically subjective factors. Additionally, Systems should be designed to avoid potential biases that could lead to unfair outcomes.

(b) **Ethical**: algorithmic decisions and the associated data lineage of a System must be unbiased. This principle is closely linked with the principle of transparency.

(c) **Transparent**: a System must ensure that Processing of Personal Data is explainable to Data Subjects and other stakeholders in non-technical terms, with appropriate supporting evidence.

(d) **Secure**: a System must keep Personal Data protected and kept confidential and prevent data breaches which could cause reputational, psychological, financial, professional or other types of harm.

(e) **Accountability**: a System must have mechanisms in place to ensure responsibility and accountability for enabling its systems and their outcomes. Such mechanisms may include internal governance and control frameworks in place for monitoring the System, processes and projects regularly or external organisation auditing our processes regularly, enabling the assessment of algorithms, data and design processes.

10.2.2 A System may not be used to Process Personal Data unless the System complies with all applicable audit and certification requirements that may be established by the Commissioner from time to time.

10.2.3 For the purposes of Regulation 10 and the Law:

(a) a person shall be deemed to act as a Controller (or, *mutatis mutandis*, a Joint Controller) in respect of the Processing of Personal Data by a System, whether or not the person actually determines the purposes and means of such Processing by the System, if (i) the System is operated by another for the benefit of such person; or (ii) such person uses, or otherwise receives the benefit of, any output generated by the System in connection with such Processing; and

(b) a person shall be deemed to act as a Processor (or, *mutatis mutandis*, a Sub-processor) in respect of the Processing of Personal Data by a System, whether or not the person actually determinatively directs such Processing by the System, if (i) the System is operated by such person; (ii) the System is operated for the benefit of another; and (iii) such person operating the System does not use or otherwise receive the benefit of any output generated by the System as a result of such Processing.

APPENDIX 1 - FEES

1.1 Table of fees

Upon receipt by the Commissioner of Data Protection of:	Category		
	I	II	III
Registration (Notification)	$1,250	$750	$250
Annual renewal of the registration	$500	$250	$100
Amendments to the registrable particulars of the notification	$100	$50	$10
Notification to inform the Commissioner of Data Protection of not Processing Personal Data	Nil	Nil	Nil
Amendments to contact details	Nil	Nil	Nil

1.2 Notes:

1.2.1 Category I includes entities ~~regulated~~authorised by the DFSA;

1.2.2 Category II includes ~~DFSA non-regulated~~ entities not authorised by the DFSA, except retail; and

1.2.3 Category III includes retail entities.

APPENDIX 2 - NOTICES

NOTICE 1 – NOTICE OF FINE

COMMISSIONER OF DATA PROTECTION

NOTICE OF ADMINISTRATIVE FINE PURSUANT TO ARTICLE 62 OF THE DATA PROTECION LAW

To: *Full name and address of Controller or Processor receiving Notice*

1. The Commissioner of Data Protection considers that you have contravened {*provisions alleged to have been contravened}.*

2. The particulars of the facts giving rise to ~~this~~the contravention~~/these contraventions~~(s) are as follows:

   {statement of the facts constituting the contravention}.

3. The main purposes of the imposition of an administrative fine is to minimise or offset any benefit a person may obtain from non-compliance with the Data Protection Law 2020, and to promote high standards of conduct and a culture of compliance by deterring persons from committing contraventions. Taking into account these purposes, the facts set out in paragraph 2 of this Notice of Administrative Fine and the general circumstances of this matter, the following fine is imposed:

   {statement of each contravention and fine imposed}.

4. This fine may be paid at any time before 5pm on {*date}* by forwarding payment to {*address}*.

5. Should you pay this fine prior to 5pm on {*date}*, then no proceedings will be commenced by the Commissioner of Data Protection against you in respect of the contraventions the subject of this notice. However, should you continue to be in contravention of the Law, the Commissioner may take action in respect of any obligation to do or refrain from doing any act or thing.

6. If you object to the imposition of this fine, you may file a notice of objection by sending or delivering such a notice in the form attached, to the following address:

   {address}

7. The notice of objection must contain every matter you wish the Commissioner of Data Protection to take into account in determining whether to commence proceedings in the Court. The notice of objection must be received by the Commissioner of Data Protection before 5pm on {*date}*. Should you file a notice of objection, the Commissioner of Data Protection will take steps with a view to immediately determining whether to commence proceedings against you for payment of the fine.

8. Should you neither pay the full amount of the fine, nor file a notice of objection before 5pm on {*date}*, then the Commissioner of Data Protection may apply to the Court for payment of so much of the fine as remains unpaid, together with costs and any other remedies set out in the Data Protection Law 2020.

9. Should no notice of objection be filed in respect of the imposition of this fine, then the Commissioner of Data Protection may publish details of the matter to which this Notice of Administrative Fine relates.

…… ……

Name: {Commissioner of Data Protection ~~Officer~~or Delegate} Date

~~Delegate of the Commissioner of Data Protection~~

~~NOTICE 2~~

NOTICE 2 - DECISION NOTICE

[ENTITY NAME]
[ENTITY ADDRESS]
Dubai International Financial Centre,
Dubai, United Arab Emirates

Dear Sirs [DATE]

FAILURE TO COMPLY WITH THE NOTICE OF ADMINISTRATIVE FINE PURSUANT TO ARTICLE 62 OF THE DATA PROTECTION LAW, DIFC LAW No. 5 of 2020 ("DATA PROTECTION LAW")

1. You have previously been given notice of contravention of Article 62 of the Data Protection Law and the Data Protection Regulations 2020 (the "Regulations").

2. You are hereby directed to pay the fine referred to in the attached Notice, and to file a notification in accordance with Article 14(7) and 14(8) of the Data Protection Law and Section 3 of the Regulations before 5 pm on [DATE].

3. This fine together with the applicable fee for filing a notification may be paid at any time before 5pm on **[DATE]** by forwarding payment to the Office of the Commissioner of Data Protection, Level 14, The Gate, PO Box 74777, Dubai, UAE. If paid by cheque, the exchange rate for US$1 is AED 3.675.If paid by bank transfer, the payment is to be made to:

   DIFC Investments LLC - Collection

   Account Emirates NBD - Deira Branch

   Account No - 101 - 1434147-605- AED

   Swift Code - EBILAEAD

   IBAN No - AE280260001011434147605

4. Should you not pay the full amount of the fine referred to in the notice before or on **[DATE]**, the Commissioner of Data Protection shall apply to the Court for an order compelling such payment, and may also publish details of the matter to which the attached relates.

…… ……

Name: {Commissioner of Data Protection or Delegate} Date

NOTICE 3

NOTICE OF OBJECTION – Administrative Fine

To: Commissioner of Data Protection
PO Box 74777
DIFC, Dubai
United Arab Emirates

1. I refer to the Notice of Administrative Fine, the details of which are as follows:

   {Date of Notice of Administrative Fine}

   {Controller or Processor to whom such Notice was addressed}

   {Date for lodgement of notice of objection as stated in Notice of Administrative Fine}

2. I object to the imposition of the fine or so much of the fine that relates to *{the details of aspects disputed}*.

3. {If the Controller or Processor to whom the Notice of Administrative Fine is addressed is not the responsible Controller or Processor: I hold the position of {*position}* within {*Controller or Processor to whom Notice of Administrative Fine is addressed}* and I am authorised on its behalf to file this notice of objection}.

4. In determining whether to {*commence proceedings in the Court*} I believe that the Commissioner of Data Protection ought to take into account the following matters:

   {*detailed statement of relevant matters*}

…… ……

Name of Company: Date

APPENDIX 3 - ADEQUATE JURISDICTIONS

1.1 List of adequate jurisdictions under Article 26(2) of the Law

Abu Dhabi Global Market	Romania
Austria	Singapore~~Portugal~~
Belgium	Slovakia~~Romania~~
Bulgaria	Slovenia ~~Slovakia~~
Colombia	South Korea
Croatia	Spain~~Slovenia~~
Cyprus	Sweden~~Spain~~
Czech Republic	United Kingdom~~Sweden~~
Denmark	Iceland~~United Kingdom~~
~~Estonia~~	~~Iceland~~
Estonia~~Finland~~	Liechtenstein
Finland~~France~~	Norway
France~~Greece~~	Andorra
Greece~~Germany~~	Argentina
Germany~~Hungary~~	Canada
Hungary~~Ireland~~	Faroe Islands
Ireland~~Italy~~	Guernsey
Italy~~Latvia~~	Isle of Man
Latvia	Japan
Lithuania	Jersey~~Japan~~
Luxembourg	New Zealand~~Jersey~~
Malta	Switzerland~~New Zealand~~
Netherlands	Uruguay~~Switzerland~~
Poland	~~Uruguay~~
Portugal	~~Abu Dhabi Global Market~~

1.2 Guidance:

1.2.1 Pursuant to Article 26(2) of the Law, the Commissioner may from time to time approve other jurisdictions, in addition to those listed in 1.1 above, as having an adequate level of protection for Personal Data. The Data Protection section of the DIFC website contains the most up to date version of the above list.

~~1.2.2 Privacy Shield, which replaced Safe Harbor in 2016, is a mechanism recognised by the European Commission for transferring personal data between the European Union / European Economic Area and the United States of America only. The DIFC does not recognise it for this reason, as DIFC has no such agreement in place for transfers of personal data from the DIFC to the United States of America. Therefore Privacy Shield cannot be relied upon for transfers from the DIFC to the United States of America.~~