DATA PROTECTION REGULATIONS

Consolidated Version No. 2
In force on 1 September 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 of Processing Activities ("RoPA")

2.1.1 For the purposes of Article 15 of the Law, a Controller or Processor shall, as a minimum, record the information set out in Article 15(1)(a) to (h) in an electronic format, or other similar database, in relation to its Personal Data Processing operations.

2.1.2 A Controller or Processor shall make the RoPA available to the Commissioner when requested to do so.

2.1.3 A Controller or Processor is required to ensure the RoPA is accurate and up to date in accordance with the requirements set out in Article 15 of the Law.

2.1.4 The RoPA shall include, or where possible shall link to, documentation covering:

(a) information such as the lawful basis for the processing and sources of the personal data;

(b) records of consent, if any;

(c) Controller and Processor contracts;

(d) the location of personal data;

(e) data protection impact assessments;

(f) records of personal data breaches;

(g) information required for processing Special Categories of Data or criminal conviction and offence related data; and

(h) retention and erasure policy documents.

2.2 Applicability

The obligations set out in Article 15 and in Regulation 2 shall not apply to a Controller or Processor employing fewer than fifty (50) persons unless it engages in High Risk Processing Activities.

3. NOTIFICATIONS TO THE COMMISSIONER OF PROCESSING OPERATIONS

3.1 Contents of the Notification

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) Personal Data;

(b) Special Categories of Data; and

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

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

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

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

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

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

(h) 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

3.2.1 The notification required by Regulation 3 must be provided to the Commissioner:

(a) as soon as possible and in any event within thirty (30) 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 thirty (30)days upon any Personal Data Processing being processed in a manner different to that described in the initial notification.

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. SUPERVISION AND MONITORING

4.1 Submission of Annual Assessment

4.1.1 For the purposes of Article 19(3) of the Law, the Commissioner has approved and published, via the DIFC Client Portal, the format, required content and deadline for submission of Annual Assessments, which may be updated from time to time.

4.1.2 Failure to Submit Annual Assessment

(a) If a Controller fails to submit an Annual Assessment within the prescribed time period, or if an Annual Assessment is incomplete, the Commissioner may direct the Controller to submit the Annual Assessment or submit a complete Annual Assessment within a further fixed time period, if proper justification is provided by the Controller for such extension.

(b) Where no proper justification is provided by a Controller pursuant to Regulation 4.1.2(a), the Commissioner may fine a Controller accordingly, including (but not limited to) a fine for failure to respond, an administrative fine for non-compliance with the Law as set out in Article 62(2) and Schedule 2 of the Law, or for any other contravention in accordance with Article 62(3) of the Law.

4.2 Inspections

4.2.1 Where the Commissioner exercises his power to conduct investigations and inspections to verify compliance with the Law in accordance with Article 46(3)(b), a Controller or Processor that receives a notice of inspection from the Commissioner's Office shall respond to any questions asked or provide any information requested in the notice within the time prescribed in the notice.

4.2.2 Failure to comply with notice of inspection

(a) If a Controller or Processor fails to respond to any question asked, or any information requested in a notice of inspection, or if any such response is incomplete, within the prescribed time period under Regulation 4.2.1, the Commissioner may direct a Controller or Processor to properly provide such responses within a further fixed time period, if proper justification is provided by the Controller or Processor.

(b) Where no proper justification is provided, the Commissioner may issue a fine accordingly to the Controller or Processor, including but not limited to a fine for failure to respond, an administrative fine for non-compliance with the Law as set out in Article 62(2) and Schedule 2 of the Law, or for any other contravention in accordance with Article 62(3) of the Law.

5. TRANSFERS OUT OF THE DIFC

For the purposes of Article 27(2)(c), the Commissioner has approved and published two (2) sets of 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 Processing complaints and procedures for 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 or complaints process, should the Commissioner determine to issue a direction requiring a Controller to do or not 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 or cease doing; and

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

6.2 Unfair or Deceptive Practices

6.2.1 Where a complaint is submitted to the Commissioner asserting that a Controller or Processor has engaged in unfair or deceptive behaviour, the Commissioner may investigate and as necessary take enforcement action against the Controller or Processor engaged in such practices.

6.2.2 Unfair or Deceptive Practices may include (without limitation) misleading notices of processing activities or public representations regarding certifications or adherence to principles, codes and compliance standards, particularly in the context of the obligations set out in Article 9, Article 26, Article 27, Article 29(1)(h)(viii), Article 29(1)(h)(ix), Article 31, Regulation 5 and Regulation 10.

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 for breach of the Law or the Regulations, 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 7.3.2, 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 A Controller 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 Article 42 Breach – Report to Data Subject

8.2.1 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.

8.2.2 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.

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

8.3.1 If the circumstances surrounding an alleged Personal Data Breach demonstrate to the Commissioner that a Controller or Processor should have notified the Commissioner or an affected 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.

8.4 Inadvertently Obtaining Personal Data

8.4.1 Where a person ("Party A") inadvertently comes into control or possession of data in either physical or electronic format, ("Inadvertently Obtained Information"), Party A shall for purposes of the Law be deemed

to be a temporary custodian of such data and shall neither be a Controller or Processor of any Personal Data contained therein.

8.4.2 Party A must reasonably attempt to identify and notify the party/ies that were previously in control or possession of the Inadvertently Obtained Information (individually or collectively "Party B") and, if successful in doing so, requesting that the same be removed or accepted by Party B within a period of thirty (30) days.

8.4.3 Where Party B positively responds to a notice provided under Regulation 8.4.2 and removes the Inadvertently Obtained Information from Party A's control or possession within thirty (30) days, Party A shall take reasonable steps to ensure that the Inadvertently Obtained Information is completely expunged from its records and, in such circumstances, any notification responsibility in relation to a Personal Data Breach related to the Inadvertently Obtained Information coming into the control or possession of Party A under Article 41 of the Law shall be that of Party B.

8.4.4 Where Party B is unreachable, unidentifiable or does not recover the Inadvertently Obtained Information from Party A within thirty (30) days after being notified pursuant to Regulation 8.4.2, Party A shall:

(a) notify the Commissioner of the same and provide possession or control of the Inadvertently Obtained Information to the Commissioner;

(b) provide the Commissioner with the details of how the Inadvertently Obtained Information came into its possession; and

(c) take reasonable steps to expunge the Inadvertently Obtained Information from its own records.

8.4.5 Where the Commissioner receives a notice pursuant to Regulation 8.4.4(a), he may attempt to access any Inadvertently Obtained Information in his possession or control as a consequence of such notice and, if he is capable of doing so, the Commissioner shall make a determination whether the Inadvertently Obtained Information contains any Personal Data and whether a Personal Data Breach occurred, in which case he may, where possible:

(a) impose sanctions or remedies against Party B, or any relevant Controller, in accordance with the Law and these Regulations in respect of such Personal Data Breach;

(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;

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

(d) order Party B to pay the costs related to storage, access, assessment, disposal or any other treatment considered reasonable by the Commissioner of the contents of the Inadvertently Obtained Information, either directly or via court order where necessary.

8.4.6 Where Party A:

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

(b) in any way uses or disposes of Inadvertently Obtained Information for its own benefit,

such actions shall constitute a contravention under Article 61 of the Law and the Commissioner may issue directions, impose fines or seek sanctions or remedies against Party A pursuant to Parts 9 and 10 of the Law where it is necessary and proportionate to do so.

8.4.7 Party A may seek costs from Party B for expenses related to the storage, assessment, disposal or other treatment of the contents of the Inadvertently Obtained Information, either directly or via court order where necessary.

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 communications 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; or

(iii) pixel tracking, in-app tracking capabilities or cross-app tracking and information exchange for targeted marketing.

9.2 Notice and Default Settings

9.2.1 In accordance with Article 29(1)(h)(viii) and Article 31 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, so 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 to use the Personal Data for specific, distinguishable purposes or for one (1) or more matters not expressly concerned with the Processing of Personal Data.

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) providing an unticked selection box, or other easy to use method, that enables a Data Subject to submit a positive selection or other 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, understandable 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 previous contact took place with a Data Subject, or previous consent has been provided by a Data Subject 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 at any time or when subsequent Digital Communications and Services are received by the Data Subject;

(e) the Controller implements appropriate and proportionate measures to assess the ongoing validity of the consent, including contacting the Data Subject without delay to reaffirm consent if the Controller's assessment determines that a Data Subject would no longer reasonably expect the Processing to be continuing; and

(f) 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 AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS

10.1 Autonomous and Semi-Autonomous Systems[1]

10.1.1 For the purposes of this Regulation 10, unless otherwise specified herein:

(a) "System" or "Systems" shall mean any machine-based system operating in an autonomous or semi-autonomous manner, that can:

(i) Process Personal Data for human-defined purposes or purposes that the system itself defines, or both; and

(ii) generate output as a result of or on the basis of such Processing.[2]

(b) "Deployer" means, with respect to a System, the natural or legal person

(i) under whose authority or on whose direction or for whose benefit the System is operated, or

(ii) who receives the benefit of the operation of the System or any output generated by the System

in each case without regard to whether or not the System is operated, supervised or hosted by such person, or such person defines or determines any of the purposes of which Personal Data is Processed by such System.[3]

(c) "Operator" means a Provider that operates or supervises a System on behalf or otherwise for the benefit, and on the direction of a Deployer, in each case without regard to whether or not that Provider exercises any control over the Processing of Personal Data by the System.[4]

(d) "Provider" means a natural or legal person that develops a System, or procures that a System is developed for or on behalf of such person, in each case with a view to providing, commercialising or otherwise making such System available to Operators or Deployers.

10.2 Obligations of Deployers and Operators of Systems

10.2.1 Without limiting any other provision in this Regulation 10, where Personal Data is Processed for use in, or to enable the learning processes of, any System, a Deployer or an Operator of the Systems involved in such

---

[1] *Guidance on Regulation 10.1:* As a System is itself comprised of data (e.g., the program code of the System), to the extent that a System resembles the physical appearance or behaviour of an Identifiable Natural Person (irrespective of whether the System has been specifically designed or trained to achieve such resemblance, or such resemblance is unintended), then the use or operation of that System (for any purpose and in any manner, and including in circumstances where the System is not used to Process any Personal Data) will be itself considered Processing of Personal Data about that Identifiable Natural Person subject to the Law.

[2] *Guidance on Regulation 10.1.1(a):* The definition of System has been adapted on the basis of the OECD guidelines and the Regulation of the European Union on harmonized rules on AI ("EU AI Act") to encompass systems that are capable of autonomous or semi-autonomous operation. The Law already contains provisions governing the use of automated Processing, so it is not intended that purely automated systems (i.e. systems which have no degree of autonomy in their operation and whose operation is deterministically controlled by humans) should be captured in this definition. With respect to the reference to Personal Data in Regulation 10.1.1(a) , it is anticipated that the definition of Personal Data could be broadly interpreted to encompass identification of virtual personas or similar virtual criteria that identify an individual.

[3] *Guidance on Regulation 10.1.1(b):* The concepts of a "Deployer" and "Operator" of an AI system have been introduced to address the potential problems of applicability of the traditional concepts of a "Controller" and "Processor" in circumstances where no person can be said to be, strictly speaking, "in control" of the processing or "determining" the purposes of the processing. The definition of "Deployer" has been adapted from the eponymous concept in the EU AI Act as well as the concept of "user" in the Management Measures for Generative AI Services promulgated by the Cyberspace Administration of China. The approach adopted in this Regulation is to assign the general responsibilities of a traditional "controller" to the person or entity that authorizes or benefits from the operation of the System and any output it produces, in order to make the "Deployer" generally accountable for its compliance with the Law.

[4] *Guidance on Regulation 10.1.1(c):* By analogy with the concept of a "Deployer", the concept of an "Operator" of the System is introduced to ensure the technical service provider acting on the instructions and for the benefit of a "Deployer" is accountable to the same extent and substantially in the same manner as a traditional "processor".

Processing must in each case adhere to the general requirements and principles for Processing Personal Data set out in Article 9 of the Law.[5]

10.2.2 Where an application or website service employing Systems to Process Personal Data is used, the following actions must be undertaken by a Deployer or an Operator 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 any Processing of Personal Data by the System that is not human-initiated, controlled or directed (for example, if the System is restricted to only Processing Personal Data for specific human-defined purposes, or if the System is capable of defining further purposes for Processing on its own, or can otherwise Process Personal Data for purposes that are not human-defined), 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);[6]

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

(i) the human-defined purposes for which Personal Data is Processed by the System[7];

(ii) all human-defined principles on the basis of which, and all human-defined limits within which, the System is capable of itself defining further purposes for Processing of Personal Data;

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

(iv) 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 this Regulation 10; and

(v) the codes, certifications or principles upon which the System is designed or developed , which may include those promulgated by the Dubai Digital Authority, the Organisation for Economic Cooperation and Development (OECD), the United Nations Educational, Scientific and Cultural Organisation (UNESCO), the National Institute of Standards and Technology (NIST) AI Framework, 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;

[5] *Guidance on Regulation 10.2.1:* Both the "Deployer" as well as the "Operator" of an System must comply with the general requirements for legitimate and lawful processing under the Law in substantially the same manner as a traditional "controller" and "processor".

[6] *Guidance on Regulation 10.2.2(a):* This requirement implements the principle of transparency and is consistent with analogous requirements implemented in the EU and Chinese regulations on the use of AI. Transparency is a fundamental element of the regulatory scheme adopted in Regulation 10 and ensures that concerned individuals who may be impacted by the use of AI in the processing of their personal data are not only made aware of the use of an System, but also provided sufficient details to enable them to make an informed assessment of the risks and ultimately decide whether to take steps to object or withdraw the legal basis permitting the processing by the System.

[7] *Guidance on Regulation 10.2.2(b)(i) – (v):* The regulatory scheme adopted in Regulation 10 categorises the purposes for processing of Personal Data by an System as either "human-defined", that is purposes that are externally pre-defined by humans and "hard coded" into the System, which the System cannot change, or "self-defined" (i.e., purposes which the System is able to generate itself). Any purposes for processing which the System is capable of dynamically generating itself must be contemplated on the basis of an exhaustive set of detailed principles, that are themselves externally predefined by humans and "hard coded" into the System, and which the System cannot change.

(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;[8]

(d) evidence, to be provided upon request by any affected party, of any algorithm(s) that causes the System to seek human intervention when Processing of Personal Data by the System may result in an unfair or discriminatory impact on a Data Subject, as well as a risk and impact assessment of the risk that Processing by the System of information made available to the System may result in unjust bias or High Risk Processing;

(e) evidence, to be provided upon request by any relevant party, of an algorithm or algorithms that cause the Systems to seek human intervention in the event any Personal Data Processed by the System must be accessed by, or on behalf of, competent government authorities, including law enforcement, for the purposes of prevention or prosecution of alleged or confirmed criminal offenses, as well as a risk and impact assessment in that respect;

(f) evidence, to be provided upon request by any relevant party, of an algorithm or algorithms that instruct the Systems to seek human intervention in the event any Processing of Personal Data by the System may result in non-compliance with Regulation 9, as well as conducting a risk and impact assessment in that respect; and

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

(i) use cases, necessity and proportionality of Processing activities, or 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 of the Law;

(iii) whether the System will be used solely to make automated decisions;

(iv) with which Third Parties or, to the extent permitted by applicable laws, which Requesting Authorities any Personal Data used in the Systems is Processed as part of stable arrangements, other than on an occasional basis,

(v) with which Third Parties or, to the extent permitted by applicable laws, which Requesting Authorities, any Personal Data used in the Systems is Processed in accordance with one or more of the lawful bases set out in Article 10 or Article 11 of the Law;

(vi) contractual obligations of Joint Controllers, Processors or Sub-processors; and

(vii) where Third Parties or Regulatory Authorities engaged in Processing Personal Data used in the Systems are located and appropriate safeguards for exporting the Personal Data thereto; and

(h) any other information the Commissioner requests to demonstrate compliance with the Law, these Regulations or other applicable laws. Information provided in accordance with Regulation 10.2.2(c), 10.2.2(d), 10.2.2(e) or 10.2.2(f) may be redacted or summarised, as reasonably determined by the Deployer or Operator, solely to the minimum extent necessary to protect their intellectual property rights in, or comply with restrictions under applicable laws, in respect of, the System or any raw data used to train the System, provided that the Deployer or Operator undertaking the summary or redacting (as applicable) must provide to the Commissioner, upon request, the full and unredacted underlying information, and implement any revisions to the

[8] *Guidance on Regulation 10.2.2(c):* The regulatory scheme adopted for Regulation 10 is premised on a permissive certification-based regime for the use of Systems to process Personal Data, rather than requiring that any licenses or registrations be made or obtained from the Commissioner. It is anticipated that the Commissioner will, in future guidance, establish certification requirements that apply to Systems used generally in the processing of Personal Data, as well as additional or different requirements applicable specifically to Systems that are used in High Risk Processing Activities involving Personal Data.

summary or redactions that are required by the Commissioner. The Deployer or Operator may consult with the Commissioner regarding any relevant evidentiary requests or directions at any time.

10.3 General Requirements for Artificial Intelligence Autonomous and Semi-Autonomous Systems

10.3.1 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:[9]

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

(b) **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, including unjust bias, or where possible, mitigate bias that could lead to unfair outcomes.

(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 outcomes. Such mechanisms may include internal governance and control frameworks in place for monitoring the System, processes and projects regularly or external organisation auditing processes regularly, enabling the assessment of algorithms, data and design processes.

10.3.2 No person may use, operate, provide, offer or otherwise make available for commercial use a System to Process Personal Data (or receive the benefit of, or output from, the operation of such System), unless such System:[10]

(a) is capable of Processing Personal Data only for purposes that are human-defined or human-approved, or are defined by the System itself solely on the basis of human-defined principles and solely within the limits of human-defined constraints; and

(b) is designed in compliance with Regulation 10.3.1 and complies with any other applicable audit and certification requirements that may be established by the Commissioner from time to time.

10.3.3 No person may use, operate, provide, offer or otherwise make available for commercial use a System to engage in High Risk Processing Activities, unless:[11]

---

[9] *Guidance on Regulation 10.3.1(a) – (e):* This provision gives force to the fundamental principles of fairness, ethical compliance, transparency, security of operation and accountability that each System that is used to process Personal Data must ultimately comply with. The regulatory purpose of the provision is to establish these principles as overarching requirements that Systems must be designed to comply with. However, the provision purposefully does not limit its application to "developers" of Systems only, because it anticipates that ultimately it may be "Deployers" and "Operators" that, being the visible entities with direct exposure to any data subjects impacted by the operation of the System, must be held accountable for compliance. "Deployers" and "Operators" would then ensure in turn that they procure Systems only from "developers" that can give them contractual comfort of compliance-by-design with these principles.

[10] *Guidance on Regulation 10.3.2:* It is anticipated that the Commissioner will establish, in future guidance, general certification and other requirements applicable to Systems used in the processing of Personal Data. When such requirements are established, all Systems must comply with them. In addition, Systems that are capable of dynamically defining for themselves further purposes of processing must do so strictly within the limits and on the basis of the principles "hard coded" into them by human action.

[11] *Guidance on Regulation 10.3.3:* Given the special nature of High Risk Processing Activities, it is intended that only Systems that fully comply with the specific certification and other requirements established by the Commissioner in future guidance may be used for any High Risk Processing Activities. Furthermore, it is the regulatory intent that no System may be used for High Risk Processing Activities until the Commissioner has promulgated these certification and other requirements.

(a) the Commissioner has established audit and certification requirements applicable to Systems used in High Risk Processing Activities;

(b) the System complies with all such requirements;

(c) the System Processes Personal Data solely for human-defined or human-approved purposes; and

(d) the Deployer or Operator has appointed an Autonomous Systems Officer (ASO), who will have the same or substantially similar competencies, status, role and task of a DPO as set out in Article 17 and Article 18 of the Law.

10.3.4 For the purposes of Regulation 10 and the Law:[12]

(a) a Deployer of a System shall be deemed to act as a Controller (or, mutatis mutandis, a Joint Controller) in respect of the Processing of Personal Data by that System; and

(b) an Operator of a System shall be deemed to act as a Processor (or, *mutatis mutandis*, a Sub-processor) in respect of the Processing of Personal Data by that System.

10.3.5 Data Subjects may submit a complaint challenging the outcome of Processing of Personal Data by such Systems in accordance with Parts 9 and 10 of the Law.

[12] *Guidance on Regulation 10.3.4(a) – (c):* The fundamental principle of accountability adopted in Regulation 10 is to assign to "Deployers" of Systems substantially the same responsibilities as traditional "controllers" and by analogy to "Operators" the same responsibilities as traditional "processors" under the Law. These deeming provisions are essential given the definitions of "Controller" and "Processor" under the Law – a "Deployer" should be accountable for how an System processes Personal Data, even if the "Deployer" does not, strictly speaking, determine the purposes of processing, because it is the "Deployer" who benefits from the operation of the System and under whose authority it operates. To the extent that an System operates fully or semi-autonomously under the authority and for the benefit of its "Deployer", its position is substantially similar to that of an employee within the "Deployer" organisation, and the "Deployer" should be therefore liable for its actions in the same way it may be liable for an employee's actions. As a corollary to that, the "Deployer" will be responsible for ensuring that, when processing Personal Data, the System always operates within the appropriate human-established limits and on the basis of human-established principles, much in the same way the "Deployer" would train and require its employees to process Personal Data on its behalf only in accordance with its privacy policies and processes.

APPENDIX 1 - FEES

1.1 Table of fees

Upon receipt by the Commissioner of Data Protection of:	Category		
	I	II	III
Registration (Notification)	USD1,250	USD750	USD250
Annual renewal of the registration	USD500	USD250	USD100
Amendments to the registrable particulars of the notification	USD100	USD50	USD10
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 authorised by the DFSA;

1.2.2 Category II includes 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 PROTECTION 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 the contravention(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 or Delegate} Date

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 {*provisions of Law alleged to have been contravened}* of the Data Protection Law and {*provisions of Regulations alleged to have been contravened}* 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	Japan
Andorra	Jersey
Argentina	Latvia
Austria	Liechtenstein
Belgium	Lithuania
Bulgaria	Luxembourg
California	Malta
Canada	Netherlands
Colombia	New Zealand
Croatia	Norway
Cyprus	Poland
Czech Republic	Portugal
Denmark	Romania
Estonia	Singapore (Including Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP))
Faroe Islands	Slovakia
Finland	Slovenia
France	South Korea (Including Cross Border Privacy Rules (CBPR))
Germany	Spain
Greece	Sweden
Guernsey	Switzerland
Hungary	United Kingdom
Iceland	Uruguay
Ireland	
Isle of Man	
Italy	

1.2 Additional Jurisdictions for Adequacy Approval

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.