



AIFC DATA PROTECTION REGULATIONS

AIFC REGULATIONS No. 10 OF 2017

**December 20, 2017
Astana, Kazakhstan**



PART 1: GENERAL

1. Name
2. Date of enactment
3. Commencement
4. Legislative authority
5. Application of these Regulations
6. Interpretation
7. Administration of these Regulations

PART 2: PROCESSING OF PERSONAL DATA GENERALLY

8. General requirements
9. Requirements for legitimate Processing
- 9-1. Conditions of consent
- 9-2. Right to withdraw consent
10. Processing of Sensitive Personal Data
- 10-1. Designation of the DPO
- 10-2. The DPO: competencies and status
- 10-3. Role and tasks of the DPO
- 10-4. DPO Data Controller assessment
- 10-5. Data protection impact assessment
11. Transfers out of AIFC
12. Transfers to jurisdictions without adequate level of protection
13. Providing information where Personal Data has been obtained from Data Subject
14. Providing information where Personal Data has not been obtained from Data Subject
15. Processing only on instructions from Data Controller
16. Security of Processing etc.

PART 2-1: JOINT DATA CONTROLLERS AND PROCESSORS

- 16-1. Joint Data Controllers
- 16-2. Data Processors and Data Sub-processors

PART 3: RIGHTS OF DATA SUBJECTS

17. Right to information about Personal Data and to rectification etc.
18. Right to object to Processing

PART 4: NOTIFICATIONS TO COMMISSIONER OF DATA PROTECTION

19. Requirement to notify Commissioner about Personal Data Processing operations etc.
- 19-1. Notification of Personal Data Breaches to the Commissioner
- 19-2. Notification of Personal Data Breaches to a Data Subject
20. Requirement to notify Commissioner of changes in operations
21. Register of Notifications

PART 5: COMMISSIONER OF DATA PROTECTION

22. Appointment of Commissioner etc.
23. Commissioner must act independently
24. Commissioner's Objectives and Functions
- 24-1. Certification schemes
- 24-2. Certification and Accreditation
25. Delegation by Commissioner
26. General power of Commissioner to obtain information
27. Power to adopt rules etc.
28. Publication of proposed rules



- 29. Funding and fees
- 30. Commissioner's annual report

PART 6: REMEDIES, LIABILITY AND SANCTIONS

- 31. Direction to comply with Legislation Administered by the Commissioner
- 32. Lodging complaints and mediation
- 33. Enforceable agreements
- 34. Administrative censures
- 35. Administrative imposition of fines
- 36. Giving false or misleading information to Commissioner etc.
- 37. Court orders for Contraventions on Commissioner's application
- 38. Court orders for compensation

PART 7: GENERAL EXEMPTIONS

- 39. General exemptions

PART 8: MISCELLANEOUS

- 40. Notification of Commissioner's decisions and reasons
- 41. Language

SCHEDULE 1: INTERPRETATION

- 1. Meaning of Legislation Administered by the Commissioner
- 2. When does a Person *Contravene* these Regulations
- 3. Definitions for these Regulations



PART 1: GENERAL

1. Name

These Regulations are *AIFC Data Protection Regulations 2017*.

2. Date of enactment

These Regulations are enacted on the day they are adopted by the Governor.

3. Commencement

These Regulations commence on 1 January 2018.

4. Legislative authority

These Regulations are adopted by the Governor under article 4 of the Constitutional Statute and subparagraph 3) of paragraph 9 of the Management Council Resolution on AIFC Bodies.

5. Application of these Regulations

- (1) These Regulations apply within the jurisdiction of the AIFC.
- (2) These Regulations apply to the Processing of Personal Data:
 - (a) by automated means; and
 - (b) other than by automated means where the Personal Data forms part of a Relevant Filing System or is intended to form part of a Relevant Filing System.
- (3) These Regulations apply as follows:
 - (a) These Regulations apply to the Processing of Personal Data by a Controller or Processor incorporated in the AIFC, regardless of whether the Processing takes place in the AIFC or not.
 - (b) These Regulations apply to a Controller or Processor, regardless of its place of incorporation, that Processes Personal Data in the AIFC as part of arrangements, other than on an occasional basis. These Regulations apply to such Controller or Processor in the context of its Processing activity in the AIFC (and not in a Third Country), including transfers of Personal Data out of the AIFC.
 - (c) For the purposes of this section 5(3), Processing “in the AIFC” occurs when the means or personnel used to conduct the Processing activity are physically located in the AIFC, and Processing “outside the AIFC” is to be interpreted accordingly.
- (4) These Regulations do not apply to the Processing of Personal Data by natural persons in the course of a purely personal or household activity that has no connection to a commercial purpose.
- (5) These Regulations are without prejudice to agreements entered into between 1 or more AIFC Bodies and:
 - (a) Third Country governments or governmental authorities;
 - (b) regulatory bodies or public authorities established under the law of a Third Country;



AIFC DATA PROTECTION REGULATIONS

or

- (c) International Organisations, that address regulating the transfer of Personal Data and include appropriate safeguards for the relevant Data Subjects.

6. Interpretation

Schedule 1 contains definitions and other interpretative provisions used in these Regulations.

7. Administration of these Regulations

These Regulations are administered by the Commissioner of Data Protection.



PART 2: PROCESSING OF PERSONAL DATA GENERALLY

8. General requirements

- (1) A Data Controller must ensure that Personal Data that the Data Controller Processes is:
 - (a) Processed fairly, lawfully and securely; and
 - (b) Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights; and
 - (c) adequate, relevant and not excessive in relation to the purposes for which it is collected or further Processed; and
 - (d) accurate and, if necessary, kept up to date; and
 - (e) kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which it is further Processed.
- (2) A Data Processor must take every reasonable step to ensure that Personal Data that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further Processed, is erased or rectified.

9. Requirements for legitimate Processing

A Data Processor must not Process Personal Data unless:

- (a) the Data Subject has consented in Writing to the Processing of the Personal Data; or
- (b) the Processing is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject for a contract to which the Data Subject intends to become a party; or
- (c) the Processing is necessary to comply with any legal obligation to which the Data Controller is subject; or
- (d) the Processing is necessary for the performance of a task carried out:
 - (i) in the interests of the AIFC; or
 - (ii) in the Exercise of Functions of the AIFCA, the AFSA, the Court, the Security Registrar or the Registrar of Companies that are vested in the Data Controller or in a Third Party to whom the Personal Data is disclosed; or
- (e) the Processing is necessary for the purposes of the legitimate interests of the Data Controller or of the Third Party or parties to whom the Personal Data is disclosed, except if those interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation.

9-1. Conditions of consent

- (1) A Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent if it is to be relied on as a basis for Processing under section 9(a) or under section 10(a). If the performance of an act by a Data Controller, a Data Subject or any other party, (including the performance of contractual obligations), is conditional on



AIFIC DATA PROTECTION REGULATIONS

the provision of consent to Process Personal Data, then such consent will not be considered to be freely given with respect to any Processing that is not reasonably necessary for the performance of such act or where the consent relates to excessive categories of Personal Data.

- (2) Where Processing is based on consent, a Data Controller must be able to demonstrate that consent has been freely given.
- (3) If the Processing is intended to cover multiple purposes, consent must be obtained for each purpose in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language.
- (4) If a Data Controller seeks to obtain consent for 1 or more other matters not expressly concerned with the Processing of Personal Data, the request for consent for the Processing of Personal Data must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
- (5) A Data Subject may withdraw consent at any time in accordance with the right afforded to Data Subjects under section 9-2. A Data Subject must be informed of this right and how to exercise it as set out in section 9-2 at the time consent is obtained. Withdrawing consent must not require undue effort on the part of the Data Subject and must be at least as easy as the process of giving consent. Withdrawal of consent does not affect the lawfulness of Processing carried out before the date of withdrawal. Where consent is withdrawn a Data Controller must comply with section 18.
- (6) Other than for the purpose of a Single Discrete Incident, where a Data Controller relies on a Data Subject's consent for Processing, the Data Controller must implement appropriate and proportionate measures to assess the ongoing validity of the consent. This includes considering whether the Data Subject, acting reasonably, would expect Processing to continue based on the consent given, taking into account the circumstances and the terms of such consent.
- (7) Where such ongoing assessment conducted in accordance with section 9-1(6) concludes that a Data Subject would no longer reasonably expect the Processing to be continuing, he must be contacted without delay and asked to re-affirm consent.
- (8) In the circumstances referred to in section 9-1(7), consent is deemed to be withdrawn if there is no positive act of re-affirmation of consent within a reasonable period after a Data Subject has been contacted.
- (9) A Data Controller must be able to demonstrate to the Commissioner that appropriate methods and procedures are in place to manage the recording of consent and the withdrawal of consent, and that periodic evaluations of the same are conducted.
- (10) Where Processing is not a Single Discrete Incident and continues on the basis of consent, a Data Subject must be given the opportunity to re-affirm or withdraw consent on a periodic basis.
- (11) A "Single Discrete Incident" means a Processing operation or a collection of Processing operations that relate to a:
 - (a) single, non-recurring transaction; or
 - (b) non-recurring and clearly defined purpose that a Data Subject is seeking to achieve, in each case, with a definable end point.
- (12) For the avoidance of doubt, consent given for Processing to perform a Single Discrete



AIFC DATA PROTECTION REGULATIONS

Incident remains subject to all foregoing provisions of this section except for Section 9-1(6) and section 9-1(10).

10. Processing of Sensitive Personal Data

- (1) A Data Controller must not Process Sensitive Personal Data unless:
 - (a) the Data Subject has Consented in Writing to the Processing of the Sensitive Personal Data; or
 - (b) the Processing is necessary to carry out the obligations and specific rights of the Data Controller; or
 - (c) the Processing is necessary to protect the vital interests of the Data Subject or another Person and the Data Subject is physically or legally incapable of giving consent; or
 - (d) all of the following subparagraphs are complied with:
 - (i) the Processing is carried out by a foundation, association or another non-profit body in the course of its legitimate activities with appropriate guarantees;
 - (ii) the Processing relates solely to the members of the body or to Persons who have regular contact with it in connection with its purposes;
 - (iii) the Personal Data of a Data Subject is not disclosed to a Third Party without the Written consent of the Data Subject; or
 - (e) the Processing relates to Personal Data that is manifestly made public by the Data Subject or is necessary to establish, exercise or defend a legal claim; or
 - (f) the Processing is necessary to comply with any legal obligation to which the Data Controller is subject; or
 - (g) the Processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, if the interests are pursued in accordance with international financial standards and the interests are not overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
 - (h) the Processing is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter terrorist financing requirements, or requirements relating to the prevention or detection of any crime, that apply to the Data Controller; or
 - (i) the Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services and the Personal Data is Processed by a health professional subject, under national laws or regulations established by national competent bodies, to an obligation of professional secrecy or by another Person also subject to an equivalent obligation of secrecy; or
 - (j) the Processing is required for protecting members of the public against:
 - (i) financial loss caused by dishonesty, malpractice or other seriously improper



AIFC DATA PROTECTION REGULATIONS

- 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.
- (2) Subsection (1) does not apply to the Processing of Sensitive Personal Data by a Data Controller if a permit issued by the Commissioner of Data Protection authorises the Data Controller to Process the Sensitive Personal Data.
- (3) The Commissioner of Data Protection may issue a permit under subsection (2) to a Data Controller subject to any conditions or restrictions the Commissioner considers appropriate, including conditions or restrictions for the purpose of ensuring that the Data Controller applies adequate safeguards in relation to the Processing of Sensitive Personal Data.
- (4) A Data Controller must not Contravene a condition or restriction of a permit issued to the Data Controller under subsection (2).
- (5) Contravention of subsection (4) is punishable by a fine.

10-1. Designation of the DPO

- (1) A Data Controller or Data Processor may elect to appoint a DPO that meets the requirements of section 10-2.
- (2) Notwithstanding section 10-1(1), a DPO must be appointed by:
- (a) AIFC Bodies, other than the Courts acting in their judicial capacity; and
- (b) a Data Controller or Data Processor performing High Risk Processing Activities on a systematic or regular basis.
- (3) A Data Controller or Data Processor to which section 10-1(2)(b) does not apply may be required to designate a DPO by the Commissioner.
- (4) If a Data Controller or Data Processor is not required to appoint a DPO, it must clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations under these Regulations, or any other applicable data protection law, within its organisation and be able to provide details of the persons with such responsibility to the Commissioner upon request.
- (5) The role of a DPO may be performed by a member of a Data Controller's or Data Processor's staff, an individual employed within a Data Controller's or Data Processor's Group in accordance with section 10-1(6) or by a third party under a service contract.
- (6) A Group may appoint a single DPO provided that he is easily accessible from each entity in the Group.
- (7) A DPO must reside in the Republic of Kazakhstan unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis.
- (8) A Data Controller or Data Processor must publish the contact details of its DPO in a



AIFIC DATA PROTECTION REGULATIONS

manner that is readily accessible to third parties, such that a third party could determine how to contact the DPO without disproportionate effort. On request, a Data Controller or Data Processor must confirm identity of its DPO to the Commissioner in writing.

10-2. The DPO: competencies and status

- (1) A DPO must have knowledge of these Regulations and its requirements and must ensure a Data Controller or Data Processor monitors compliance with these Regulations.
- (2) A DPO must:
 - (a) have the ability to fulfil the tasks in section 10-3;
 - (b) be able to perform his duties and tasks in an independent manner, and be able to act on his own authority;
 - (c) have direct access and report to senior management of the Data Controller or Data Processor;
 - (d) have sufficient resources to perform his duties in an effective, objective and independent manner; and
 - (e) have timely and unrestricted access to information within the Data Controller or Data Processor organisation to carry out his duties and responsibilities under these Regulations.
- (3) Without prejudice to the mandatory notification requirements under these Regulations, a DPO must be transparent and cooperative with the Commissioner and must notify the Commissioner of all relevant information within the Data Controller or Data Processor organisation, other than information that is subject to legal privilege or a conflicting obligation of non-disclosure under the Applicable Law.
- (4) Subject to section 10-3(1)(c), a DPO may hold other roles or titles within a Data Controller or Data Processor or within each such Group, and may fulfil additional tasks and duties other than those described in these Regulations.

10-3. Role and tasks of the DPO

- (1) A Data Controller or Data Processor must ensure that:
 - (a) its DPO is properly involved in a timely manner, on all issues relating to the protection of Personal Data and is given sufficient resources necessary to carry out the role;
 - (b) its DPO is free to act independently; and
 - (c) any additional tasks and duties fulfilled by its DPO, other than those required under these Regulations, do not result in a conflict of interest or otherwise prevent the proper performance of the role of the DPO.
- (2) A Data Subject may contact the DPO of a Data Controller or Data Processor with regard to all issues related to the Processing of his Personal Data and to the exercise of his rights under these Regulations.
- (3) A DPO performs at least the following tasks:
 - (a) monitor a Controller or Processor's compliance with:



AIFC DATA PROTECTION REGULATIONS

- (i) these Regulations;
 - (ii) any other data protection or privacy-related laws or regulations to which the organisation is subject within the AIFC; and
 - (iii) any policies relating to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in Processing operations, and the related audits;
- (b) inform and advise a Data Controller or Data Processor and its employees who carry out Processing of its obligations pursuant to these Regulations and to other data protection provisions, including where the organisation is subject to overseas provisions with extra-territorial effect;
 - (c) provide advice where requested in relation to data protection impact assessments undertaken pursuant to section 10-5;
 - (d) cooperate with the Commissioner in accordance with section 10-2(3);
 - (e) act as the contact point for the Commissioner on issues relating to Processing; and
 - (f) receive and act upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued or made by the Commissioner.

10-4. DPO Data Controller assessment

- (1) Where a Data Controller is required to appoint a DPO under sections 10-1(2) or 10-1(3), the DPO undertakes an assessment of the Data Controller's Processing activities, at least once per year ("the Annual Assessment"), which will be submitted to the Commissioner.
- (2) A Data Controller reports on its Processing activities in the Annual Assessment and indicate whether it intends to perform High Risk Processing Activities in the following annual period.
- (3) The Commissioner must prescribe and make publicly available the format, required content and deadline for submission of Annual Assessments.

10-5. Data protection impact assessment

- (1) Prior to undertaking High Risk Processing Activities a Data Controller must carry out an assessment of the impact of the proposed Processing operations on the protection of Personal Data, considering the risks to the rights of the Data Subjects concerned. A Data Controller may also elect to carry out such assessment in relation to the Processing of Personal Data that is not a High Risk Processing Activity.
- (2) A single assessment may address a set of similar Processing operations that present similar risks. If another member of a Data Controller's Group has conducted a data protection impact assessment, complying with the requirements of section 10-5(6), in relation to substantially the same Processing that remains current and accurate, the Data Controller may rely on such data protection impact assessment for the purpose of this section.
- (3) A DPO, where appointed, shall be responsible for overseeing data protection impact assessments.



AIFC DATA PROTECTION REGULATIONS

- (4) The Commissioner may at his discretion publish a non-exhaustive list of types or categories of Processing operations that are considered to be High Risk Processing Activities. Such a list is not intended to be exhaustive and does not absolve a Data Controller from responsibility for complying with these Regulations in all respects with regard to High Risk Processing Activities.
- (5) The Commissioner may also publish a list of the types or categories of Processing operations for which no data protection impact assessment is required.
- (6) A data protection impact assessment must contain at least:
 - (a) a systematic description of the foreseen Processing operations and the purpose(s) of the Processing, including, where applicable, the legitimate interest pursued by a Data Controller;
 - (b) an assessment of the necessity and proportionality of the Processing operations in relation to the purpose(s);
 - (c) identification and consideration of the lawful basis for the Processing, including:
 - (i) where legitimate interests are the basis for Processing, an analysis and explanation of why a Data Controller believes the interests or rights of a Data Subject do not override its interests; and
 - (ii) where consent is the basis for Processing, validation that such consent is validly obtained, consideration of the impact of the withdrawal of consent to such Processing and of how a Data Controller will ensure compliance with the exercise of a Data Subject's right to withdraw consent;
 - (d) an assessment of the risks to the rights of Data Subjects; and
 - (e) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with these Regulations, taking into account the rights and legitimate interests of Data Subjects and other concerned persons.
- (7) Taking into account protection of commercial or public interests or the security of Processing operations, a Data Controller must seek the input of Data Subjects or their representatives on the intended Processing, where appropriate.
- (8) A new data protection impact assessment is not required unless Legislation Administered by the Commissioner requires that it is necessary to carry out such an assessment prior to undertaking Processing activities, where:
 - (a) Processing pursuant to sections 9(c) or 9(d) has a lawful basis in Legislation Administered by the Commissioner to which a Data Controller is subject;
 - (b) Legislation Administered by the Commissioner regulates the specific Processing operation or set of operations in question; and
 - (c) a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that lawful basis.
- (9) A Controller must carry out a review to assess if Processing is performed in accordance with a data protection impact assessment:



AIFC DATA PROTECTION REGULATIONS

- (a) on a regular basis, proportionate to the extent and type of Processing the Controller conducts; or
 - (b) when there is a change in the risk related to the Processing operations.
- (10) A Data Processor appointed, or in the process of being appointed, by a Data Controller to carry out a Processing activity must assist the Data Controller by providing all information reasonably requested by the Data Controller in connection with the relevant data protection impact assessment.

11. Transfers out of AIFC

- (1) A Person must not transfer Personal Data to a Recipient located in a jurisdiction outside the AIFC unless:
 - (a) the jurisdiction has an adequate level of protection for Personal Data; or
 - (b) the transfer complies with section 12 (Transfers to jurisdictions without adequate level of protection).
- (2) For subsection (1), a jurisdiction has an adequate level of protection for Personal Data if the jurisdiction is prescribed under the Rules or approved, in Writing, by the Commissioner of Data Protection.

12. Transfers to jurisdictions without adequate level of protection

- (1) The transfer of Personal Data to a Recipient located in a jurisdiction outside the AIFC complies with this section if:
 - (a) the transfer is authorised by a permit issued by the Commissioner of Data Protection under subsection (2); or
 - (b) the Data Subject has consented in Writing to the transfer of the Personal Data; or
 - (c) the transfer is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject for a contract to which the Data subject intends to become a party; or
 - (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the Data Subject between the Data Controller and a Third Party; or
 - (e) the transfer is necessary or legally required on grounds important to the interests of the AIFC, or is necessary to establish, exercise or defend a legal claim; or
 - (f) the transfer is necessary to protect the vital interests of the Data Subject; or
 - (g) the Personal Data was accessed, in accordance with the Acting Law of the AIFC, from a register (however described) established or maintained under the Acting Law of the AIFC that is accessible either by the public in general or by any Person who can demonstrate a legitimate interest (however described) to access; or
 - (h) the transfer is necessary to comply with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, the police, or another government agency, of any jurisdiction; or



AIFC DATA PROTECTION REGULATIONS

- (i) the transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, if the interests are pursued in accordance with international financial standards and the interests are not overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
 - (j) the transfer is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter terrorist financing requirements, or requirements relating to the prevention or detection of any crime, that apply to the Data Controller.
- (2) The Commissioner of Data Protection may issue permits authorising the transfer of Personal Data to Recipients located in jurisdictions outside the AIFC.
- (3) The Commissioner of Data Protection may issue a permit under subsection (2) to a Person subject to any conditions or restrictions the Commissioner considers appropriate, including conditions or restrictions for the purpose of ensuring that the Person applies adequate safeguards to protect Personal Data to which the permit applies.
- (4) A Person must not Contravene a condition or restriction of a permit issued to the Person under subsection (2).
- (5) Contravention of subsection (4) is punishable by a fine.

13. Providing information where Personal Data has been obtained from Data Subject

- (1) If a Data Controller collects Personal Data from a Data Subject, the Data Controller must give the Data Subject at least the following information as soon as possible after commencing to collect the Personal Data:
 - (a) the identity of the Data Controller;
 - (b) the purposes of the Processing for which the Personal Data has been collected;
 - (c) any further information so far as further information is necessary, having regard to the specific circumstances in which the Personal Data has been collected, to guarantee fair Processing of the Data Subject's Personal Data, including, for example, information about any or all of the following matters as appropriate:
 - (i) the Recipients or categories of Recipients of the Personal Data;
 - (ii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of Failure to reply;
 - (iii) the Data Subject's rights to obtain information about the Personal Data and to rectify, erasure or block the Personal Data;
 - (iv) whether the Personal Data is proposed to be used for direct marketing purposes;
 - (v) whether the Personal Data will be Processed relying on section 9(e) (Requirements for legitimate Processing) or section 10(1)(g) (Processing of Sensitive Personal Data) and, if so, what the provision provides.
- (2) The Data Controller need not give the Data Subject information otherwise required by subsection (1) if the Data Controller reasonably expects that the Data Subject is already aware of the information.



14. Providing information where Personal Data has not been obtained from Data Subject

- (1) This section applies if a Data Controller has Personal Data of a Data Subject that was not obtained from the Data Subject.
- (2) The Data Controller must give the Data Subject at least the following information not later than the time the Personal Data is first Processed or, if the Personal Data is to be disclosed to a Third Party, the time the Personal Data is first disclosed to a Third Party:
 - (a) the identity of the Data Controller;
 - (b) if the Personal Data is to be Processed—the purposes of the Processing;
 - (c) any further information so far as further information is necessary, having regard to the specific circumstances in which the Personal Data is Processed, to guarantee fair Processing of the Data Subject's Personal Data, including, for example, information about any or all of the following matters as appropriate:
 - (i) the categories of Personal Data being Processed;
 - (ii) the Recipients or categories of Recipients of the Personal Data;
 - (iii) the Data Subject's rights to obtain information about the Personal Data and to rectify, erasure or block the Personal Data;
 - (iv) whether the Personal Data will be used for direct marketing purposes;
 - (v) whether the Personal Data will be Processed relying on section 9(e) (Requirements for legitimate Processing) or section 10(1)(g) (Processing of Sensitive Personal Data) and, if so, what the provision provides.
- (3) The Data Controller need not give the Data Subject information otherwise required by subsection (2) if:
 - (a) the Data Controller reasonably expects that the Data Subject is already aware of the information; or
 - (b) giving the information to the Data Subject proves impossible or would involve a disproportionate effort.

15. Processing only on instructions from Data Controller

- (1) This section applies to a Person if:
 - (a) the Person is:



- (i) a Data Processor; or
 - (ii) a director, officer, partner, employee or agent of, or another Person acting under, a Data Controller or Data Processor; and
- (b) the Person has access to Personal Data of a Data Subject.
- (2) The Person must not Process the Personal Data unless instructed to do so by the Data Controller or otherwise required to do so by law.

16. Security of Processing etc.

- (1) A Data Controller must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction, or accidental loss, alteration or unauthorised disclosure or access and against all other unlawful forms of Processing or unlawful transfers, particularly when the Processing of Personal Data is performed under section 10 (Processing of Sensitive Personal Data) or Personal Data is transferred to a Recipient located in a jurisdiction outside the AIFC under section 11(1)(b) (Transfers out of AIFC).
- (2) Having regard to the cost of their implementation, the measures must ensure a level of security appropriate to the risks represented by the Processing or transfer and the nature of the Personal Data to be protected.
- (3) If the Processing or transfer of Personal Data is to be performed on behalf of a Data Controller, the Data Controller must choose a Data Processor that can provide appropriate technical and organisational measures to protect the Personal Data, and must ensure that the measures are complied with by the Data processor.
- (4) If there is an unauthorised intrusion, either physical, electronic or otherwise, to any database containing Personal Data, the relevant person must inform the Commissioner of Data Protection of the incident as soon as practicable.
- (5) In subsection (4):

relevant person means:

- (a) the Data Controller; or
- (b) if a Data Processor is performing tasks in relation to the Personal Data on behalf of the Data Controller at the time of the intrusion—the Data Processor.



PART 2-1: JOINT DATA CONTROLLERS AND PROCESSORS

16-1. Joint Data Controllers

- (1) Where 2 or more Persons jointly determine the purposes and means of Processing Personal Data, they will be Joint Data Controllers.
- (2) Joint Data Controllers must, by way of legally binding written agreement, define their respective responsibilities for ensuring compliance with the obligations under these Regulations. Such agreement must clarify the process for ensuring that a Data Subject can exercise his rights under these Regulations and for providing a Data Subject with the information referred to in sections 17 and 18.
- (3) The written agreement referred to in section 16-1(2) or an appropriate summary must be made available to an affected Data Subject.
- (4) Notwithstanding the terms of any written agreement between the Joint Data Controllers, they will remain responsible for all Data Controller obligations under these Regulations and the Data Subject's rights may be exercised under these Regulations in respect of and against each of the Joint Data Controllers, regardless of place of incorporation.

16-2. Data Processors and Data Sub-processors

- (1) Where Processing is to be carried out on behalf of a Data Controller by a Data Processor, the Processing will be governed by a legally binding written agreement between the Data Controller and the Data Processor. A Controller must only enter into agreements with Processors that provide sufficient assurances to implement appropriate technical and organisational measures that ensure the Processing meets the requirements of these Regulations and protects a Data Subject's rights.
- (2) A Data Processor must not engage another Data Processor to act as a Sub-processor without the prior written authorisation of a Data Controller. A Data Controller may only give a general written authorisation where it has ensured that conditions are in place to enable appointed Sub-processors (present or future) to provide the assurances under section 16-2(1). If a general written authorisation has been given, a Data Processor must inform a Data Controller of any intended changes concerning the addition or replacement of a Data Sub-processor. A Processor must take into account any good faith objection raised by a Data Controller to such intended changes.
- (3) Subject to section 16-2(2), a Data Processor may not engage a Data Sub-processor for carrying out specific Processing activities on behalf of the Data Controller, unless a legally binding written agreement containing the requirements set out in section 16-2(5) is in place with such Data Sub-processor that ensures a full delegation of the obligations that the Data Processor owes to the Data Controller under the agreement with the Data Controller in respect of such specific Processing activities.
- (4) Where a Data Sub-processor fails to fulfil its data protection obligations under an agreement or Legislation Administered by the Commissioner, the Data Processor that engaged it will remain fully liable to a relevant Data Controller for the performance of the Data Sub-processor's obligations.
- (5) Each agreement referred to in sections 16-2(1) and 16-2(3):
 - (a) must set out the:



AIFC DATA PROTECTION REGULATIONS

- (i) subject-matter and duration of the Processing;
 - (ii) nature and purpose of the Processing;
 - (iii) type of Personal Data and categories of Data Subjects; and
 - (iv) obligations and rights of the Data Controller; and
- (b) must include commitments that each Data Processor and Data Sub-processor (if any) shall:
- (i) Process Personal Data based on documented instructions from a Data Controller, including sharing of Personal Data in response to a request made by any public authority over the person or any part of its Group, or transfers of Personal Data to a Third Country or an International Organisation, unless required to do so by Legislation Administered by the Commissioner to which the Data Processor is subject;
 - (ii) where Legislation Administered by the Commissioner, as referred to in section 16-2(5)(b)(i), applies:
 - (A) inform any relevant counterparty; or
 - (B) where there is a chain of Processors and Sub-processors, ensure that the Controller is notified, unless the applicable law in question prohibits such information being provided on grounds of substantial public interest;
 - (iii) ensure that persons authorised to Process relevant Personal Data are under legally binding written agreements or duties of confidentiality;
 - (iv) take all measures required pursuant to section 8;
 - (v) comply with the conditions referred to in sections 16-2(2) and (3) for engaging any Data Sub-processor;
 - (vi) assist a relevant counterparty by providing appropriate technical and organisational measures for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights, having taken into account the nature of the Processing;
 - (vii) assist a relevant counterparty in ensuring the Data Controller's compliance with the obligations under these Regulations, taking into account the nature of Processing and the information available to the Data Processor;
 - (viii) delete or return all Personal Data to the Data Controller, at the Data Controller's option, or make the same available for return to a relevant counterparty after the end of the provision of services relating to Processing, and delete existing copies unless Legislation Administered by the Commissioner requires storage of the Personal Data;
 - (ix) make available to the Data Controller, relevant counterparty or the Commissioner (upon request) all necessary information to demonstrate compliance with the obligations in this section; and
 - (x) permit and provide reasonable assistance with audits, including inspections, conducted by:



AIFC DATA PROTECTION REGULATIONS

- (A) a relevant counterparty;
 - (B) another auditor mandated by a relevant counterparty; or
 - (C) the Commissioner.
- (6) A Data Processor or Data Sub-processor must immediately inform the Data Controller or Data Processor (as applicable) whether, in its opinion, the Processing activity infringes these Regulations.
- (7) Adherence by a Data Processor or Data Sub-processor to an approved certification mechanism referred to in section 24-2, may demonstrate the sufficiency of the measures referred to in section 24-1(1) and 24-1(2).
- (8) The Commissioner may publish standard contractual clauses for the matters referred to in section 16-2(1) and (3). The incorporation of such clauses in an applicable written agreement will be sufficient to discharge the obligations in section 16-2(5)(b)(i) to 16-2(5)(b)(x) inclusive.
- (9) If a Data Processor infringes these Regulations by determining the purposes and means of Processing, the Data Processor will be considered to be a Data Controller in respect of that Processing and will assume all the responsibilities and obligations of a Data Controller.
- (10) Both a Data Controller and Data Processor are in breach of these Regulations if they commence mutually agreed Processing activity without a written agreement referred to in sections 16-2(1) and 16-2(3).



PART 3: RIGHTS OF DATA SUBJECTS

17. Right to information about Personal Data and to rectification etc.

A Data Subject (**A**) has the right to obtain from the Data Controller on request, at reasonable intervals and without excessive delay or expense:

- (a) Written confirmation about whether or not Personal Data relating to A is being Processed and Written information at least about the purposes of any Processing, the categories of any Personal Data being Processed, and the Recipients or categories of Recipients to whom any Personal Data is disclosed; and
- (b) communication to A in an intelligible form of the Personal Data being Processed and of any available information about its source; and
- (c) as appropriate, the rectification, erasure or blocking of Personal Data if the Processing of the Personal Data Contravenes these Regulations.

18. Right to object to Processing

- (1) A Data Subject (**A**) has the right:
 - (a) to object at any time, on reasonable grounds relating to A's particular situation, to the Processing of Personal Data relating to A; and
 - (b) to be informed before the Personal Data is disclosed for the first time to a Third Party or used on a Third Party's behalf for the purposes of direct marketing, and to be expressly offered the right to object to such a disclosure or use.
- (2) If there is a justified objection by A in relation to Personal Data, the Data Controller must no longer Process that Personal Data.



PART 4: NOTIFICATIONS TO COMMISSIONER OF DATA PROTECTION

19. Requirement to notify Commissioner about Personal Data Processing operations etc.

- (1) A Data Controller must establish and maintain the records required by the Rules of Personal Data Processing operations performed by or on behalf of the Data Controller.
- (2) The Data Controller must, in accordance with the Rules, notify the Commissioner of Data Protection about the particulars of those Personal Data Processing operations required by the Rules.

19-1. Notification of Personal Data Breaches to the Commissioner

- (1) If there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy, the Data Controller involved must, as soon as practicable in the circumstances, notify the Personal Data Breach to the Commissioner.
- (2) A Data Processor must notify a relevant Data Controller without undue delay after becoming aware of a Personal Data Breach.
- (3) A Data Controller or Data Processor must fully co-operate with any investigation of the Commissioner in relation to a Personal Data Breach.
- (4) The notification referred to in section 19-1(1) must at least:
 - (a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate amount of Personal Data records concerned;
 - (b) communicate the name and contact details of the DPO or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the Personal Data Breach; and
 - (d) describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- (5) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases when available.
- (6) A Data Controller must document in writing any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. The information recorded must be sufficient to enable the Commissioner to verify compliance with this section and must be made available without delay on request.

19-2. Notification of Personal Data Breaches to a Data Subject

- (1) When a Personal Data Breach is likely to result in a high risk to the security or rights of a Data Subject, the Data Controller must communicate the Personal Data Breach to an affected Data Subject as soon as practicable in the circumstances. If there is an immediate risk of damage to the Data Subject, the Data Controller must promptly communicate with the affected Data Subject.
- (2) The communication to the Data Subject referred to in section 19-2(1) must describe in clear and plain language the nature of the Personal Data Breach and contain at least the information provided for in sections 19-1(4)(b) to (d). Such communication must, where



AIFIC DATA PROTECTION REGULATIONS

possible, make recommendations for the Data Subject to mitigate potential adverse effects.

- (3) Where a communication to the individual Data Subjects referred to in Section 19-2(1) will involve disproportionate effort, a public communication or similar measure by the Data Controller whereby the Data Subjects are informed in an equally effective manner will be sufficient.
- (4) If a Data Controller has not already communicated the Personal Data Breach to all relevant Data Subjects, the Commissioner may require it to do so, including where the Commissioner considers that there is a high risk to the security or rights of the Data Subjects involved, or otherwise direct it to make a public communication under section 19-2(3).

20. Requirement to notify Commissioner of changes in operations

- (1) This section applies if:
 - (a) a Data Controller has notified the Commissioner of Data Protection under section 19 (Requirement to notify Commissioner about Personal Data Processing operations etc.) about the particulars of Personal Data Processing operations required by the Rules; and
 - (b) the particulars change.
- (2) The Data Controller must, in accordance with the Rules, notify the Commissioner of Data Protection about the changed particulars.

21. Register of Notifications

- (1) The Commissioner of Data Protection must keep a register (the **Register of Notifications**) relating to the Personal Data Processing operations notified under section 19 (Requirement to notify Commissioner about Personal Data Processing operations etc.).
- (2) The Commissioner of Data Protection must make the register available for inspection by any Person in accordance with the Rules.
- (3) Each entry in the register about Personal Data Processing operations must consist of:
 - (a) the particulars of the operations notified under section 19 or, if any of the particulars have changed, the changed particulars notified under section 20 (Requirement to notify Commissioner of changes in operations); and
 - (b) the other information the Commissioner of Data Protection considers appropriate.
- (4) Any entry in the register is valid for 12 months, but may be renewed for a further period or further periods of 12 months.



PART 5: COMMISSIONER OF DATA PROTECTION

22. Appointment of Commissioner etc.

- (1) The Office of Commissioner of Data Protection is established within the framework of the AIFCA.
- (2) The Board of Directors of the AIFCA must appoint an individual who is appropriately experienced and qualified as the Commissioner of Data Protection, and may dismiss the person from office for incapacity (other than temporary incapacity), misbehaviour or other proper cause.
- (3) The Board of Directors of the AIFCA must consult with the Governor before appointing, reappointing or dismissing the Commissioner of Data Protection.
- (4) The Commissioner of Data Protection is appointed for the period (not longer than 3 years) decided by the Board of Directors of the AIFCA, and may be reappointed for periods (not longer than 3 years at a time) decided by the Board.

23. Commissioner must act independently

The Commissioner of Data Protection must act in an independent way in Exercising the Commissioner's Functions.

24. Commissioner's Objectives and Functions

- (1) The Commissioner of Data Protection must pursue the following objectives (the Commissioner's **Objectives**) in Exercising the Commissioner's Functions:
 - (a) to promote good practices and observance of the requirements of these Regulations, the Rules and any other Legislation Administered by the Commissioner, particularly by Data Controllers;
 - (b) to administer these Regulations, the Rules and any other Legislation Administered by the Commissioner in an effective and transparent way;
 - (c) to prevent, detect and restrain conduct that is, or may be, in a Contravention of these Regulations, the Rules and any other Legislation Administered by the Commissioner;
 - (d) to promote greater awareness and understanding in the AIFC of data protection and the requirements of these Regulation, the Rules and other Legislation Administered by the Commissioner.
- (2) The Commissioner of Data Protection has the Functions given to the Commissioner by or under these Regulations, the Rules or any other AIFC Regulations or AIFC Rules.
- (3) The Commissioner of Data Protection must Exercise the Commissioner's Functions only in pursuit of the Commissioner's Objectives.
- (4) Without limiting subsection (2), the Functions of the Commissioner of Data Protection include the following:
 - (a) issuing warnings or admonishments, and making recommendations, to Data Controllers;



AIFC DATA PROTECTION REGULATIONS

- (b) imposing fines for Contraventions of these Regulations;
 - (c) bringing proceedings in the Court for or in relation to Contraventions of these Regulations, including proceedings for compensation on behalf of Data Subjects;
 - (d) preparing draft rules, standards and codes of practice and submitting them to the Board of Directors of the AIFCA for its consideration;
 - (e) preparing and adopting non-binding guidance for AIFC Participants, and advising the Board of Directors of the AIFCA of any guidance adopted by the Commissioner;
 - (f) issuing or prescribing forms to be used for these Regulations, the Rules or any other Legislation Administered by the Commissioner;
 - (g) issuing or prescribing procedures and requirements relating to these Regulations, the Rules or any other Legislation Administered by the Commissioner;
 - (h) Exercising any Function delegated to the Commissioner under these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (5) The Commissioner of Data Protection may do anything the Commissioner considers necessary or desirable to be done for or in connection with, or reasonably incidental to, the Exercise of the Commissioner's Functions.
- (6) Without limiting subsection (5), the Commissioner of Data Protection may:
- (a) access Personal Data Processed by Data Controllers and Data Processors; or
 - (b) collect information.
- (7) The Commissioner of Data Protection, any member of the AIFCA's staff, and any other delegate or agent of the Commissioner, is not liable for anything done or omitted to be done in the Exercise or purported Exercise of the Commissioner's Functions (including any Function delegated to the Commissioner).
- (8) Subsection (7) does not apply to an act or omission if the act or omission is shown to have been in bad faith.

24-1. Certification schemes

- (1) A certification scheme may be established for the purposes of enabling a Data Controller or Data Processor to demonstrate compliance with these Regulations. Participation in a certification scheme is to be voluntary and available by a transparent process.
- (2) Any certification achieved by a Data Controller or Data Processor does not relieve it of any responsibility for compliance with these Regulations.
- (3) Certification may only be issued by a certification body approved under Section 24-2 or by the Commissioner (if he establishes a certification scheme).
- (4) A certification issued under an approved scheme remains valid for a maximum period of three years and may be renewed for equivalent periods, provided the relevant conditions continue to be met by the Data Controller or Data Processor in question. The approved body or Commissioner must withdraw the certification of a Data Controller or Data Processor that is found to no longer meet the requirements for certification.



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

24-2. Certification and Accreditation

- (1) The Commissioner may receive applications for accreditation for the purposes of running a certification scheme referred to in section 24-1.
- (2) The Commissioner must only award accreditation where a body has:
 - (a) demonstrated independence and expertise in relation to the subject-matter of the certification to the satisfaction of the Commissioner;
 - (b) undertaken in writing to respect the criteria of the proposed scheme;
 - (c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks in connection with the proposed scheme, including establishing explicitly defined specific criteria for granting or not granting certification to an applicant;
 - (d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by a Data Controller or Data Processor, and has made those procedures and structures transparent to Data Subjects and the public;
 - (e) demonstrated, to the satisfaction of the Commissioner, that its tasks and duties do not result in a conflict of interests; and
 - (f) demonstrated its compliance with any criteria for accreditation approved by the Commissioner and made public from time to time, whether via Rules or otherwise.
- (3) The Commissioner must revoke accreditation if he believes the above conditions are not met or if the body has infringed these Regulations.
- (4) The body applying for accreditation must make available all information in written form necessary or requested by the Commissioner, in order for him to make a determination for the purposes of section 24-2(2).
- (5) The maximum period of any accreditation is to be 5 years, subject to renewal provided the body can demonstrate continuing compliance with all relevant requirements.
- (6) When accredited, a certification body is responsible for the proper assessment of a Controller or Processor leading to the certification or the refusal or withdrawal of certification regardless of responsibility of the Controller or Processor for compliance with these Regulations.

25. Delegation by Commissioner

The Commissioner of Data Protection may delegate any of the Commissioner's Functions under these Regulations, the Rules or any other Legislation Administered by the Commissioner:

- (a) to a member of the AIFCA's staff; or
- (b) with the approval of the Board of Directors of the AIFCA, to any other Person.



26. General power of Commissioner to obtain information

- (1) The Commissioner of Data Protection may, by Written notice, require a Data Controller, or any director, officer, partner, employee or agent of a Data Controller, to give specified information, produce specified Documents, or ensure that specified information or Documents are given or produced, to the Commissioner. A Person given a notice under this subsection must comply with the requirement within the time specified in the notice.
- (2) The Commissioner of Data Protection may, by Written notice, require a Data Controller to allow the Commissioner to enter any premises of the Data Controller during normal business hours, or at any other time agreed between the Commissioner and the Data Controller, for the purpose of inspecting and copying information or Documents, in any form, on the premises. The Data Controller must comply with the requirement.
- (3) The Commissioner of Data Protection may exercise a power under subsection (1) or (2) if the Commissioner considers that it is necessary or desirable to do so for the Exercise of the Commissioner's Functions under these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (4) Information or a Document given, produced or obtained because of the exercise by the Commissioner of Data Protection of powers under subsection (1) or (2) is admissible in evidence in any proceedings, if the information or Document complies with any requirements relating to the admissibility of evidence in the proceedings.
- (5) Subsections (1) and (2) do not apply to information or a Document if the information or Document is subject to legal professional privilege.
- (6) The Commissioner of Data Protection may apply to the Court for an order to require a Person to comply with a requirement under subsection (1) or (2), and the Court may make the orders that it considers appropriate.

27. Power to adopt rules etc.

- (1) The Board of Directors of the AIFCA may adopt rules prescribing matters:
 - (a) required or permitted by these Regulations, or any other AIFC Regulations that are Legislation Administered by the Commissioner, to be prescribed by the Rules; or
 - (b) necessary or convenient to be prescribed for carrying out or giving effect to these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (2) However, the Board may not adopt rules under this section on matters related to the regulation of financial services and related operations in the AIFC.
- (3) Also, before adopting rules under this section, the Board must consult with the Commissioner of Data Protection about the rules unless the rules are being adopted on the Commissioner's recommendation.
- (4) Without limiting subsection (1), the Board may adopt rules:
 - (a) with respect to any matters relating to the Objectives or Functions of the Commissioner of Data Protection; or
 - (b) to facilitate the administration of, or further the purposes of, these Regulations,



AIFC DATA PROTECTION REGULATIONS

- the Rules or any other Legislation Administered by the Commissioner; or
- (c) with respect to the procedures for the imposition or recovery of fines, including any circumstances in which the procedures do not apply to the imposition of a fine; or
 - (d) setting limits for fines and other penalties that may be imposed for Contraventions of these Regulations; or
 - (e) with respect to any of the following:
 - (i) forms, procedures and requirements under these Regulations, the Rules or any other Legislation Administered by the Commissioner;
 - (ii) the development and publication of information to AIFC Participants and AIFC Bodies, and their directors, officers, partners, employees and agents, about these Regulations, the Rules and other Legislation Administered by the Commissioner, including their application and interpretation;
 - (iii) procedures for or in relation to the making and mediation of complaints;
 - (iv) procedures for or in relation to the reconsideration or review of decisions of the Commissioner of Data Protection;
 - (v) the keeping and inspection of the Register of Notifications;
 - (vi) the conduct of the Commissioner of Data Protection, members of the staff of the AIFCA, and delegates and agents of the Commissioner in relation to the Exercise of the Commissioner's Functions, including discretionary Functions and the conduct of investigations and hearings.
- (5) Rules adopted by the Board may incorporate standards and codes of practice by reference. A standard or code of practice incorporated into the Rules has the same effect as it had been adopted in the Rules, except so far as the Rules otherwise provide.
- (6) Instead of incorporating a standard or code of practice into rules adopted by the Board, the Board may adopt the standard or code of practice as non-binding guidance for AIFC Participants.
- (7) Without limiting subsection (1), rules adopted by the Board may do any of the following:
- (a) make different provision for different cases or circumstances;
 - (b) include supplementary, incidental and consequential provisions;
 - (c) make transitional and savings provisions.
- (8) If any rules purport to be adopted in the exercise of a particular power or powers, the rules are taken also to be adopted in the exercise of all the powers under which they may be adopted.
- (9) Until rules mentioned in subsection (4)(d) are adopted by the Board, there are no limits on the fines and other penalties that may be imposed for a Contravention of these Regulations.



28. Publication of proposed rules

- (1) Before making rules under section 27 (Power to adopt rules etc.), the Board of Directors of the AIFCA must publish a notice under this section.
- (2) The notice must include, or have attached to it:
 - (a) a summary of the proposed rules; and
 - (b) the text of the rules; and
 - (c) a statement of the substance and purpose of the material provisions of the rules; and
 - (d) if the rules incorporate a standard or code of practice by reference—a summary, and the text, of the standard or code of practice and a statement of the substance and purpose of the material provisions of the standard or code of practice.
- (3) The notice must invite interested Persons to make representations about the proposed rules within a stated period of at least 30 days.
- (4) Subsections (1), (2) and (3) do not apply to the making of rules if the Board of Directors of the AIFCA considers:
 - (a) that any delay likely to arise because of complying with those subsections is prejudicial to the interests of the AIFCA; or
 - (b) that the rules are merely consequential on any other Rules adopted (or proposed to be adopted) by the Board; or
 - (c) that the rules do not change, or significantly change, the policy intended to be give effect to by these Regulations and the Rules or any other AIFC Regulations or AIFC Rules.

29. Funding and fees

- (1) For each financial year of the Commissioner of Data Protection, the office of the Board of Directors of the AIFCA must provide financial resources to the Commissioner to the extent necessary to ensure that the Commissioner is able adequately to Exercise the Commissioner's Functions.
- (2) The Rules may require the payment to the AIFCA of fees by Data Controllers.
- (3) Without limiting subsection (2), the Rules may require the payment to the AIFCA of fees by Data Controllers and other Persons for or in relation to:
 - (a) the Exercise by the Commissioner of Data Protection of Functions under or for these Regulations, the Rules or any other Legislation Administered by the Commissioner, including the receipt by the Commissioner of any notification or Document that is required to be, or may be, given or delivered to, or filed with, (however described) the Commissioner; and
 - (b) the inspection of Documents or other material held, or any register kept, by the Commissioner of Data Protection under these Regulations, the Rules or any other Legislation Administered by the Commissioner.



AIFC DATA PROTECTION REGULATIONS

- (4) The AIFCA may charge a fee for any services provided by the Commissioner otherwise than under an obligation imposed on the Commissioner by or under these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (5) If a fee is prescribed or charged under this section for the Exercise of a Function, or the provision of services, by the Commissioner of Data Protection, no action need be taken by the Commissioner until the fee is paid and, if the fee is payable to the AIFCA on the receipt by the Commissioner of a Document required to be, or that may be, given or delivered to, or filed with, (however described) with the Commissioner, the Commissioner is taken not to have received the Document until the fee is paid.

30. Commissioner's annual report

- (1) As soon as practicable after 1 January in each year, the Commissioner of Data Protection must give the Governor a report on the management of the administrative affairs of the Commissioner for the Commissioner's previous financial year.
- (2) The report must give a true and fair view of the state of the regulatory operations of the Commissioner of Data Protection, and financial statements of the Commissioner, as at the end of the relevant financial year.



PART 6: REMEDIES, LIABILITY AND SANCTIONS

31. Direction to comply with Legislation Administered by the Commissioner

- (1) This section applies if a Data Controller Fails to comply with a requirement (however expressed and including, to remove any doubt, a requirement applying for the benefit of a Person other than the Commissioner of Data Protection):
 - (a) under a provision of these Regulations, the Rules or any other Legislation Administered by the Commissioner; or
 - (b) made by the Commissioner under these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (2) The Commissioner of Data Protection may, by Written notice given to the Data Controller or another Person who is a director, officer, partner, employee or agent of the Data Controller, direct the Data Controller or other Person to do any or all of the following:
 - (a) comply with the requirement within a stated time;
 - (b) do anything else, or refrain from doing anything, stated in the notice within a stated time;
 - (c) without limiting paragraph (a) and (b), refrain from Processing stated or all Personal Data or refrain from Processing Personal Data for a stated purpose or in a stated way.
- (3) A Person who is given a direction under subsection (2) must comply with the direction.
- (4) Contravention of subsection (3) is punishable by a fine.
- (5) A Person who is given a direction under subsection (2) may, by Written notice given to the Commissioner of Data Protection within 14 days after the day the Person is given the direction, ask the Commissioner to review the direction.
- (6) If the Commissioner of Data Protection receives a request under subsection (5), the Commissioner must review the direction and may:
 - (a) confirm the direction; or
 - (b) revoke or amend the direction.
- (7) If a Person Fails to comply with a direction given to the Person under subsection (2), the Commissioner of Data Protection may apply to the Court for 1 or more of the following orders:
 - (a) an order directing the Person to comply with the direction or with any relevant provision of these Regulations, the Rules or any other Legislation Administered by the Commissioner;
 - (b) an order directing the Person to pay any costs incurred by the Commissioner or any other Person relating to:
 - (i) the giving of the direction by the Commissioner; or
 - (ii) the relevant Contravention of these Regulations;



- (c) any other order that the Court considers appropriate.
- (8) This section does not affect the operation of any other provision of these Regulations, the Rules or any other Legislation Administered by the Commissioner under which penalties may be imposed on a Data Controller or another Person in respect of a Failure to comply with a requirement to which this section applies, or any powers that the Commissioner of Data Protection, another Person or the Court may have under any other provision of these Regulations, the Rules or any other AIFC Regulations or AIFC Rules.

32. Lodging complaints and mediation

- (1) This section applies if a Data Subject (**A**) believes, on reasonable grounds:
 - (a) that A has been adversely affected by a Contravention of these Regulations in relation to the Processing of A's Personal Data by a Data Controller; or
 - (b) that A's rights under section 17 (Right to information about Personal Data and to rectification etc.) or section 18 (Right to object to Processing) have been Contravened by a Data Controller.
- (2) A may lodge a complaint with the Commissioner of Data Protection.
- (3) The Commissioner of Data Protection may mediate between A and the Data Controller.
- (4) On the basis of the mediation, the Commissioner of Data Protection may, by Written notice, direct the Data Controller to do, or refrain from doing, what the Commissioner considers appropriate.
- (5) The Data Controller must comply with the direction within the time stated in the notice.
- (6) Contravention of subsection (5) is punishable by a fine.

33. Enforceable agreements

- (1) The Commissioner of Data Protection may accept a Written undertaking given by a Person if the Commissioner considers that accepting the undertaking is necessary or desirable in the pursuit of the Commissioner's Objectives.
- (2) The Person may withdraw or vary the undertaking at any time, but only with the consent of the Commissioner of Data Protection.
- (3) If the Commissioner of Data Protection considers that the Person who gave the undertaking has Breached or is Breaching any of its terms, the Commissioner may apply to the Court for an order under subsection (4).
- (4) If the Court is satisfied that the Person has Breached or is Breaching a term of the undertaking, the Court may make 1 or more of the following orders:
 - (a) an order directing the Person to comply with the term;
 - (b) an order directing the Person to pay to any other Person or to the Commissioner of Data Protection an amount up to the amount of any profit, gain or benefit that the Person has obtained directly or indirectly and that is reasonably attributable to the Breach;



AIFC DATA PROTECTION REGULATIONS

- (c) any order that the Court considers appropriate directing the Person to compensate any other Person who has suffered loss or damage because of the Breach;
- (d) any other order the Court considers appropriate.

34. Administrative censures

- (1) The Commissioner of Data Protection may censure a Person if the Person Contravenes these Regulations or Contravenes any Guidance.
- (2) In deciding whether to censure a Person under subsection (1), the Commissioner of Data Protection must comply with the Decision-making Procedures.
- (3) The Commissioner of Data Protection may censure a Person by any means, including by way of publishing a notice of censure in any way the Commissioner considers appropriate.

35. Administrative imposition of fines

- (1) If the Commissioner of Data Protection is satisfied that a Person has Contravened these Regulations and Contravention of the relevant provision or of a relevant requirement is expressed to be punishable by a fine, the Commissioner may impose a fine on the Person.
- (2) In deciding whether to impose a fine on a Person and, if so, the amount of the fine to be imposed, the Commissioner of Data Protection must comply with any applicable Decision-making Procedures and any limits for fines set by the Rules.

36. Giving false or misleading information to Commissioner etc.

- (1) A Person must not:
 - (a) make a statement, or give information, to the Commissioner of Data Protection (whether orally, in a Document or in any other way) that is false or misleading in a material particular; or
 - (b) give a Document to the Commissioner that is false or misleading in a material particular; or
 - (c) conceal information or a Document if the concealment is likely to mislead or deceive the Commissioner.
- (2) Contravention of this section is punishable by a fine.

37. Court orders for Contraventions on Commissioner's application

- (1) This section applies if the Court is satisfied, on the application of the Commissioner of Data Protection, that a Person has Contravened these Regulations.
- (2) The Court may make any orders that the Court considers just and appropriate in the circumstances, including orders for damages, penalties or compensation.
- (3) This section does not affect the operation of any other provision of these Regulations, the Rules or any other Legislation Administered by the Commissioner under which penalties may be imposed on a Data Controller or another Person for a Contravention of these Regulations, or any powers that the Commissioner of Data Protection, another Person or



AIFC DATA PROTECTION REGULATIONS

the Court may have under any other provision of these Regulations, the Rules or any other AIFC Regulations or AIFC Rules.

38. Court orders for compensation

- (1) This section applies if the Court is satisfied, on the application of a Data Subject (**A**), that A has suffered damage or loss because of a Contravention of these Regulations by a Data Controller.
- (2) The Court may make any orders that the Court considers just and appropriate in the circumstances, including orders for damages or compensation.
- (3) This section does not affect of any powers that the Commissioner of Data Protection, another Person or the Court may have under any other provision of these Regulations, the Rules or any other AIFC Regulations or AIFC Rules.



PART 7: GENERAL EXEMPTIONS

39. General exemptions

- (1) The Rules may exempt Data Controllers from any provisions of these Regulations, the Rules or any other Legislation Administered by the Commissioner.
- (2) Without limiting subsection (1), the relevant provisions of these Regulations do not apply to the AFSA, AIFCA, the Security Registrar or the Registrar of Companies if the application of the provisions would be likely to prejudice the proper Exercise by any of those entities of their Functions under any AIFC Regulations or AIFC Rules, including any delegated Functions, so far as the Functions are designed to protect members of the public against:
 - (a) financial loss because of 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 activities and services, (including insurance and reinsurance activities and services), financial market activities and services, and financial and monetary brokerage activities and 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 activities and services.
- (3) In this section:

relevant provisions means the following sections:

- (a) section 11 (Transfers out of AIFC);
- (b) section 12 (Transfers to jurisdictions without adequate level of protection);
- (c) section 13 (Providing information where Personal Data has been obtained from Data Subject);
- (d) section 14 (Providing information where Personal Data has not been obtained from Data Subject);
- (e) section 17 (Right to information about Personal Data and to rectification etc.);
- (f) section 18 (Right to object to Processing).



PART 8: MISCELLANEOUS

40. Notification of Commissioner's decisions and reasons

- (1) This section applies if, under these Regulations, the Rules or any other Legislation Administered by the Commissioner:
 - (a) the Commissioner of Data Protection makes a decision (including a decision refusing to make a decision) on the application (however described) of a Person (the **affected Person** for the decision); or
 - (b) the Commissioner of Data Protection makes a decision affecting the interests of a Person (the **affected Person** for the decision) on the Commissioner's own initiative.
- (2) As soon as practicable after the Commissioner of Data Protection makes the decision, the Commissioner must give the affected Person Written notice of the decision.
- (3) Without limiting subsection (2), the notice must:
 - (a) if the decision is to take effect on the day after the day the notice is given to the Person—state that fact; or
 - (b) if the decision is to take effect at a different time—specify the time; or
 - (c) if the decision is to grant or issue (however described) a licence, permit, registration or anything else subject to conditions, restrictions or limitations of any kind—state the conditions, restrictions or limitations; or
 - (d) if the decision is to grant or issue (however described) a licence, permit, registration or anything else for a period—specify the period.
- (4) The notice must include, or be accompanied by, a statement of the reasons of the Commissioner of Data Protection for the decision.
- (5) However, if the decision was made on the application (however described) of the affected Person, subsection (4) does not apply to the decision so far as the decision was the decision the affected Person applied for.
- (6) Also, subsection (4) does not apply to the decision if a provision of any Legislation Administered by the Commissioner of Data Protection expressly provides that the Commissioner need not provide reasons for the decision.
- (7) This section is additional to, and does not limit, any other provision of any the AIFC Regulations or AIFC Rules.

41. Language

The Commissioner of Data Protection may require communications to which the Commissioner is a party (including communications under any other Legislation Administered by the Commissioner) to be conducted in the English language.



SCHEDULE 1: INTERPRETATION

Note: See section 6.

1. Meaning of *Legislation Administered by the Commissioner*

Each of the following is *Legislation Administered by the Commissioner*:

- (a) these Regulations and the Rules;
- (b) any other AIFC Regulations or AIFC Rules if the Regulations or Rules declare that they are administered by the Commissioner;
- (c) a provision of any other AIFC Regulations or AIFC Rules if the provision gives a Function to the Commissioner or relates to the Exercise of a Function given to the Commissioner by another provision of the AIFC Regulations or AIFC Rules.

2. When does a Person *Contravene* these Regulations

- (1) A Person *Contravenes* these Regulations if the Person:
 - (a) does something that the Person is prohibited from doing by or under these Regulations, the Rules or any other Legislation Administered by the Commissioner; or
 - (b) does not do something that the Person is required or directed to do (however described) by or under these Regulations, the Rules or any other Legislation Administered by the Commissioner; or
 - (c) otherwise Contravenes these Regulations, the Rules or any other Legislation Administered by the commissioner.
- (2) This section does not apply to anything done, or omitted to be done, by the Governor, AFSA, AIFCA or Commissioner of Data Protection.

3. Definitions for these Regulations

In these Regulations:

Acting Law of the AIFC has the meaning given by article 4 of the Constitutional Statute.

AFSA means the Astana Financial Services Authority.

AIFC means the Astana International Financial Centre.

AIFCA means the Astana International Financial Centre Authority.

AIFC Bodies has the meaning given by article 9 of the Constitutional Statute and the document entitled *The Structure of the Bodies of the Astana International Financial Centre* adopted by the Management Council on 26 May 2016.

AIFC Participants has the meaning given by article 1(5) of the Constitutional Statute.

AIFC Regulations means regulations adopted by the Management Council or the Governor, and includes, for example, these Regulations.

AIFC Rules means rules adopted by the Board of Directors of the AFSA, the Board of Directors



AIFC DATA PROTECTION REGULATIONS

of the AIFCA or the Governor, and includes, for example, the Rules made under these Regulations.

Annual Assessment has the meaning given in section 10-4(1).

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.

Breach includes Contravene.

Commissioner means the Commissioner of Data Protection.

Commissioner of Data Protection means the individual who is appointed as Commissioner of Data Protection under section 22 (Appointment of Commissioner etc.).

Constitutional Statute means Constitutional Statute of the Republic of Kazakhstan dated 7 December 2015 entitled *On Astana International Financial Centre*.

Contravene includes Fail to comply with.

Contravenes these Regulations has the meaning given by section 2 of this Schedule (When does a Person *Contravene* these Regulations).

Court means the Astana International Financial Centre Court.

Data means any information:

- (a) that is being Processed by means of equipment operating automatically in response to instructions given for the purpose; or
- (b) that is recorded with intention that it should be Processed by means of equipment mentioned in paragraph (a); or
- (c) is recorded as part of a Relevant Filing System or with intention that it should form part of Relevant Filing System.

Data Controller means any Person in the AIFC who, alone or jointly with other Persons, determines the purposes and means of the Processing of Personal Data.

Data Processor means any Person who Processes Personal Data on behalf of a Data Controller.

Data Subject, in relation to Personal Data, means the individual to whom the Personal Data relates.

Data Sub-processor means a processor appointed by the Processor as set out in section 16-2(2).

Decision-making Procedures, in relation to the making of a decision by the Commissioner of Data Protection, means the procedures prescribed by the Rules that apply to the making of the decision by the Commissioner.

Document includes any summons, notice, statement, return, account, order and other legal process, and any register.

DPO means a data protection officer appointed by a Controller (including a Joint Controller), or



AIFC DATA PROTECTION REGULATIONS

Processor to independently oversee relevant data protection operations in the manner set out in sections 10-1, 10-2, 10-3 and 10-4.

Exercise a Function includes perform the Function.

Fail includes refuse.

Function includes authority, duty and power.

Governor means the Governor of the Astana International Financial Centre.

Group means any group of entities that are related to each other by virtue of being Subsidiaries of the same Ultimate Holding Company or subsidiaries of any such Subsidiaries. Ultimate Holding Company and Subsidiary have the meaning given in section 2 of Schedule 1 (Interpretation) of the AIFC Companies Regulations.

Guidance means:

- (a) guidance adopted by the Commissioner of Data Protection under section 24(4)(e) (Commissioner's Objectives and Functions); or
- (b) a standard or code of practice adopted as guidance by the Board of Directors of the AIFCA under section 27(6) (Power to adopt rules etc.).

High Risk Processing Activities means Processing of Personal Data where 1 or more of the following applies:

- (a) Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights;
- (b) a considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, including due to the sensitivity of the Personal Data or risks relating to the security, integrity or privacy of the Personal Data;
- (c) the Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
- (d) a material amount of Sensitive Personal Data is to be Processed.

Identifiable Natural Person means a living natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to 1 or more factors specific to the person's biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Joint Data Controller means any Data Controller that jointly determines the purposes and means of Processing with another Data Controller.

Legislation Administered by the Commissioner has the meaning given by section 1 of this Schedule (Meaning of Legislation Administered by the Commissioner).

Management Council means the Management Council of the Astana International Financial



Centre.

AIFC DATA PROTECTION REGULATIONS

Management Council Resolution on AIFC Bodies means *The Structure of the Bodies of the Astana International Financial Centre*, adopted by resolution of the Management Council on 26 May 2016, as amended by resolution of the Management Council, *The Amendments and supplementations to the Structure of the Bodies of the Astana International Financial Centre*, adopted on 9 October 2017.

Objectives, of the Commissioner of Data Protection, has the meaning given by section 24(1) (Commissioner's Objectives and Functions).

Person includes any natural person or incorporated or unincorporated body, including a company, partnership, unincorporated association, government or state.

Personal Data means any Data referring to an Identifiable Natural Person.

Personal Data Breach means 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.

Process, in relation to Personal Data, means perform any operation or set of operations on the Personal Data, whether or not by automatic means, and includes, for example, the collection, recording, organisation, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of the Personal Data.

Recipient, in relation to Personal Data, means any Person to whom the Personal Data is disclosed (whether or not a Third Party), but does not include a regulator, the police or another government agency of any jurisdiction if the agency receives the Personal Data in the framework of a particular inquiry.

Register of Notifications means the register kept by the Commissioner of Data Protection under section 21 (Register of Notifications).

Registrar of Companies means the individual who is the Registrar of Companies appointed under the AIFC Companies Regulations.

Relevant Filing System means any set of information relating to an Identifiable Natural Person to the extent that, although the information is not Processed by means of equipment operating automatically in response to instructions given for the purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Rules means rules adopted by the Board of Directors of the AIFCA under section 27 (Power to adopt rules etc.).

Sensitive Personal Data means Personal Data revealing or concerning (directly or indirectly) 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 section 9-1(11).

Third Country means a jurisdiction other than the AIFC, whether in the Republic of Kazakhstan or elsewhere.



AIFC DATA PROTECTION REGULATIONS

Third Party, in relation to Personal Data, means any Person other than the Data Subject, the Data Controller, the Data Processor or a Person who, under the direct control of the Data Controller or Data Processor, is authorised to Process the Personal Data.

Writing includes:

- (a) in relation to a certificate, instrument, notice or other thing—the thing in any form that preserves a record of the information contained in it and is capable of being reproduced in tangible form, including by electronic means; and
- (b) in relation to a communication—any method of communication that preserves a record of the information contained in it and is capable of being reproduced in tangible form, including by electronic means.