

**AIFC DATA PROTECTION RULES
(DPR)**

AIFC RULES NO. 1 OF 2018

**January 22, 2018
Astana, Kazakhstan**



PART 1: INTRODUCTION

- 1.1. Name
- 1.2. Commencement
- 1.3. Legislative authority
- 1.4. Application of these Rules
- 1.5. Definitions etc.
- 1.6. Administration of these Rules

PART 2: PERMIT TO PROCESS SENSITIVE PERSONAL DATA

- 2.1. Permit to Process Sensitive Personal Data

PART 3: PERMIT TO TRANSFER PERSONAL DATA OUT OF AIFC

- 3.1. Permit to transfer Personal Data out of AIFC

PART 4: RECORDS AND NOTIFICATIONS

- 4.1. Records about Personal Data Processing operations
- 4.2. Notifications about Personal Data Processing operations
- 4.3. Notifications about changes in Personal Data Processing operations

PART 5: IMPOSITION OF FINES

- 5.1. Notice of administrative imposition of fines etc.

PART 6: COMPLAINTS AND MEDIATION

- 6.1. Lodging complaints and mediation

PART 7: MISCELLANEOUS

- 7.1. Forms
- 7.2. Fees
- 7.3. Jurisdictions with adequate levels of protection
- 7.4. Fine limits

SCHEDULE 1: FEES

SCHEDULE 2: JURISDICTIONS WITH ADEQUATE LEVELS OF PROTECTION FOR PERSONAL DATA

SCHEDULE 3: FINE LIMITS



PART 1: INTRODUCTION

1.1. Name

These Rules are *AIFC Data Protection Rules 2018* (or DPR).

1.2. Commencement

These Rules commence on 1 January 2018.

1.3. Legislative authority

These Rules are adopted by the Board of Directors of the AIFCA under section 27 (Power to adopt rules etc.) of the AIFC Data Protection Regulations.

1.4. Application of these Rules

These Rules apply within the jurisdiction of the AIFC.

1.5. Definitions etc.

Terms used in these Rules have the same meanings as they have, from time to time, in the AIFC Data Protection Regulations, or the relevant provisions of those Regulations, unless the contrary intention appears.

Note: For definitions in the AIFC Data Protection Regulations applying to these Rules, see Schedule 1 of those Regulations. The definitions in that Schedule relevant to these Rules include the following:

- AFSA
- AIFC
- AIFCA
- Commissioner of Data Protection (or Commissioner)
- Contravene
- Court
- Data
- Data Controller
- Data Subject
- Document
- Legislation Administered by the Commissioner
- Person
- Personal Data
- Process
- Recipient
- Sensitive Personal Data
- Writing.

1.6. Administration of these Rules

These Rules are administered by the Commissioner of Data Protection.



AIFC DATA PROTECTION RULES

PART 2: PERMIT TO PROCESS SENSITIVE PERSONAL DATA

2.1. Permit to Process Sensitive Personal Data

2.1.1 A Data Controller may apply to the Commissioner of Data Protection for the issue of a permit under section 10(2) (Processing of Personal Sensitive Data) of the AIFC Data Protection Regulations to Process Sensitive Personal Data.

2.1.2 The application must be in Writing and must state the following:

- (a) the name and address of the applicant;
- (b) the name, address, phone and fax numbers, and e-mail address, of the individual responsible for making the application for the permit;
- (c) a description of the Processing of Sensitive Personal Data for which the permit is being sought, including a description of the nature of the Sensitive Personal Data involved;
- (d) the purpose of the Processing of the Sensitive Personal Data;
- (e) the identity of the Data Subjects to whom the Sensitive Personal Data relates or, if it relates to a class of Data Subjects, a description of the class of Data Subjects;
- (f) the identity of each intended Recipient of any of the Sensitive Personal Data and, if any intended Recipient is located in a jurisdiction outside the AIFC, the jurisdiction;
- (g) a description of the safeguards put in place by the applicant to ensure the security of the Sensitive Personal Data.

2.1.3 The Commissioner of Data Protection may require the applicant to provide additional information reasonably required by the Commissioner to decide the application.

2.1.4 The Commissioner of Data Protection may, at the Commissioner's absolute discretion, refuse to issue the permit applied for.



AIFC DATA PROTECTION RULES

PART 3: PERMIT TO TRANSFER PERSONAL DATA OUT OF AIFC

3.2. Permit to transfer Personal Data out of AIFC

3.1.1 A Person may apply to the Commissioner of Data Protection for the issue of a permit under section 12(2) (Transfers to jurisdictions without adequate level of protection) of the AIFC Data Protection Regulations authorising the transfer of Personal Data to a Recipient located in a jurisdiction outside the AIFC.

3.1.2 The application must be in Writing and state the following:

- (a) the name and address of the applicant;
- (b) the name, address, phone and fax numbers, and e-mail address, of the individual responsible for making the application for the permit;
- (c) a description of the proposed transfer of Personal Data for which the permit is being sought, including a description of the nature of the Personal Data involved;
- (d) the purpose of the proposed transfer of Personal Data;
- (e) the identity of the Data Subjects to whom the Personal Data relates or, if it relates to a class of Data Subjects, a description of the class of Data Subjects;
- (f) the identity of the proposed Recipient of the Personal Data;
- (g) the jurisdiction in which the proposed Recipient is located and a description of the laws and regulations that apply to the proposed Recipient in relation to Personal Data protection;
- (h) a description of the safeguards put in place by the applicant to ensure the security of the Personal Data if the transfer takes place.

3.1.3 The Commissioner of Data Protection may require the applicant to provide additional information reasonably required by the Commissioner to decide the application.

3.1.4 The Commissioner of Data Protection may, at the Commissioner's absolute discretion, refuse to issue the permit applied for.



AIFC DATA PROTECTION RULES

PART 4: RECORDS AND NOTIFICATIONS

4.1. Records about Personal Data Processing operations

4.1.1 For section 19(1) (Requirement to notify Commissioner about Personal Data Processing operations etc.) of the AIFC Data Protection Regulations, a Data Controller must establish and maintain the following records of the Personal Data Processing operations performed by or on behalf of the Data Controller:

- (a) a description of the Personal Data Processing operations;
- (b) an explanation of the purpose of the Personal Data Processing operations;
- (c) the identity of the Data Subjects to whom the Personal Data relates or, if it relates to a class of Data Subjects, a description of the class of Data Subjects;
- (d) a description of the class of Personal Data being processed;
- (e) a list of the jurisdictions outside the AIFC to which Personal Data may be transferred by the Data Controller, together with a statement for each of the jurisdictions about whether the jurisdiction has an adequate level of protection for section 11(1) (Transfers out of AIFC) of those Regulations.

4.1.2 Without limiting subrule 4.1.1(b), the following may, if appropriate, be used as an explanation of the purpose of Personal Data Processing operations:

- (a) accounting and auditing;
- (b) administration of justice;
- (c) administration of membership records;
- (d) advertising, marketing and public relations for the Data Controller;
- (e) advertising, marketing and public relations for others;
- (f) benefits, grants and loans administration;
- (g) consultancy and advisory services;
- (h) credit referencing;
- (i) debt administration and factoring;
- (j) education;
- (k) information and data bank administration;
- (l) insurance administration;
- (m) legal services;



AIFC DATA PROTECTION RULES

- (n) licensing and registration;
- (o) pastoral care;
- (p) pensions administration;
- (q) policing;
- (r) private investigation;
- (s) property management;
- (t) provision of financial services;
- (u) research;
- (v) staff administration.

4.1.3 Without limiting subrule 4.1.1(c), the following may, if appropriate, be used to describe a class of Data Subjects:

- (a) staff, including agents, temporary and casual workers;
- (b) clients and customers;
- (c) suppliers;
- (d) members;
- (e) complainants, correspondents and enquirers;
- (f) relatives and associates of the Data Subject;
- (g) advisors, consultants and other professional experts.

4.2. Notifications about Personal Data Processing operations

4.2.1 For section 19(2) (Requirement to notify Commissioner about Personal Data Processing operations etc.) of the AIFC Data Protection Regulations, a Data Controller must notify the Commissioner of Data Protection about particulars of the following Personal Data Processing operations performed or to be performed by or on behalf of the Data Controller:

- (a) any Personal Data Processing operation, or set of operations, involving the Processing of Sensitive Personal Data;
- (b) any Personal Data Processing operation, or set of operations, involving the transfer of Personal Data to a Recipient located in a jurisdiction outside the AIFC if the jurisdiction does not have an adequate level of protection for Personal Data for section 11(1) of the AIFC Data Protection Regulations.



AIFC DATA PROTECTION RULES

- 4.2.2 A notification in relation to the Personal Data Processing operations must include the following information:
- (a) a general description of the Personal Data Processing operations;
 - (b) an explanation of the purpose of the Personal Data Processing operations;
 - (c) the identity of the Data Subjects to which the Personal Data relates or, if it relates to a class of Data Subjects, a description of the class of Data Subjects;
 - (d) a description of the class of Personal Data being processed;
 - (e) the jurisdictions outside the AIFC to which Personal Data has been, is being or will be transferred by the Data Controller and, for each of those jurisdictions, whether the jurisdiction has an adequate level of protection for section 11(1) (Transfers out of AIFC) of the AIFC Data Protection Regulations.
- 4.2.3 Notification for the Personal Data Processing operations must be provided to the Commissioner of Data Protection:
- (a) no later than 14 days start of the operations; and
 - (b) if the operations continue beyond the anniversary of the initial notification under paragraph (a)—on that anniversary and on every subsequent anniversary beyond which the operations continue.

4.3. Notifications about changes in Personal Data Processing operations

For section 20(2) (Requirement to notify Commissioner of changes in operations) of the AIFC Data Protection Regulations, a Data Controller must notify the Commissioner of Data Protection about changed particulars of Personal Data Processing operations as soon as possible after the particulars change, but no later than 14 days after the day the particulars change.



AIFC DATA PROTECTION RULES

PART 5: IMPOSITION OF FINES

5.1. Notice of administrative imposition of fines etc.

- 5.1.1 If the Commissioner of Data Protection decides, under section 35 (Administrative imposition of fines) of the AIFC Data Protection Regulations, to impose a fine on a person for a Contravention, the Commissioner must give the Person a Written notice (the ***fine notice***):
- (a) stating that the Commissioner is satisfied that the Person has committed the Contravention; and
 - (b) giving particulars of the facts alleged by the Commissioner to constitute the Contravention; and
 - (c) stating the fine imposed by the Commissioner for the Contravention; and
 - (d) stating that the Person may file a notice of objection to the imposition of the fine and that, if the Person does so, the notice must set out every matter that the Person believes ought to be taken into account by the Commissioner of Data Protection in deciding whether to commence proceedings in the Court for recovery of the fine; and
 - (e) providing an address for filing a notice of objection; and
 - (f) specifying the period (the ***specified period***) within which the fine must be paid or a notice of objection filed.
- 5.1.2 If the Commissioner of Data Protection issues a form under rule 7.1.1 (Forms) for the notice of objection, a copy of the form must accompany the fine notice.
- 5.1.3 If, within the specified period, the Person files a notice of objection in accordance with fine notice, the Commissioner of Data Protection may not recover the fine as a debt owing to the Commissioner, but may commence proceedings in the Court for payment of the fine.
- 5.1.4 If, at the end of the specified period, the Person has not paid the full amount of the fine to the Commissioner of Data Protection and has not filed a notice of objection in accordance with the fine notice, the amount of the fine that has not been paid is a debt owing to the Commissioner and may be recovered by the Commissioner by proceedings in the Court.
- 5.1.5 The Commissioner of Data Protection may, at any time, withdraw a notice imposing a fine.



AIFC DATA PROTECTION RULES

PART 6: COMPLAINTS AND MEDIATION

6.1. Lodging complaints and mediation

6.1.1 For section 32(2) (Lodging complaints and mediation) of the AIFC Data Protection Regulations, a Data Subject (**A**) may lodge a complaint with the Commissioner of Data Protection by filing a Written notice with the Commissioner:

- (a) providing A's full name and address; and
- (b) stating the name and address of the Data Controller the complaint relates to; and
- (c) setting out the Contravention the complaint relates to; and
- (d) providing a detailed statement of the facts that A believes constitute the Contravention; and
- (e) states the relief sought by A.

6.1.2 In a mediation under section 32(3) of the AIFC Data Protection Regulations, the Commissioner of Data Protection may follow the practices and procedures that will, in the Commissioner's opinion, lead to the most timely, fair and effective resolution of the matter.



AIFC DATA PROTECTION RULES

PART 7: MISCELLANEOUS

7.1. Forms

- 7.1.1 If the Commissioner of Data Protection issues or prescribes a form (an **approved form**) to be used for a particular purpose under or in connection with the AIFC Data Protection Regulations or these Rules, the form must be used for that purpose.
- 7.1.2 Substantial compliance with an approved form is sufficient.
- 7.1.3 However, an approved form is properly completed only if each mandatory requirement applying to the form is complied with.
- 7.1.4 For subrule 7.1.3, a **mandatory** requirement is any requirement mentioned in subrule 7.1.5 and any other requirement that the form states is a mandatory requirement.
- 7.1.5 Each of the following is a mandatory requirement for every approved form, except so far as a particular approved form otherwise provides:
- (a) the form must be on white paper of international A4 size;
 - (b) the form must be clearly printed or written in black in a way that is permanent and is able to be reproduced or copied by photographic or electronic means;
 - (c) the form must contain, where applicable, original signatures of the Person or Persons indicated on the form and the date on which they signed;
 - (d) if the form relates to a Person—the form must state the Person’s full name and, if the Person has an identification number, the identification number;
 - (e) if the form has an annexure—the annexure must be endorsed with the following words ‘This is the (*or, if appropriate, an*) annexure to the (*insert the name of the form or a description of it*) relating to (*insert the name of the Person the form relates to*) dated (*insert date of form*);
 - (f) the form must be completed in the English language.
- 7.1.6 Without limiting subrule 7.1.4, an approved form may state that any of the following requirements is a mandatory requirement:
- (a) that the form be signed or witnessed, or signed and witnessed in a particular way;
 - (b) that the form, or information or a Document given with or attached to the form, be in a particular format (for example, in writing or a particular electronic format);
 - (c) that particular information be included in the form, or a particular document be attached to or given with the form;
 - (d) that the form, information in the form, or a Document attached to or given with the form, be verified in a particular way.

7.2. Fees



AIFC DATA PROTECTION RULES

7.2.1 A Person applying to the Commissioner of Data Protection under the AIFC Data Protection Regulations (*the Regulations*) for the issue of either of the following permits must pay the AIFCA the following application fee:

- (a) for a permit under section 10(2) of the Regulations (Processing of Personal Sensitive Data)—the appropriate fee specified in column 3 of item 1 of the table in Schedule 1 (the *fees table*);
- (b) for a permit under section 12(2) of the Regulations (Transfers to jurisdictions without adequate level of protection)—the appropriate fee specified in column 3 of item 2 of the fees table.

7.2.2 Any application fee paid under subrule 7.2.1 is non-refundable, whether or not the permit applied for is issued.

7.2.3 A Data Controller must pay the following fees to the AIFCA:

- (a) on the each notification by the Data Controller under section 19 (Requirement to notify Commissioner about Personal Data Processing operations etc.) of the Regulations—the appropriate fee specified in column 3 of item 3 of the fees table;
- (b) on the renewal of an entry in the Register of Notifications under section 21 of the Regulations relating to the Data Controller—the appropriate fee specified in column 3 of item 4 of the fees table;
- (c) on each notification by the Data Controller under section 20 (Requirement to notify Commissioner about Personal Data Processing operations etc.) of the Regulations—the appropriate fee specified in column 3 of item 5 of the fees table.

7.2.4 In applying column 3 of the fees table to a Person:

- (a) Category 1 applies to the Person if the Person is regulated by the AFSA; and
- (b) Category 2 applies to the Person if the Person is not regulated by the AFSA and does not conduct retail activities in the AIFC; and
- (c) Category 3 applies to the Person if the Person is not regulated by the AFSA, but conducts retail activities in the AIFC.

7.3. Jurisdictions with adequate levels of protection

For section 11(2) of the AIFC Data Protection Regulations, the jurisdictions specified in Schedule 2 (Jurisdictions with adequate levels of protection for Personal Data) are prescribed.

7.4. Fine limits

The maximum fine that may be imposed on a Person by the Commissioner of Data Protection for a Contravention of a provision of the AIFC Data Protection Regulations mentioned in column 2 of an item of the table in Schedule 3 (Fine limits) is the amount specified in column 4 of the item.



AIFC DATA PROTECTION RULES

SCHEDULE 1: FEES

Note: See rule 7.2.

1. Table of fees

The following table prescribes the fees payable under the AIFC Data Protection Regulations (*the Regulations*).

column 1 item	column 2 description of fee	column 3 category		
		1	2	3
1	application for permit under section 10(2) of the Regulations	\$ 250	\$ 150	\$ 50
2	application for permit under section 12(2) of the Regulations	\$ 250	\$ 150	\$ 50
3	notification under section 19 of the Regulations	\$ 1,000	\$ 500	\$ 200
4	renewal of entry in Register of Notifications	\$ 500	\$ 250	\$ 100
5	each notification under section 20 of the Regulations	\$ 100	\$ 50	\$ 10



AIFC DATA PROTECTION RULES

SCHEDULE 2: JURISDICTIONS WITH ADEQUATE LEVELS OF PROTECTION FOR PERSONAL DATA

Note: See rule 7.3.

1. Table of jurisdictions

The following table specifies jurisdictions that have an adequate level of protection for Personal Data.

column 1 item	column 2 jurisdiction with adequate level of protection for Personal Data
1	Andorra
2	Argentina
3	Austria
4	Belgium
5	Bulgaria
6	Canada
7	Cyprus
8	Czech Republic
9	Denmark
10	Dubai International Financial Centre
11	Estonia
12	Faeroe Islands
13	Finland
14	France
15	Germany
16	Gibraltar
17	Greece
18	Guernsey
19	Hungary
20	Iceland
21	Ireland
22	Isle of Man
23	Italy
24	Jersey
25	Latvia
26	Liechtenstein
27	Lithuania
28	Luxembourg
29	Malta
30	Netherlands
31	New Zealand
32	Norway



AIFC DATA PROTECTION RULES

33	Poland
34	Portugal
35	Romania
36	Slovakia
37	Slovenia
38	Spain
39	Sweden
40	Switzerland
41	United Kingdom
42	Uruguay
43	jurisdictions to which the US Department of Commerce and European Commission EU-US Privacy Shield Framework applies)



AIFC DATA PROTECTION RULES

SCHEDULE 3: FINE LIMITS

Note: See rule 7.4.

1. Table of fine limits

The following table sets the maximum fines that may be imposed for certain Contraventions of the AIFC Data Protection Regulations.

column 1 item	column 2 provision contravened	column 3 relevant section heading	column 4 maximum fine US\$
1	10(4)	Processing of Sensitive Personal Data	10,000
2	12(4)	Transfers to jurisdictions without adequate level of protection	20,000
3	31(3)	Direction to comply with Legislation Administered by the Commissioner	25,000
4	32(5)	Lodging complaints and mediation	25,000
5	36	Giving false or misleading information to Commissioner etc.	5000