CONSULTATION PAPER NO. 17
On proposed amendments to AIFC Data Protection Regulations and AIFC Data Protection Rules

INTRODUCTION

1. Why are we issuing this paper?

The Astana International Financial Centre Authority (the "***AIFC Authority***") has issued this Consultation Paper to invite public feedback and comments on the proposed amendments to AIFC Data Protection Regulations and AIFC Data Protection Rules (the "***Amendments***").

The proposed Amendments aim to improve AIFC Data Protection Regulations and Rules and align them with international standards.

2. Who should read this paper?

This Consultation Paper may be of interest to the current and prospective AIFC Participants, as well as all the AIFC Bodies and their organisations, individuals employed by AIFC Participants or AIFC Bodies or individuals seeking to be employed by AIFC Participants or AIFC Bodies, as well as legal advisors, and generally, to all interested in providing their feedback to the Amendments.

3. How to provide comments?

The AIFC Authority encourages interested parties to provide their views and comments in writing on the issues outlined in the Consultation Paper.

All comments should be provided to:
E-mail: LegalDevelopment@aifc.kz, dataprotection@aifc.kz

You may as well identify your organisation in the provided comments.

By submitting your comments to the AIFC Authority you expressly consent to the processing by the AIFC Authority of the personal data pertaining to you, including, but not limited to 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 thereof, as per the AIFC Data Protection Regulations 2017.

The AIFC Authority reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise at the time of making comments. Comments supported by reasoning and evidence will be given more weight by the AIFC Authority.

4. What happens next?

The deadline for providing comments on the proposals in this Consultation Paper is **31 December 2024**.

Once we receive your comments, we will consider if any further refinements are required to the Amendments annexed to this Consultation Paper. Once the task is complete, the draft of the Amendments will be further processed in accordance with the requirements, stipulated in the AIFC Regulations on AIFC Acts 2017.

The Amendments are in draft form only and are, therefore, subject to change following consultation as mentioned above. Consequently, you should not act on it until the Amendments are formally enacted.

LEGISLATIVE PROPOSAL

Annex 1 – Policy paper on amendments
Annex 2 – Proposed amendments to AIFC Data Protection Regulations
Annex 3 – Proposed amendments to AIFC Data Protection Rules

Annex 1

POLICY PAPER
ON AMENDMENTS TO AIFC DATA PROTECTION REGULATIONS AND RULES

Astana Date 03/12/24

1. Author

Name:
Division: Legal Development Department/Office of the Commissioner of Data Protection
E-mail: dataprotection@aifc.kz

2. Proposal type

a) New	☐ Regulations	☐ Rules	☐ Policy	☐ Procedure	☐ Other:_____
b) Amendment of	X Regulations	X Rules	☐ Policy	☐ Procedure	☐ Other:_____

3. Introduction

[Please, list the current framework documents that already exist in this field. What are the key issues with the current framework?]

This Policy Paper aims to provide a summary of the proposed amendments to the AIFC Data Protection Regulations 2017 and AIFC Data Protection Rules 2018 to align them with international standards on data protection and enhance data subjects' rights.

The AIFC Data Protection Regulations 2018 (hereinafter, the "**DPR**") commenced on 1 January 2018. The DPR aims to safeguard the personal data of individuals whose data is processed by AIFC-registered entities by determining the process of collection, use and transfer of personal data in and from the AIFC.

Recognising that legal frameworks in the international standards have been updated, the AIFC must align and introduce the leading global practice on data protection, and apply global standards that will encourage the application of new technologies in processing and storing personal data in the AIFC.

In particular, key issues within the current framework are outlined below:

1) **Providing clarification on the scope of application of the AIFC DPR Application.**
2) **Introduction of statutory requirement on appointment of a Data Protection Officer ("DPO") by certain AIFC Bodies and AIFC Participants.**
3) **Introduction of statutory requirements on joint processing and co-controlling, including the definition of "Joint Controller".**
4) **Introduction of the statutory conditions of obtaining/providing consent and data subject's right to withdraw the consent to process the personal data.**
5) **Introduction of the statutory mechanisms to implement measures to mitigate outcomes of a breach of personal data and protect the rights of data subjects.**
6) **Introduction of voluntary Certification and Accreditation of Data Controller and Data Processor**.
7) **Revisiting the list of jurisdictions with adequate levels of protection for personal data.**
8) **Reduced fees for providing notification on Personal Data Processing operations.**

4. Issues

[What is the intended purpose of your proposal? What is the scope of your proposal? How is the proposal expected to solve the identified issues outlined above?]

As of today, all of the AIFC Bodies and AIFC-registered companies are subject to the DPR and must comply with its requirements since they either process the personal data of clients or the sensitive personal data of the employees.

The DPR requires every company engaged in data processing in the AIFC to process all personal data of their stakeholders (clients, employees, business partners, shareholders etc.) in compliance with the requirements of the AIFC Data Protection Framework, including providing notification to the Commissioner of Data Protection on occasions when AIFC Participants initiating collection of personal or sensitive data, transferring the collected data to recipients located outside of the AIFC.

Whereas section 5 of the DPR does not provide explicit requirements on the type of processing, whether by automated or other than automated means, the Regulations apply.

> **5. Application of these Regulations**
>
> These Regulations apply within the jurisdiction of the AIFC.

Furthermore, section 5 of the DPR does not consider the fact that the processing of personal data by the AIFC Participants, if conducted as part of their business activities, might also take place outside the AIFC. As established by the AIFC Companies Regulations, the AIFC Participants may conduct their business in or from the AIFC, which requires amendments to determine triggers on the application of the DPR.

Furthermore, it is crucial to determine the High Risk Processing Activities in the AIFC, and further decide whether the requirement to appoint a DPO would be necessary.

Overall, the primary objective of this proposal is to enhance the existing framework, bringing it in line with international standards and ensuring appropriate safeguards for relevant Data Subjects. The scope of the proposal is extensive, encompassing various aspects of the AIFC DPR. Namely, 3 directions can be outlined:

1) **Clarification on application of the AIFC DPR;**
2) **Enhancement of Data Subject's Rights;**
3) **Developing data management, obligations and certification schemes of Data entities**[1].
4) **Update of jurisdictions with adequate Data Protection under the AIFC Data Protection Rules.**
5) **Reduced fees for providing notification on Personal Data Processing operations.**

On the first item from the abovementioned list, the current framework only indicates that AIFC DPR "*applies within the jurisdiction of the AIFC*". The **goal is to make some clarifications** to the Application of the AIFC DPR, by:

- indicating the types and methods of data processing it applies;
- specifying the Data subjects and Data entities to whom it applies;
- outlining the types of data to which it does not apply.

On the second item from the list, it is **aimed to determine conditions of consent and to implement the right to withdraw the consent**. Clearly defined conditions of consent eliminate ambiguity and let data subjects have the option to withdraw their consent for the processing of their personal data, with prescribed mechanisms.

On the third item, Data entities refer to any entity or individual involved in the processing, collection, and storage of personal data. In our case, these entities include the Data Commissioner, Data Controller and Data Processor. In practice, it is common for multiple data controllers or data processors to be involved in a single data processing operation. Therefore, one of the **primary objectives is to define joint controllership and establish effective mechanisms for joint control**. This will resolve the current issues related to the management and division of responsibilities among each involved data controller.

As part of the third item, there is also a need of appointing a DPO, who will handle important tasks instructed by data controller and data processor and conduct assessments on large scale and high risk data processing activities independently.

As per the Article 37 of EU GDPR, **DPO should be appointed in any case where**:

1) the processing is carried out by a **public authority or body,** except for courts acting in their judicial capacity;

[1] Collective name of: Data Commissioner, Data Controller, Data Processor;

2) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, **require regular and systematic monitoring of data subjects on a large scale;**
3) the core activities of the controller or the processor consist of processing **on a large scale of special categories of data** pursuant to Article 9 or **personal data relating to criminal convictions and offences** referred to in Article 10.

Adhere to this model, affiliated bodies to whom the designation of the DPO applies would be:

1) the AIFC Bodies, except for the AIFC Court and IAC.
2) AIFC Participants , which are subjects of the AIFC Anti-Money Laundering Rules, namely, **Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions (the "DNFBPs"), Registered Auditors.** For the reason that they possess comprehensive financial licenses and accommodate large-scale clients, which means regular and systematic data processing.

For reference purposes:
Authorised Firm *- A Centre Participant which has been licensed by the AFSA to carry on one or more Regulated Activities;*
Authorised Market Institution *- A Centre Participant which has been licensed by the AFSA to carry on one or more Market Activities;*
DNFBPs *- The following class of persons whose business or profession is carried on in or from the AIFC constitute DNFBPs: (a) A real estate developer or agency which carries out transactions with a customer involving the buying or selling of real property; (b) A dealer in precious metals or precious stones; (c) A dealer in any saleable item of a price equal to or greater than USD 15,000; (d) A law firm, notary firm, or other independent legal business; (e) An accounting firm, audit firm, or insolvency firm; or (f) A Company service provider; or (g) A Single Family Office. A person who is an Authorised Person or a Registered Auditor is not a DNFBP.*
Registered auditor *or audit firm registered, licensed, or otherwise regulated by any competent authority worldwide.*

Another part of the third item is to extend data controller's obligations in relation to the data breach notifications. This would ensure that the data controller promptly notifies affected individuals in the event of a breach, providing them with relevant information about the nature of the breach and the measures taken.

The next goal is to implement certification schemes for data controllers. This will ensure compliance and adherence to established data protection standards.

It is worth noting that the last two items pertain to amendments to the AIFC DP Rules. The first one aimed to update the list of jurisdictions with adequate levels of data protection. This update aligns the AIFC with international practices and serves as a guarantee that personal data is transferred exclusively to jurisdictions with strong data protection laws. In addition, it will enhance trust in the AIFC's commitment and strengthen its reputation.

The second point draws significant attention, as the Office of the Commissioner of Data Protection has recently received numerous requests from AIFC Participants regarding the consideration of waiver of fees under section 19(2) of the Requirement to Notify the Commissioner of Data Protection. Specifically, section 19(2) requires all Data Controllers to notify the Commissioner of Data Protection about the details of Personal Data Processing operations as required by the Rules. Subrule 4.2.2 of the AIFC DP Rules, in turn, specifies the required contents of the notification and imposes certain fees for submitting it.

Having considered ongoing requests from Participants on this matter, it is proposed to reduce the amount of fees, which falls under section 19(2) of AIFC DP Regulations, by 50% to lessen the financial burden on AIFC Participants.

5. Operation of the proposed AIFC Act

[Please specify the key features of the proposed AIFC Act. What new rights and obligations does the proposed AIFC Act intend to create? How the proposed AIFC Act will affect existing rights and obligations?]

The proposed AIFC amendments intend to supplement existing data subjects' rights to demonstrate integrity and enhance overall data protection measures, ensuring a secure and transparent environment for personal data processing. In particular:

1) The detailed scope outlined in the proposed AIFC Act will determine the subjects of data processing, thereby indicating the rights and obligations of all parties concerned;
2) It will implement a fundamental right for data subjects: the right to withdraw their consent;
3) It will mandate data controllers to inform data subjects in the event of a data breach;
4) It will establish joint-controllers' rights and responsibilities.

6. Outcomes

[What goals would be achieved by implementing your proposal?
What potential negative outcomes could arise?]

Outcomes

1. Clarification on the Application of the AIFC DPR

a) **Clarity and transparency.** Indicating the detailed scope of the application of Data Protection Regulations is vital for both data subjects and data controllers and data processors, ensuring that everyone understands the boundaries of data protection.

b) By indicating the types of data processing, it gives a **clear understanding** of the *methods* through which personal data can be handled.

c) By specifying the individuals to whom regulations apply, it helps to understand their legal obligations.

d) Outlining what types of data is out of the scope of regulations helps to prevent regulatory overreach.

2. Designation of the DPO

a) One of the primary outcomes of appointing a Data Protection Officer (DPO) is to guarantee thorough **data compliance** across organisations that accommodate large-scale processing. DPO will handle important tasks instructed by data controller and data processor and conduct assessments on **high-risk data processing activities**.

b) Under the proposed amendment, a Data Protection Officer (DPO) will be required to be appointed in cases where data processing involves regular and systematic monitoring of data subjects on a large scale. Accordingly, AIFC Participants subject to the AIFC Anti-Money Laundering Rules—including Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions (DNFBPs), and Registered Auditors—may fall within the scope of entities obligated to designate a DPO. The outcome for AIFC Participants will be improved data privacy practices, expert guidance on handling sensitive information, and increased transparency in data processing and accountability, thereby maintaining responsible data management.

3. Establishment of Joint Controllership

Joint Controller means any Controller that jointly determines the purposes and means of Processing with another Controller. In practice joint controllers may define their respective responsibilities **in the legally binding written agreement**.

The implementation of joint controllers is of paramount importance, especially in scenarios involving data breaches. For instance, in the event of a data breach, all Controllers participating in the same processing activities will share joint and several liability for any resulting damages. Even in the absence of any breach, controllers and joint-controllers can be imposed fines based on their liabilities (please see the case between the ***NVSC and State Inspectorate on Data Protection***, which took place in 2021, Republic of Lithuania; Regional Administrative Court of Lithuania imposed fines on the NVSC and the ITSS, in their capacity as joint-controllers, for the breach of Articles 5, 13, 24, 32 and 35 of the GDPR).

In all cases, it is important to sign a written agreement with every controller, as joint controllers may be involved at different stages of the data processing so the level of responsibility of each of them must be assessed with regard to all the relevant circumstances in each case.

4. Right to withdraw a consent

a) **Absolute right.** Rights to withdraw consent is considered an absolute right. In the GDPR, it is specified that the data subject has the right to withdraw consent at any time (Article 7(3)). Thus,

implementation of the right to withdraw consent will demonstrate alignment with mentioned benchmark legal frameworks.

b) **Enhanced trust and control.** Knowing that the Data Subject can withdraw consent at any time fosters trust between data subjects and data controllers/data processors. In addition, it gives them to make decisions and take control over personal data.

5. **Notification on data breach to Data Subject**
   a) **Enhancing rights of data subjects.** In the interest of transparency and data subjects' rights, it is imperative that data subjects are promptly and directly notified about any data breach that affects their personal data. Data subjects should be the first to receive information about data breaches and the actions taken to address them.
   b) **Risk assessment and Remedial Actions.** Exhaustive mechanisms require a thorough risk assessment to understand the extent of the breach's impact. It also sets conditions which must be met before communication with the data subject, for example, if the data controller has implemented appropriate technical and organisational protection measures.

6. **Certification and Accreditation Schemes.**
   a) **International standards.** Certification schemes encourage the development of standardized data protection practices.
   b) **Accountability and assurance.** It fosters accountability, providing data subjects with the confidence that their personal data is managed in strict accordance with established frameworks, thus ensuring transparency and assurance.

As a result of the proposed amendments, we will fill certain gaps to provide certainty to AIFC Participants and everyone involved in the data processing. Additionally, the proposed amendments will bring in line the AIFC DPR with its counterparts in other peer jurisdictions.

7. Legislative amendments

[What legislative amendments are required to enforce the proposal?]
Amendments to the AIFC Data Protection Regulations
Amendment to the AIFC Data Protection Rules

Annex 2

AIFC DATA PROTECTION AMENDMENT REGULATIONS 2024

AIFC REGULATIONS NO. _ of 2024
November _, 2024

Astana, Kazakhstan

CONTENTS

PART 1: GENERAL

1. **Name**

These Regulations are *the AIFC Data Protection Amendment Regulations 2024*.

2. **Commencement**

These Regulations commence on 1 January 2025, except section 8 of these Regulations which commence on 1 June 2025.

3. **Legislative Authority**

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

4. **Interpretation**

Terms used in these Regulations have the same meanings as they have, from time to time, in the AIFC Data Protection Regulations, unless the contrary intention appears.

PART 2: AMENDMENTS TO AIFC DATA PROTECTION REGULATIONS

5. This Part amends the *AIFC Data Protection Regulations*.

6. In section 5 (Application of these Regulations), after "These Regulations apply within the jurisdiction of the AIFC", insert –

"(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 established 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 apply 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; or

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

7. After section 9 (Requirements for legitimate Processing), insert –

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

9-2. Right to withdraw consent

(1) Where the basis for the Processing of Personal Data is consent under section 9(a) or under Section 10(1)(a), the Data Subject may withdraw consent at any time by notifying the Data Controller in accordance with Section 9-1(5). Where a Data Controller has not complied with Section 9-1(5) a Data Subject may notify the Data Controller by any reasonable means.

(2) The right to withdraw consent is an absolute right available to a Data Subject if the basis for the Processing of the Data Subject's Personal Data is consent under section 9(a) or section 10(1)(a)."

8. After section 10 (Processing of Sensitive Personal Data), insert –

"**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 Court 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 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:

(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.

(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 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:

(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."

9. After Part 2 (Processing of Personal Data Generally), insert –

"**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:

(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:

(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 Contravenes 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.

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)."

10. After section 19 (Requirement to notify Commissioner about Personal Data Processing operations etc.), insert –

"**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 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)."

11. After section 24 (Commissioner's Objectives and Functions), insert –

"**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 3 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 Contravened 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."

12. In paragraph 3 (Definitions for these Regulations) of Schedule 1: Interpretation:

(a) after definition of 'AIFC Rules', insert –

"**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."

(b) after definition of 'Data Processor', insert –

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

(c) after definition of 'Document', insert –

"DPO means a data protection officer appointed by a Controller (including a Joint Controller), or Processor to independently oversee relevant data protection operations in the manner set out in sections 10-1, 10-2, 10-3 and 10-4."

(d) after definition of 'Governor', insert –

"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."

(e) after definition of 'Guidance', insert –

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

(i) 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;

(ii) 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;

(iii) 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

(iv) a material amount of Sensative Personal Data is to be Processed."

(f) after definition of 'Identifiable Natural Person', insert –

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

(g) after definition of 'Personal Data', insert –

"**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."

(h) after definition of 'Process', insert –

"**Profiling** means the automated Processing of Personal Data to evaluate the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements."

(i) in the definition of 'Sensitive Personal Data':

(i) after "(directly or indirectly)", omit "racial or ethnic origin, communal origin,";

(ii) after "sex life", insert "and including genetic data and biometric data where it is

used for the purpose of uniquely identifying a natural person."

(j) after definition of 'Sensitive Personal Data', insert –

"**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."

Annex 3

AIFC DATA PROTECTION AMENDMENT RULES 2024

AIFC RULES NO. _ of 2024
November _, 2024

Astana, Kazakhstan

AIFC DATA PROTECTION AMENDMENT RULES 2024

CONTENTS

AIFC DATA PROTECTION AMENDMENT RULES 2024

PART 1: GENERAL

1. Name

These Rules are *the AIFC Data Protection Amendment Rules 2024*.

2. Commencement

These Rules commence on 1 January 2025.

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.

4. Interpretation

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

PART 2: AMENDMENTS TO AIFC DATA PROTECTION RULES

5. This Part amends the *AIFC Data Protection Rules*.

6. In subrule 4.2.1 of rule 4.2 (Notifications about Personal Data Processing operations), after "the following Personal Data Processing operations", omit:

"performed or to be performed by or on behalf of the Data Controller:

(k) any Personal Data Processing operation, or set of operations, involving the Processing of Sensitive Personal Data;

(l) 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." and insert:

":

(a) Personal Data;

(b) Sensitive Personal Data;

(c) 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.".

7. In paragraph 1 of Schedule 1: Fees, after table, insert –

"Note: For the period commencing on 1 January and concluding on 31 December 2025, the fees under items 2 and 3 of the Table of fee are applied with 50% reduction."

8. In Schedule 2: Jurisdictions with adequate levels of protection for personal data:

(a) in paragraph 1 (Table of jurisdictions):

(i) before –

1.	Andorra

insert –

1.	Abu Dhabi Global Market

(ii) after –

6.	Bulgaria

insert –

7.	California

(iii) after –

17.	Germany

omit –

18.	Gibraltar

(iv) after –

25.	Italy

insert –

26.	Japan

(v) after –

38.	Romania

insert –

26.	Singapore (Including Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP))

(vi) after –

41.	Slovenia

insert –

42.	South Korea (Including Cross Border Privacy Rules (CBPR))

(vii) after –

47.	Urugay

omit –

	jurisdictions to which the US Department of Commerce and European Commission EU-US Privacy Shield Framework applies

(b) after paragraph 1 (Table of jurisdictions), insert –

"2. Additional Jurisdictions for Adequacy Approval

Pursuant to section 11(2) of the Regulations, the Commissioner may from time to time approve other jurisdictions, in addition to those listed above, as having an adequate level of protection for Personal Data. The Data Protection section of the AIFC website contains the most up to date version of the above list."