GUIDANCE ON DATA PROTECTION AND AI IN THE AIFC

Astana, Kazakhstan

2024

I. INTRODUCTION

The goal of the Commissioner of Data Protection ("Commissioner") in producing this Guidance is to provide easy-to-understand information about the AIFC Data Protection Regulations No. 10 of 2017 (the "DP Regulations") and Data Protection Rules No.1 of 2018 (the "DP Rules"), as well as to address considerations related to the use of Artificial Intelligence ("AI") within the Astana International Financial Centre ("AIFC").

Personal Data is defined in the DP Regulations as "Any Data referring to an Identifiable Natural Person." Sensitive Personal Data is defined as "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership, and health or sex life." Such data includes, but is not limited to, name, address, business or personal email address, business or personal phone numbers, geolocations, job title or other employee data, health and biometric data, religious affiliations, or criminal history. In the context of AI, special consideration must be given to how AI systems process such data, ensuring that they operate in compliance with DP Regulations.

II. SCOPE

This guidance should be read in conjunction with the existing AIFC DP Regulations and DP Rules. It also provides additional considerations specific to the use of AI technologies within the AIFC. Please note that this guidance expresses no opinion on the lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice. Please contact legal counsel for assistance in determining your data protection, privacy policies, and AI implementation strategies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.

III. GENERAL CONSIDERATION OF AIFC DP REGULATIONS, RULES, AND AI

The Commissioner is responsible for administering the DP Regulations and DP Rules in the Astana International Financial Centre (the "AIFC"). This framework governs how Personal Data may be collected, used, stored, and transferred, including when AI systems are involved. AI systems, due to their capacity for processing large amounts of data and identifying patterns, must adhere strictly to these regulations to prevent misuse or unlawful data processing. AI models must be customized and managed with stringent data governance practices. This includes data minimization, quality control, and continuous monitoring to ensure the AI system's accuracy, fairness, and compliance with legal requirements.

AI Strategy

Organisations should formulate an AI Strategy to demonstrate the commitment of top management to the ethical and responsible procurement, implementation and use of AI. The AI Strategy, which should provide directions on the purposes for which AI solutions may be procured, and how AI systems should be implemented and used, may include the following elements:

1. Defining the functions that AI systems would serve in the technological ecosystem of the organisation;

2. Setting out ethical principles for the procurement, implementation and use of AI solutions that are specific and applicable to the organisation by referring to the Ethical Principles for AI;
3. Determining the unacceptable uses of AI systems in the organisation;
4. Establishing an AI inventory to facilitate the implementation of governance measures;
5. Establishing specific internal policies and procedures regarding how to ethically procure, implement and use AI solutions;
6. Ensuring that the appropriate technical infrastructure is in place to support lawful, responsible and quality AI implementation and use, ranging from data storage, management and processing tools, and computing resources and facilities, to machine learning operations for deployment and monitoring, etc;
7. Regularly communicating the AI strategy, policies and procedures to all relevant personnel, including internal staff at all levels and, where appropriate, external stakeholders such as business partners and customers;
8. Considering emerging laws and regulations that may be applicable to the procurement, implementation and use of AI, including data protection and intellectual property laws.

Key Concepts Relevant to AI

To fully understand the application of the DP Regulations and DP Rules in the context of AI, it is essential to grasp the following concepts: Personal Data, Sensitive Personal Data, Processing, Data Subject, Data Processor, and Data Controller. Each of these concepts is defined in the DP Regulations and will be explained in this guide with additional focus on their implications for AI.

Personal Data and AI

AI systems often process vast amounts of Personal Data to function effectively. Personal Data in the context of AI includes data generated or inferred by AI systems, such as user profiles, behavioral predictions, and other analytics that can identify an individual. AI developers and operators must ensure that the collection and processing of this data comply with DP Regulations, particularly regarding consent, purpose limitation, and data minimization.

Sensitive Personal Data and AI

Sensitive Personal Data processed by AI systems requires special protection due to the potential for significant harm if misused. AI systems that analyze or infer sensitive data categories must implement stringent safeguards, including enhanced encryption, access controls, and anonymization techniques, to protect this data from unauthorized access or breaches.

Processing and AI

Processing in the context of AI refers to any operation performed on Personal Data by an AI system, including collection, analysis, inference, storage, and deletion. The broad definition of Processing in DP Regulations means that virtually all AI activities involving Personal Data must be scrutinized to ensure compliance. AI systems should be designed with privacy by design principles, embedding data protection throughout the entire lifecycle of data processing activities.

Data Controller, Data Processor, and AI

AI systems can function as Data Controllers or Data Processors depending on how they are utilized. An AI developer or operator may be a Data Controller if they determine the purposes and means of processing Personal Data. Conversely, if an AI system processes data on behalf of another

entity, it acts as a Data Processor. Regardless of the role, it is crucial that AI systems are configured to uphold the responsibilities outlined in the DP Regulations.

AI-Specific Considerations

1. **Transparency and Explainability**: AI systems must operate transparently, providing Data Subjects with clear information about how their data is being used and processed. Explainability is crucial, particularly in automated decision-making, to ensure that decisions made by AI can be understood and contested if necessary.

2. **Fairness and Non-Discrimination**: AI systems must be designed to prevent bias and ensure fairness, particularly when processing Sensitive Personal Data. Algorithms should be regularly audited for discriminatory outcomes and adjusted to mitigate any identified biases.

3. **Accountability**: AI developers and operators must ensure that there are mechanisms in place to hold them accountable for the AI system's data processing activities. This includes maintaining records of processing activities, conducting regular audits, and implementing robust data protection impact assessments (DPIAs). Organizations must ensure transparency in AI operations by providing clear information to data subjects about how their data is used.

4. **Anonymisation and AI**: While anonymisation of Personal Data can be challenging in AI, it is a crucial step to mitigate risks. AI systems should employ advanced anonymisation techniques, ensuring that even sophisticated re-identification attempts are thwarted. However, as AI technologies evolve, entities must stay informed about new risks and adapt their anonymisation strategies accordingly.

IV. DATA SUBJECT RIGHTS IN THE CONTEXT OF AI

Data Subjects have specific rights under the DP Regulations that must be upheld when AI systems process their Personal Data.

These rights include:

1. **Right to information about personal data and to rectification (section 17 of DP Regulations)**

   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;
   (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. Rectification may be understood as the right to ask and obtain from the Data Controller the correction of inaccurate data and the completion of incomplete data.

In the context of AI, these rights are particularly important because AI systems can generate inferences or predictions about individuals that may be inaccurate or biased. Data Subjects must have the ability to challenge and correct such data.

2. **Right to object to Processing (section 18 of DP Regulations)**

   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.

If there is a justified objection by A in relation to Personal Data, the Data Controller must no longer process that Personal Data. This right is crucial in AI applications, particularly in automated decision-making processes where individuals may want to contest the processing of their data or its use in specific AI-driven decisions.

V. COMPLIANCE WITH DP REGULATIONS IN AI SYSTEMS

Compliance with DP Regulations in the context of AI involves several steps:

1. **AI Strategy and Governance:** Organizations should establish an AI strategy that outlines the ethical principles guiding AI procurement, implementation, and use. This strategy should include governance structures like an AI governance committee, regular updates based on stakeholder feedback, and a clear definition of unacceptable AI uses.

2. **Data Protection by Design and by Default**: AI systems should be designed with data protection principles at their core, ensuring that privacy is maintained throughout the data processing lifecycle.

3. **Data Minimisation**: AI systems should collect and process only the data necessary for the specific purposes identified, avoiding unnecessary data accumulation.

4. **Consent Management**: When AI systems process Personal Data, especially for purposes beyond the initial scope, explicit and informed consent must be obtained from Data Subjects.

5. **Data Subject Rights**: AI systems must be configured to respect the rights of Data Subjects under the DP Regulations, including rights to access, rectification, erasure, and objection to processing.

6. **Risk Management**: Regular risk assessments should be conducted to identify and mitigate any potential threats to data privacy posed by AI systems. A comprehensive risk assessment must be conducted during the procurement and use of AI systems, with human oversight tailored to the risk levels. High-risk AI systems should incorporate a 'human-in-the-loop' approach to maintain accountability.

VI. NOTIFICATION AND PERMITS FOR AI DATA PROCESSING

Annex 1 to this Guidance provides template notification form in relation to data processing in the AIFC that must be sent to the following email: dataprotection@aifc.kz according to section 19 of DP Regulations.

VII. QUESTIONS AND COMMENTS

Please contact the AIFC Commissioner of Data Protection (the Commissioner) either via email at dataprotection@aifc.kz or via regular mail sent to the Office of Commissioner of Data Protection at Office 336, 55/18 Mangilik El Ave., block C3.3, Astana, Kazakhstan for any clarifications or questions related to this document.

To the Commissioner of Data Protection of
Astana International Financial Centre

No. _____
[Month] ___, [Year]

Re: <u>On notification about Personal Data Processing operations</u>

Hereby [company legal name] (*hereinafter referred to as "the Company"*) kindly requests to accept and process notification about Personal Data Processing operations concerning personal data protection by the Company as per the Annex 1 to this letter.

- Annex 1 – Application for notification about Personal Data Processing operations.

Sincerely,
[company executive, director, or other senior staff responsible for data protection]

_____

[Name Surname]

Annex 1

Application for notification about
Personal Data Processing operations

Reference: Section 19(2) (Requirement to notify Commissioner about Personal Data Processing operations etc.) of the AIFC Data Protection Regulations

Information type	Description
(a) a general description of the Personal Data Processing operations	***For example:*** *Personal data that the Company controls may be processed by both automated and manual means. The company processes personal data in the Company's offices, data centres as well as outsources processing to the third-party data processor.*
(b) an explanation of the purpose of the Personal Data Processing operations	***For example:*** *- accounting and auditing* *- consultancy and advisory services* *- advertising, marketing and public relations for the Data Controller* *- licensing and registration* *- provision of financial services* *- staff administration* *- to comply with any legal obligation to which the Company is subject*
(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	***For example:*** *- staff, including agents, temporary and casual workers* *- clients and customers* *- suppliers* *- beneficiaries* *- directors*
(d) a description of the class of Personal Data being processed	***For example:*** *Personal data include all personal data received by us from Data Subject, third persons or publicly accessible sources or available with us that is necessary for the performance of a contract to which the Data Subject is a party on the properly legal basis, required to including but not limited to the data specified in the questionnaires and other fill-in forms. This includes data on property, property rights and liabilities, data of contracts (including names, numbers and conclusion dates), data on the accounts opened with us or third parties with us, data on transactions and other operations performed by Data Subject or on behalf or for the benefit of Data Subject as well as the specified (updated, amended) data received by us subsequently.*
(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.	***For example:*** ***Jurisdictions with adequate level of protection for Personal Data per AIFC list (Schedule 2, AIFC Data Protection Rules No.1 of 2018):*** *- Netherlands (EU GDPR)* *- Cyprus (EU GDPR) etc.*