Approved by the Board of Directors

Approval Date: 12.07.2023

NGDEM Global Limited

DATA PROTECTION POLICY

This Data Protection Policy of NGDEM Global Limited (from now on – Firm) has been designed to maintain a good understanding of and strict compliance with applicable laws and regulations in part of personal data protection.

This Data Protection Policy (from now on – Policy) is based on applicable laws, including Astana International Financial Center (from now on – AIFC) acts and the Firm's internal documents.

1. General provisions

1.1. This Policy has been developed in compliance with the data protection laws of the Astana International Financial Centre (from now on – AIFC) and the internal regulations of the Firm.

1.2. This Policy incorporates key definitions and abbreviations provided by the relevant legislation and internal regulations of the Firm, as well as the following terms and definitions:

– Personal Information (Personal Data) – any data concerning a specific individual or an identifiable individual recorded on electronic, paper, or other tangible media;

– Data Subject – an individual who can be directly or indirectly identified based on Personal Information;

– Sensitive Personal Information – Personal Information that reveals or pertains to racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade union membership, and health or sex life;

– Subject of personal data – the natural person to whom the personal data relates;

– DPO – an employee of the Firm responsible for coordinating work on compliance by the Firm with legislation on the protection of personal data and the Policy;

– Processing of personal data – actions aimed at accumulation, storage, modification, addition, use, distribution, depersonalisation, blocking and destruction of personal data;

– Storage of personal data – actions to ensure personal data's integrity, confidentiality and availability.

2. Principles of Personal Information Processing

2.1. The Firm processes Personal Information under fairness, lawfulness, and security principles.

2.2. Personal Information is processed by the Firm for specific, explicit, and legitimate purposes based on the consent of the Data Subject.

2.3. During the processing of Personal Information, the Firm ensures that it is adequate and relevant to the purposes for which it is collected or further processed. The processing of Personal Information should be reasonable for the declared purposes.

2.4. The Firm ensures that the Personal Information is processed:

– is accurate and up-to-date, as required;

– is retained in a form that allows the identification of a Data Subject only for the necessary period, based on the purposes for which the Personal Information was collected and further processed.

2.5. The Firm processes Personal Information at the request of the Firm or based on the relevant requirements of the applicable legislation.

2.6. Data Subjects have the right to request information regarding the collection and processing of their Personal Information and to request the correction, deletion, or blocking of Personal Information.

2.7. The AIFC Data Protection Regulations define issues of interaction with the Commissioner.

3. Purposes and duration of Personal Information processing

3.1. Processing of Personal Information refers to any action or set of actions related to Personal Information, whether automated or not. This includes collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure, transmission, dissemination, blocking, erasure, or destruction of Personal Information.

3.2. The purpose of this policy is:

– ensuring the protection of personal data with which the Firm work, taking into account all automated and telecommunication systems, the owner and / or user of which is the Firm;

– prevention of destruction, loss or theft of personal data;

– determination of information related to personal data with which the Firm work, determination of the permissible purposes for collecting this information;

– ensuring the availability of the necessary consent from the subjects of personal data;

– definition of duties and areas of responsibility of the DPO and other employees of the Firm regarding collecting and processing personal data.

3.3. The Firm collects and processes Personal Information for the following purposes (if applicable):

– Provision of services specified in the License to clients according to the terms of the Regulations;

– Biometric identification of clients (agents and representatives) when establishing remote business relations, as well as during the provision of electronic services according to the terms of the Regulations;

– Internal control, monitoring, and accounting of services provided by the Firm to clients according to the terms of the Regulations;

– Performance of due diligence of clients (agents and representatives) by the Firm as a financial monitoring entity under applicable legislation when establishing business relations and conducting transactions;

– Ensuring compliance with legislative requirements applicable to the Firm and its affiliates;

– Development and improvement of services provided by the Firm and its affiliates;

– Development of marketing and advertising campaigns by the Firm and its affiliates for marketing purposes, including the provision of information materials to clients;

– Authentication and authorisation of clients (agents and representatives) to access the Firm's systems and platforms;

– Compliance with reporting and disclosure obligations imposed by applicable laws and regulations;

– Resolution of disputes and enforcement of contractual obligations between the Firm and its clients;

– Protection of the rights and legitimate interests of the Firm, its clients, and third parties;

– Fulfillment of other obligations and exercise of rights arising from the License and applicable legislation.

3.4. The duration of Personal Information processing by the Firm may vary depending on the specific purpose for which it is collected and processed. Personal Information is retained for as long as necessary to fulfil the purposes outlined in this Policy or as required by applicable laws and regulations.

4. Basic requirements for the protection of personal data

4.1. The protection of personal data in the Firm is carried out by applying a set of measures, including legal, organisational and technical, to:

– realisation of the rights to privacy, personal and family secrets;

– respect for their confidentiality;

– exercising the right to access them;

– ensuring their integrity and safety;

– prevention of their illegal collection and processing.

4.2. The obligations of the Firm to protect personal data arise from the moment of collection of personal data and are valid until the moment of their destruction or depersonalisation.

5. Rights and obligations of Data Subjects

5.1. Data Subjects have the following rights regarding the processing of their Personal Information:

– The right to be informed: Data Subjects have the right to obtain information about collecting and processing their Personal Information with the Firm.

– The right to access: Data Subjects have the right to access their Personal Information held by the Firm and to obtain copies of their Personal Information unless otherwise provided by applicable laws and regulations.

– The right to rectification: Data Subjects have the right to request the correction or amendment of their inaccurate or incomplete Personal Information held by the Firm.

– The right to erasure: Data Subjects have the right to request the deletion or removal of their Personal Information held by the Firm, subject to certain conditions and exceptions under applicable laws and regulations.

– The right to restriction of processing: Data Subjects have the right to restrict the processing of their Personal Information by the Firm under certain circumstances provided by applicable laws and regulations.

– The right to data portability: Data Subjects have the right to receive their Personal Information in a structured, commonly used, and machine-readable format and to transmit that data to another data controller, where technically feasible.

– The right to object: Data Subjects have the right to object to the processing their Personal Information by the Firm in certain situations, including direct marketing purposes.

– The right to withdraw consent: Data Subjects have the right to withdraw their consent to processing their Personal Information at any time, where the processing is based on their consent.

5.2. Data Subjects also must provide accurate and up-to-date Personal Information to the Firm and inform the Firm of any changes or inaccuracies in their Personal Information.

6. Personal Information security

6.1. The Firm implements appropriate technical and organisational measures to ensure Personal Information's security and protect it against unauthorised access, disclosure, alteration, or destruction.

6.2. These measures include:

– Restricting access to Personal Information on a need-to-know basis, with access granted only to authorised individuals who require access to perform their duties.

– Implementing physical, electronic, and procedural safeguards to protect Personal Information during collection, storage, and transmission.

– Regularly monitoring and reviewing the effectiveness of security measures and updating them as necessary to address new security risks and developments.

– Conducting periodic training and awareness programs for employees to ensure they understand their responsibilities in safeguarding Personal Information.

– In case of a Personal Information breach, the Firm will promptly take appropriate measures to mitigate the impact of the breach and notify the affected Data Subjects and the relevant authorities as required by applicable laws and regulations.

7. Restrictions on the use of information

7.1. All employees of the Firm in terms of personal data must:

– before performing functional duties, sign an agreement on non-disclosure of personal data;

– periodically undergo training (according to Annex 1 to the Policy) in terms of personal data protection (at least once a year, as well as during employment), and also be guided by the Employee Memo of Firm (Annex 2 to the Policy);

– immediately report to your manager and DPO information about violations of the requirements of the Policy and applicable law regarding the protection of personal data.

7.2. The heads of units of the Firm must ensure that their employees are provided with information (including access to information systems) only to the extent necessary to perform their functional duties.

7.3. Employees of the Firm inform the DPO of identified violations and shortcomings regarding personal data protection in Writing.

8. Transfer of Personal Information

8.1. The Firm may transfer Personal Information to third parties under the purposes specified in this Policy and applicable laws and regulations. These third parties may include:

– Regulatory authorities, law enforcement agencies, or other governmental entities as required by applicable laws and regulations.

– Affiliates of the Firm who assist in providing services to clients.

– Service providers, contractors, or agents the Firm engages to perform certain functions or services on its behalf.

8.2. When transferring Personal Information to third parties, the Firm takes steps to ensure that adequate safeguards are in place to protect the privacy and security of the Personal Information.

8.3. The Firm wishing to engage a third party to work with personal data, including those involving the cross-border transfer of personal data, must conduct a detailed check of such a person, which includes verification of the following:

– whether the country of location and registration of this person provides an adequate level of personal data protection, including under the standards of the European Union. The Firm is guided by AIFC Data Protection Rules (jurisdictions with adequate levels of protection for personal data);

– ensure that the transfer is in full compliance with local laws and regulations governing data protection and international transfers of personal data;

– availability of organisational and technical security measures in terms of data protection;

– the availability of the relevant consent of the subject of personal data or his legal representative (including, if necessary, for the cross-border transfer of his data) and the compliance of the purposes for the transfer of information to this person;

– the presence of provisions in the contract providing for the confidentiality of personal data and a ban on distribution without the consent of the subject of personal data and only for previously declared purposes;

– the presence of negative information.

8.4. The Firm must depersonalise personal data if transferred to third parties for statistical, sociological, scientific, or marketing research.

8.5. If access to the processing of personal data must be granted to persons who are not employees of the Firm (individuals involved under civil law contracts, representatives of counterparties, etc.):

– a confidentiality agreement must be signed with such a person;

– it is necessary to conduct a briefing on the basic requirements of the Firm in the field of processing and protection of personal data (conducted at the discretion of the Firm).

9. Storage of personal data

9.1. The Firm carries out storage of personal data in a database located on the territory of the Republic of Kazakhstan (AIFC jurisdiction).

9.2. The storage period of personal data is determined by the date of achievement of their collection and processing goals unless otherwise provided by the applicable legislation.

9.3. Storage of personal data of restricted access is carried out using cryptographic information protection tools that have parameters not lower than the third level of security under the standard of the Republic of Kazakhstan ST RK 1073-2007 "Means of cryptographic information protection. General technical requirements".

10. Depersonalization of personal data

10.1. Personal data is anonymised for statistical, sociological, scientific, and marketing research.

10.2. Anonymization of personal data is carried out before their distribution by any method of depersonalisation that does not contradict the legislation, allowing to solve the tasks of processing personal data.

10.3. The procedure for depersonalisation of personal data excludes the possibility of reverse recovery of the original personal data.

10.4. Reimbursement of expenses for anonymising personal data is carried out at the expense of the person who requested the anonymised personal data unless otherwise determined by the concluded agreement.

10.5. The description of the depersonalisation procedure provides an unambiguous interpretation of the ongoing actions to depersonalise personal data. It includes depersonalisation algorithms and procedure characteristics related to depersonalised data quality, labour intensity, and attack resistance.

10.6. Personal and anonymised data are stored separately using depersonalisation procedures.

11. Blocking of personal data

11.1. Personal data is blocked at the request of the subject of personal data if there is information about a violation of the conditions for collecting and processing personal data.

11.2. The Firm blocks personal data related to personal data within one working day if there is information about a violation of the conditions for their collection and processing.

12. Destruction of personal data

12.1. Personal data is subject to destruction:

– after the expiration of the storage period;

– upon the termination of legal relations between the Firm and the subject of personal data;

– upon entry into force of a court decision;

– at the request of the subject of personal data if personal data was collected and processed in violation of the legislation;

– in other cases established by the applicable legislation on protecting personal data.

12.2. Personal data is destroyed by deleting information or destroying material carriers of personal data.

13. Powers and Responsibilities of the DPO

13.1. DPO features include:

– coordination of measures to create an effective system for the protection of personal data in the Firm;

– implementation of internal control over compliance by the Firm and its employees with the Policy and applicable legislation on personal data and their protection;

– keeping records of all revealed facts of violations of the Policy and applicable legislation regarding the protection of personal data, control over the development and implementation of corrective measures by responsible employees;

– participation in the verification process of third parties with access to personal data, in cases specified by concluded agreements and applicable law, monitoring the inclusion of special conditions and provisions on the protection of personal data in contracts with such persons;

– exercise control over the process of receiving and timely processing of applications from personal data subjects or their legal representatives;

– support for inspections carried out by state bodies in terms of personal data protection;

– bring to the attention of the employees of the Firm periodically the main requirements of the applicable legislation in terms of data protection, conduct training and testing the acquired knowledge (if necessary);

– ensuring the storage of information and materials obtained as part of the above activities.

13.2. DPO has the right to involve any employees of the Firm in the processes of conducting internal investigations related to possible violations of the Policy, assessing the impact on the protection of personal data, and other processes related to compliance with the Policy and applicable legislation on the protection of personal data.

13.3. DPO, on an ongoing basis, informs the management and the CEO of the Firm about any violations or shortcomings in implementing the Policy and applicable legislation regarding protecting personal data.

14. Final provisions

14.1. Violating any applicable laws, rules and regulations or any policies, rules or procedures outlined in this Policy may result in disciplinary action, including but not limited to oral or written warning, demerit, bonus adjustments and contract termination as appropriate.

14.2. The DPO is responsible for the revision of this Policy. The policy is updated periodically, not less than once every year, or when changes or additions to the applicable laws and AIFC Acts are made available throughout the Firm.

14.3. If, as a result of changes in the AIFC legislation, certain paragraphs of this Policy contradict the current AIFC Acts or applicable laws, the latter shall prevail, and the Firm takes measures to amend this Policy in compliance with applicable regulations.

14.4. In situations not covered by this Policy, an employee should seek advice from the DPO. If employees, customers, or counterparties have questions or difficulties related to data protection, they can contact the DPO.

14.5. Issues of possible material outsourcing or delegation arrangement within the framework of Policy are reflected in the Outsourcing Rules of the Firm.

14.6. The Firm may occasionally update or amend this Policy to reflect changes in its privacy practices or applicable laws and regulations.

Annex 1

to the Data Protection Policy

List of questions included in the training course

The list of questions included in the training course, but not limited to:

1. Requirements of the applicable legislation regarding the protection of personal data:

– AIFC Data Protection regulations;

– AIFC Data Protection Rules (DPR).

– Law of the Republic of Kazakhstan "On personal data and their protection" and other normative acts of the Republic of Kazakhstan.

– Information about the Regulation of the European Parliament and the Council of the European Union "On the protection of individuals about the processing of personal data and the free circulation of such data, as well as repealing Directive 95/46" (General Regulation on the protection of personal data).

2. Information about internal documents and procedures of the Firm.

3. Other information (optional).

Annex 2

to the Data Protection Policy

Memo for employees of the Firm

1. Do not disclose the personal data of other company employees and third parties that become known in performing official duties.
2. Do not post in the public domain (corporate address books, directories, a portal, Internet sites, etc.) the personal data of employees of the company and third parties, except data recognised by employees as public (full name, position, work phone and e-mail, photo, date, month and year of birth).
3. Do not transfer processed personal data to other employees of companies that are not allowed to process personal data.
4. Before starting the processing of personal data, make sure that:
   – during the absence from the workplace, no unauthorised access was made to the personal workstation, information system, safe or cabinet (drawer);
   – the workplace is organised in a way that excludes the viewing of information from paper (documentary) carriers of personal data, as well as from the display of the workstation (computer/laptop) by unauthorised persons;
   – means of processing personal data are in good condition.
6. After the end of the working day, remove all personal data carriers (flash drives, disks, paper documents, etc.) in safes or lockable metal cabinets (boxes).
5. Comply with the requirements for working with personal data (on any media), including taking personal data media outside the company's territory with a working need.
7. Before transferring personal data to a third party, ensure that the consent of the subject of personal data has been obtained.
7. Before transferring personal data to a third party, make sure that the contract with the third party contains requirements to ensure the confidentiality of the transferred personal data.
8. Keep secret logins and passwords to access the operating and application systems.

10 Promptly inform DPO:

   – in case of detection of attempts of unauthorised access to the workstation, information system, safe, closet, etc.;
   – about attempts to disclose personal data that have become known to him, as well as about other reasons or conditions for possible leakage of personal data;
   – in case of loss of the carrier of personal data;
   – in case of deviations from normal functioning, unstable operation or failure of the technical components of information systems.