

## PERSONAL DATA PROCESING POLICY

POLICY of "GLOBAL FX" on personal data processing A Foreign entity – "GLOBAL FX", hereinafter referred to as the Company, establishes the Company's policy for processing the personal data of (hereinafter referred to as the Policy): individuals, including individual entrepreneurs; individuals - beneficial owners of legal persons, or those that have the ability to control the actions of legal entities; the individual who is the beneficial owner of an individual, except if there is reason to believe that the beneficial owner is other individual person. The aforementioned persons for the purposes of this Policy shall be referred to as the "Contractors" and each of them individually "Contractor". The "Company" and "Contracting Party", including representatives of each of them, for the purposes of this Policy are referred to as "Partners".

### General provisions

1. This Policy governs the relationship between Company and Contractors in connection with the processing of their personal data contained in the documentary and (or) nondocumentary (electronic) databases by using automation technology, including information and telecommunications networks (including the Internet), or without such means, if the processing of personal data without the use of such means is consistent with the nature of actions (operations) performed with personal data using the automation tools, i.e. allows to search, in accordance with specified search algorithm, the personal data recorded on a tangible medium and contained in files or other systematic collections of personal data, and (or) access such personal data.
2. This Policy applies to the Contractors of the Company and (or) other Contractors, as well as their representatives.
3. The Policy is aimed at protecting the rights and freedoms of the Partners in the processing of their personal data, including protection of the right to inviolability of private life, personal and family privacy of each of them, as well as the confidentiality of this information.
4. This Policy applies to cases when the processing of personal data of Contractors, Partners, allows them in existing or potential circumstances increase revenues, avoid unnecessary expenses, maintain the position on the market of goods, works, services, or get a commercial advantage. In this case, in respect of personal data, the privacy mode is established, which is under the law on commercial secret.
5. This Policy applies to the processing of personal data included in insider information, as well as in the case when personal data operator is an insider. The Policy is valid where it does not contradict the legislation and other legal acts regulating the provision and distribution of insider information.

### Basic concepts

Personal data is any information relating to, directly or indirectly, a specific or identifiable individual (personal data subject) or his representative, the information contained in the documentary and (or) non-documentary (electronic) databases. Processing of personal data is any action (operation) or a set of actions (operations) performed in the information system using the automation tools (processing of personal data by means of computer facilities) or without using such means with personal information, including collection, recording, systematization, accumulation, storage,

updating, modifying, retrieval, use, transfer (distribution, provision, access), depersonalization, blocking, erasure, destruction of personal data. Cross-border transfer of personal data - transfer of personal data to the territory of a foreign state to an authority of a foreign state, a foreign individual or foreign legal entity. Operator of personal data is the Company, its Contractors, who, whether alone or jointly with others, organize and (or) carry out the processing of personal data, as well as define the purpose of the processing of personal data, the composition of the personal data to be processed, the actions (operations) performed with personal data. The operator of personal data can be represented by a person to which the Company entrusts the processing of personal data on the basis of a concluded contract with that person. Operators of personal data may not be represented by the Contractor and its individuals, as well as third parties who carried out the unlawful or accidental access to personal data, despite their performance of the processing of personal data. Contractors of Partners - the individuals, including the individual entrepreneurs, having legal relations with the Company on the basis of concluded contracts and agreements of a civil nature, their representatives, as well as individuals specified in the third and fourth preambular paragraphs of the present Policy. Current threats to security of personal data - a set of conditions and factors that create actual risk of unauthorized, including accidental, access to personal data when they are processed in the information system using automation tools, which can result in destruction, modification, blocking, copying, making available, distribution of personal data, as well as other illegal actions.

#### Processing of personal data

1. Processing only applies to personal data that meet the objectives of the processing.
2. The content and volume of the processed personal data must comply with the stated purposes of the processing. Processed personal information must not be excessive in relation to the stated objectives of processing.
3. In accordance with the Policy, the processing of personal data is required in order to:
  - protect the life, health or other vital interests of personal data of Contractors of Partners, if it is impossible to obtain their consent;
  - perform the contract, the party or the beneficiary or sponsor to which is the Company or the Contractor, including in the case of exercising of the Company's right to the assignment of the rights (demands) under such contract, as well as to the conclusion of the contract on the initiative of the Company or the Contractor, to which the Company or the Contractor will be the beneficiary or sponsor;
  - publish or mandatorily disclose the personal data of Contractors of Partners in accordance with the legislation;
  - promote goods, works and services in the market through direct contacts with potential Contractors using means of communication.
4. The processing of personal data must be carried out in a legal and fair manner.
5. The processing of personal data should be limited to the achievement of specific, pre-defined and legitimate purposes. The processing of personal data is not permitted, if it is incompatible with the purposes of collecting personal data.
6. For the processing of personal data, the accuracy of the personal data, their sufficiency and, where necessary, and relevance in relation to the purposes of processing personal data shall be ensured.

Personal data operator shall take the necessary measures or have them taken for removal or refining of incomplete or inaccurate data.

7. Storage of personal data is carried out by the Company, as well as persons specified in parts 5 and 6 of article V of the Policy, in documentary and (or) electronic forms, within a time period which shall be not less than 5 years. A longer period of storage of personal data can be stipulated in agreements, to which the Contractor is the beneficiary or sponsor.
8. The processing of personal data of Contractors of Partners is carried out subject to their consent to the processing of such personal data, except as required by law and the Policy.
9. The Contractors of the Company express consent to the processing of their personal data by the Operator of personal data, except for other Contractors and their individuals, as well as third parties as a result of their unauthorized or accidental access to personal data.
10. Personal data operator that performs the processing of personal data on behalf of the Company shall not be obliged to obtain the consent of Contractors to processing of their personal data.
11. In case the Company entrusts the processing of personal data to other Operator of personal data, the Company bears the liability to Contractors for the actions of that person. Personal data operator that performs the processing of personal data on behalf of the Company shall be liable to the Company.

Personal data operator responsible for the organization of processing of personal data shall, in particular:

- carry out the internal monitoring of compliance by it and its employees with the legislation on personal data, including personal data protection requirements;
  - bring to the attention of the employees of the Operator of personal data the personal data laws and international legal acts, this Policy on the processing of personal data, the personal data protection requirements;
  - organize the reception and processing of appeals and requests of Contractors or their representatives and (or) supervise the reception and processing of such applications and requests;
  - not transfer its commitments to other persons in any form whatsoever.
12. The Contractor and its individuals, as well as third parties who, as a result of unauthorized or accidental access to personal data, may exercise their processing, bear legal responsibility to the Company and (or) the Operator of personal data.

#### Cross-border transfer of personal data

1. The Company is a resident of a state which is not a party to the Council of Europe's Convention on the protection of individuals with regard to automatic processing of personal data and can be included to the list of foreign states ensuring the proper protection of the rights of Contractors of Partners, subject to compliance of the state's established laws and measures of personal data security with the provisions of the said Convention.
2. For the purposes of this Policy, the cross-border transfer of personal data is carried out in cases of the execution of the agreement, to which the Contractor is a party, as well as for the protection of life, health, and other vital interests of the Contractor or third parties, if it is impossible to obtain the written consent of the Contractor in the cases stipulated by the legislation and this Policy.
3. Prior to the implementation of the cross-border transfer of personal data and their subsequent processing, the Company ensures the proper protection of the Contractors' rights by:

- determining the threats to the security of personal data during their processing in the information systems of personal data;
  - taking the organizational and technical measures to ensure the security of personal data processing in the information systems needed to comply with the requirements to protection of personal data, which provide the levels of protection of personal data;
  - applying the means of information protection, which properly passed the conformity assessment procedure;
  - evaluating the effectiveness of the measures taken to ensure the security of personal data before commissioning of personal data information system;
  - accounting the machine carriers of personal data;
  - detecting the unauthorized access to personal data and taking measures to eliminate those violations;
  - restoring the personal data modified or destroyed as a result of unauthorized access to them;
  - establishing the rules of access to personal data that are processed in the information system of personal data, as well as ensuring the recording of all actions carried out with personal data in the information system of the personal data;
  - monitoring the measures taken to ensure the security of personal data and the level of security of the information systems of personal data.
4. This article applies to Contractors of Partners in case of legitimate cross-border transfer of their personal data. The Contractors of Partners guarantee and take the appropriate security measures to prevent accidental or unauthorized destruction of personal data, or the accidental loss, as well as to prevent unauthorized access, alteration or distribution of such data in accordance with the requirements laid down in national legislation and under the Convention on the protection of individuals with regard to automatic processing of personal data dated 28.01.1981 (hereinafter referred to as the "Convention"), taking into account the participation of the Member States of the Council of Europe that are the signatories to this Convention. If a resident state is not a party to the Convention, the Contractors of Partners comply with the requirements of this Policy.

#### Transfer of personal data

1. When transferring personal data of Contractors of Partners, unless otherwise provided for in the Policy, the following requirements shall be met:
2. It is prohibited to disclose personal data to third parties except when necessary to prevent a threat to life and health of Contractors, Contractors of Partners, as well as in cases stipulated by law.

For purposes of this paragraph, third parties shall mean any individuals or legal entities, with which the Contractors, Contractors of Partners may enter into legal relations on contractual and noncontractual basis.

3. It is prohibited to disclose the personal data of Contractors, Contractors of Partners for any purposes whatsoever, which do not match the purposes of this Policy.
4. Personal data operator is obliged to notify the Contractors, Contractors of Partners obtaining the personal information that these data may be used only for the purposes for which they are communicated, and demand written confirmation from these persons (or confirmation issued

in electronic form) that this rule is respected. The persons receiving the personal data are obliged to respect their privacy.

5. The operator of personal data is required to appoint an official (employee) responsible for ensuring the security of personal data in the information system. An official (employee) shall exercise control over the transfer of only those personal data that are needed to perform a specific function and for the purposes stipulated by the Policy.
6. Personal data are stored in the division for security and storage of personal data established by Contractors of Partners. In case of absence of such a division, the Contractor may conclude a contract with other Contractor - a legal entity, which has such a division, for storing personal data with compulsory written acknowledgement of this Policy.
7. The personal data can be obtained, further processed and transferred to storage both in documentary form and in electronic form.

#### Access to personal data

The right of access to personal data of Contractors of Partners is given to:

- the Contractors of Partners in relation to their personal data;
- the operator of personal data;
- a legal entity that has a division for security and storage of personal data, with which Contractors of Partners may conclude a contract.

#### Security of personal data

1. In addition to the implementation of actions provided for in part 3 of article IV of this Policy, the persons responsible for processing of personal data are obliged to take all necessary measures to counteract actual threats to security of personal data:
  - unauthorized access to personal data by Contractors, Contractors of Partners having authority in information system of personal data, including that in the process of development, operation, maintenance and (or) repair, upgrades, decommissioning of information system of personal data;
  - effects of malicious code that is external to the information system of the personal data;
  - use of social engineering techniques against Contractors, Contractors of Partners with the authority in the information system of personal data;
  - unauthorized access to removable media of personal data;
  - loss of personal data carriers, including the portable personal computers of users of the information system of personal data;
  - unauthorized access to personal data contained in the personal data information system using vulnerabilities in the security of personal data;
  - unauthorized access to personal data contained in the personal data information system using vulnerabilities in the software of personal data information system;
  - unauthorized access to personal data contained in the personal data information system using vulnerabilities in the security of networking and data transfer channels;
  - unauthorized access to personal data contained in the personal data information system using vulnerabilities in the security of computing networks of personal data information system;

- unauthorized access to personal data contained in the personal data information system using vulnerabilities caused by non-compliance with requirements to operation of cryptographic information protection facilities.
2. Current threats to the security of personal data are divided into 3 types and must be taken into account by the persons responsible for the processing of personal data in the exercise of security measures:
- Threats of type 1 are relevant for the information system, if its relevant threats also include threats associated with the presence of undocumented (undeclared) capabilities in the system software used in the information system.
  - Threats of type 2 are relevant for the information system, if its relevant threats also include threats associated with the presence of undocumented (undeclared) capabilities in the applied software used in the information system.
  - Threats of type 3 are relevant for the information system, if its relevant threats include threats not associated with the presence of undocumented (undeclared) capabilities in the system and applied software used in the information system.
3. With regard to the processing of personal data in information systems, there are 4 levels of protection of personal data:
- i) The level 1 personal data protection in the information system is required, when at least one of the following conditions is met:
- type 1 threats are relevant to the information system and it processes the special categories of personal data or biometric personal data, or other categories of personal data;
  - type 2 threats are relevant to the information system and it processes the special categories of personal data of over 100,000 personal data subjects who are not the employees of the personal data operator;
- ii) The level 2 personal data protection in the information system is required, when at least one of the following conditions is met:
- type 1 threats are relevant to the information system and it processes the public personal data;
  - type 2 threats are relevant to the information system and it processes the special categories of personal data of the employees of the personal data operator or the special categories of personal data of less than 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 2 threats are relevant to the information system and it processes the biometric personal data;
  - type 2 threats are relevant to the information system and it processes the public personal data of over 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 2 threats are relevant to the information system and it processes other categories of personal data of over 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 3 threats are relevant to the information system and it processes the special categories of personal data of over 100,000 personal data subjects who are not the employees of the personal data operator;



- c) The level 3 personal data protection in the information system is required, when at least one of the following conditions is met:
- type 2 threats are relevant to the information system and it processes the public personal data of the employees of the personal data operator or the public personal data of less than 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 2 threats are relevant to the information system and it processes other categories of personal data of the employees of the personal data operator or other categories of personal data of less than 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 3 threats are relevant to the information system and it processes the special categories of personal data of the employees of the personal data operator or the special categories of personal data of less than 100,000 personal data subjects who are not the employees of the personal data operator;
  - type 3 threats are relevant to the information system and it processes the biometric personal data;
  - type 3 threats are relevant to the information system and it processes other categories of personal data of over 100,000 personal data subjects who are not the employees of the personal data operator.
- d) The level 4 personal data protection in the information system is required, when at least one of the following conditions is met:
- 3 threats are relevant to the information system and it processes the public personal data;
  - type 3 threats are relevant to the information system and it processes other categories of personal data of the employees of the personal data operator or other categories of personal data of less than 100,000 personal data subjects who are not the employees of the personal data operator.
4. For ensuring the security of all levels of protection of personal data, in addition to obligations under parts 5 and 6 of article V, additional conditions must be met:
- automatic registration in electronic security log of appearance, modification and termination of the powers of the persons specified in article VI for access to personal data contained in the information system;
  - access to contents of electronic security log was possible solely for persons specified in article VI and strictly for the purposes stipulated by the Policy.
  - ensuring the security of personal data carriers;
  - organization of security of the premises hosting the information system, which eliminate the possibility of uncontrolled infiltration or stay in these premises of persons not having the right of access to these areas.
5. In the event of unlawful processing of personal data reported by the Contractors, Contractors of Partners, the Personal data operator is obliged to block the improperly processed personal data relating to Contractors, Contractors of Partners, or have them blocked upon such report. In case of detection of inaccurate personal data reported by Contractors, Contractors of Partners or their representatives, the Personal data operator is obliged to block the personal data relating to the Contractors, Contractors of Partners, or have them blocked upon such report, if the blocking of personal data does not violate the rights and lawful interests of Contractors, Contractors of Partners or other persons.

6. In the case of confirmation of inaccuracies of personal data, the personal data operator on the basis of the information submitted by Contractors, Contractors of Partners or their representatives, or other required documents must update the personal data or have them updated within seven working days from the date of the submission of such information and remove the blocking of personal data.
7. In the event of detection of unlawful processing of personal data carried out by the operator or the Contractors, Contractors of Partners, as well as by third parties, these persons within three working days from the date of this detection shall stop the unlawful processing of personal data or have it stopped. In case it is impossible to ensure the legitimacy of the processing of personal data, the stated persons, within a period not exceeding 10 working days from the date of the detection of unlawful processing of personal data, are obliged to destroy such personal data or ensure their destruction. The stated persons shall notify the Company, Contractors, Contractors of Partners or their representatives about elimination of the violations or destruction of personal data.
8. In the absence of the possibility of destruction of personal data within the term specified in part 4 of this article, the personal data operator blocks such personal data or has them blocked and secures the destruction of the personal data within a period of not more than six months, unless otherwise required by law.
9. In the event of the achievement of the purposes of personal data processing, the personal data operator must terminate the processing of personal data or have it terminated and destroy the personal data or have them destroyed not earlier than the time provided for in part 7 of article III of the Policy, or if the operator cannot execute the personal data processing without the consent of Contractors, Contractors of Partners - not earlier than the time provided for in this Policy and (or) the legislation.
10. In the Contractors, Contractors of Partners withdraw their consent to personal data processing, the personal data operator must terminate the processing of personal data or have it terminated and, if storage of the personal data is no longer required for the purposes of personal data processing, destroy the personal data or have them destroyed not earlier than the time provided for in part 7 of article III of the Policy, or if the operator cannot execute the personal data processing without the consent of Contractors, Contractors of Partners - not earlier than the time provided for in this Policy and (or) the legislation.
11. The withdrawal of consent of the Contractors, Contractors of Partners to the processing of their personal data may be submitted personally to the personal data operator in writing or through their representative, or by means of electronic communication.

The withdrawal of consent of the Contractors, Contractors of Partners to the processing of their personal data may be submitted personally to the personal data operator in writing or through their representative, or by means of electronic communication.

#### Confidentiality of personal data

1. The operator of personal data ensures the conditions of privacy and security of material carriers of personal data that eliminate the unauthorized access to them since the inception of these documents to expiry of their storage and destruction
2. The obligation envisaged in part 1 of this article occurs for all other persons which directly or indirectly gain access to personal data, including the information provided for in part 4 of article I.



3. In order to protect the confidentiality of personal data, the Company will provide all necessary legal assistance and support to the Contractor, Contractors of Partners, including reference to the competent authorities and organizations of the resident countries, international organizations and officials working in the area of financial markets, as well as the self-regulatory organizations of participants of civil legal community.

#### Responsibility for violation of the Policy

Personal data operator, the Contractors, Partners, Contractors of Partners or third parties shall bear legal responsibility in accordance with the law in case of their unauthorized or accidental access to personal data.

#### Allowable exceptions

The present Policy includes allowable exceptions, which do not contradict the legislation:

- under part 10 of article 3;
- the operator of personal data is released from the duty to provide Contractors, Contractors of Partners with information about the name or family name, first name, middle name and address of the operator of personal data or his representative;
- about the purpose of the processing of personal data and its legal basis;
- about the alleged users of personal data;
- about the rights of Contractors, Contractors of Partners under this Policy;
- about the source of personal data in cases when personal data operator obtains the personal data in accordance with the laws or in connection with the performance of the contract, the beneficiary or sponsor to which is the Contractor, Contractors of Partners;
- other exceptions stipulated by laws.

Consent of the Contractor to the Policy. The Contractor's consent to the processing of personal data

1. Contractor has carefully read the Policy, understands its meaning and contents, including special terms and definitions, and agreed with the Policy.
2. The Contractor agrees to fully comply with the Policy. In case of non-compliance in full or in part, the Contractor shall bear legal liability established by the legislation, including for the actions of all other persons prescribed by the Policy.
3. The Contractor agrees to the processing of his/her personal data freely, on the own free will and in the own interest, and strictly for the purposes set for the processing of such personal data.

\* The purpose of the processing of personal data (see: part 3 of article III) - CODE: 3/III.

\*\* List of personal data, the consent to processing of which is given: data contained in the ID of the Contractor, information about the occupation, subscriber number, information on participation in government of business partnerships and companies, the size of stakes (parts, shares), and any other personal data, including those contained in the agreements, the beneficiary or sponsor to which is the Contractor - CODE: LPD-1.

\*\*\* If unavailable, a hyphen is specified.

\*\*\*\* See: part 2 of article II, article III, IV, V, VII - CODE: 2/II-ETC.

\*\*\*\*\* See: part 10 of article VII - CODE: 10/VII.

In the case of incapacity of the Contractor which is an individual, the consent to the processing of his/her personal data is given by the legal representative of the Contractor who is an individual.

In case of death of the Contractor who is an individual, the consent to the processing of his/her personal data is given by the heirs of the Contractor who is an individual, if such consent was not given by such Contractor during the lifetime.

In case of reorganization of the Counterparty that is a legal entity, the consent to processing of its personal data is given by its successors - individuals who are the beneficial owners of the reorganized Contractor, or such persons who have the ability to control the actions of the reorganized Contractor; the individual who is the beneficial owner of an individual, except if there is reason to believe that other individual is the beneficial owner.

The personal data may be obtained by the Company from a person other than the Contractor, subject to providing to the Company the confirmation of grounds stipulated by the legislation.