Personal Data Processing Policy

The Bank and the Contractor shall be referred to individually as the "**Party**" and together as the "**Parties**".

Whereas,

The provisions on the processing of personal data of the data subjects defined herein represent a set of values, principles and norms that a person in a business relationship with the Bank shall use when processing Personal Data.

The term "Contractor" defined by this Policy means a natural and/or legal person who is in contractual relations with the Bank and the Agreement concluded with the Bank provides for a relevant reference to this Policy. The Policy is an integral part of the Agreement. Compliance with each provision of the Policy shall be mandatory for the Contractor, and its violation shall entail the consequences stipulated in the Agreement and the Policy.

1. GENERAL OBLIGATIONS OF THE CONTRACTOR

1.1. Personal Data shall be transferred to the Contractor under the Agreement concluded between the Parties, for the purposes specified in the Agreement. The Contractor shall process transferred Personal Data in compliance with the Agreement and legislation of Georgia solely for the purpose indicated herein and defined by the legislation of Georgia.

1.2. The Contractor undertakes to act in such a manner that processing of Personal Data will meet the requirements established by the personal data protection legislation of Georgia and international regulations and ensure the protection of the rights of the data subject.

1.3. The Contractor warrants that the Contractor will limit an access to personal data to a narrow circle of users/administrators and only grant the authority to those who have been given appropriate instructions in advance regarding data protection and who directly need access to the data, are aware of the obligation to protect the confidentiality/security of the data and ensure the protection of the confidentiality of the data, including in the event of termination employment contract.

1.4. The Contractor undertakes not transfer to a third-party personal data received from the Bank under the Agreement without the Bank's prior approval. If such an approval is provided, requirements envisaged hereunder will apply to any third party receiving the data, without any limitations.

1.5. The Contractor confirms that the Contractor will keep records of data processing activities.

1.6. The Contractor undertakes to work with the Bank to resolve data subject's access requests.

1.7. In case of the approval from the Bank, the Contractor shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved, where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

1.8. The Contractor undertakes to process Personal Data only in accordance with the Bank's specific instructions.

2. OBLIGATIONS REGARDING DATA PROTECTION

2.1. The Contractor undertakes to regularly take relevant technical and administrative measures with respect to the risks related to the nature of the data and the data subject in order to prevent unauthorized processing of personal data (including unauthorized dissemination, access, modification and destruction) .

2.2. The Contractor shall be on the lookout for any practices that violate the requirements established by the personal data protection legislation of Georgia and international regulations and should immediately notify the bank promptly.

2.3. Not Process Company Personal Data other than on the relevant bank's documented instructions including with regard to transfers of personal data to a third country or an international organization. The Contractor shall immediately regulations of any other state/jurisdiction.

2.4. The Contractor shall not transfer personal data outside of Georgia. In the event if the activities of the Contractor require transfer of personal data outside of Georgia, the Contractor will immediately notify the bank about this via e-mail, at the e-mail address privacycommittee@tbcbank.com.ge, and wait for the Bank's instructions regarding the mentioned. In any case, the transfer of the Personal Data to a third party is allowed, only with the assurance that the data will be transferred to such countries, which according to the legislation of Georgia and in accordance with the requirements of the GDPR regulations, are considered as so-called White list countries.

2.5. The Contractor shall not transfer or authorize the transfer of Personal Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected.

2.6. The Contractor may assign personal data processing to subcontractors only on special occasions and upon the Bank's written approval. These subcontractors shall have the appropriate security mechanisms in place and shall be subject to requirements envisaged hereunder, without any limitations. Assignment of personal data processing to subcontractors does not relieve the Contractor of the obligations assumed or limit the Contractor's responsibilities in case of damages resulting from the breach of the obligations.

3. SCOPE OF COOPERATION

3.1. Special Categories Personal Data is not transferred to the Contractor. Term Special Categories Personal Data shall have the meaning determined in Law of Georgia on personal Data Protection.

3.2. The Contractor shall work and cooperate with the Bank for the purposes to protecting the rights and privacy of data subjects.

3.3. The Contractor shall make available to the bank all information necessary to demonstrate compliance with the obligations laid down by the regulations on personal data protection.

3.4. The Contractor shall allow for and contribute to audits, including inspections, conducted by the bank or another auditor mandated by the bank in order to determine the compliance of personal data processing;

3.5. The Contractor shall assist the bank in data protection impact assessments where applicable.

3.6. In the case of involving sub-contractors in the process of personal data processing, the Contractor shall inform the Bank regarding the identity of subcontractors and make any changes related thereto only upon the Bank's written approval. The Bank is authorized not to approve the subcontractor proposed by the Contractor. Unless the disagreement is resolved through negotiations, the Bank is authorized to terminate the Agreement with the Party prematurely, without incurring any compensation liabilities.

4. INCIDENT REPORT RULES

4.1. In the event of accidental or unauthorized access to personal data, destruction, loss, alteration or disclosure of such data, the Contractor shall, immediately, but not later than 48 (forty-eight) hours after the occurrence of such incident, notify the Bank of the circumstances, face and time of the incident, and the disclosed/extracted/damaged/deleted/destroyed/lost personal data. Also, if possible, the Contractor provide the Bank with information on the data category and the exact amount and in what form the integrity of the personal data was violated (on the estimated categories and quantities of data, as well as on the estimated categories and number of data subjects that were threatened by the incident). The notification shall additionally contain the contact data of the person responsible for the protection of personal data and information on the means through which additional information may be obtained. The Contractor shall also inform the Bank if the Contractor had communicated with Personal Data Protection Inspector regarding the incident, in which chase the Bank shall have the right to request the Contractor all additional information regarding incident, which was shared with Personal Data Protection Inspector and the Contractor is obliged to comply with such request and provide aforementioned documentation/information to the Bank. The Bank will also be provided with information on the measures carried out or planned by the person responsible for processing for the alleged damage caused by the incident, reduction or elimination of the incident, as well as on whether the data is planned or planned in accordance with the procedure established by the legislation.

4.2. The Contractor shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effect and inform the Bank about these measures.

5. TERMINATION OF PROCESSING AND ERASURE OR DESTRUCTION OF DATA

5.1. The Contractor shall process and store Personal Data transferred to the Contractor by the Bank only for a period when the Agreement concluded between the Contractor and the Bank is effective (in force). Processing and storing Personal Data by the Contractor may be terminated in accordance with the legislation of Georgia or in accordance with the Agreement concluded between the Bank and the Contractor.

5.2. In the event that the data subject requests the termination of data processing, the exercise of other rights provided for by law (right to access and right to get a copy of the data, correction, updating, addition, blocking, termination of the data processing, deletion, portability, destruction, etc.) and / or information about data processing, including information (including but not limited to information determined in this Clause 5.1) the Contractor shall immediately but no later than on the second working day, notify the bank by e-mail to privacycommittee@tbcbank.com.ge about the above and wait for the bank's instructions. Upon the bank's instruction the contractor shall provide information to the data subject in the form requested him/her on the same day. Even if the bank does not respond to the contractor notification the contractor Within the time limit established by the legislation, is obliged to provide the requested information to the data subject. In case of violation of this specified rule, all responsibility lies with the contractor.

5.2.1. Which personal data are being processed;

5.2.2. The purpose of data processing;

5.2.3. The legal grounds for data processing;

5.2.4. The ways in which the data were collected;

5.2.5. On the shelf life of the data, and if a specific time limit cannot be determined, on the criteria for determining this term;

5.2.6. to whom the data was transfered (the identity of the data recipient or the categories of data recipients), the basis and purpose of the data transfer, as well as the appropriate guarantees of data protection, if the data is transferred to another state or international organization;

5.2.7. automated processing (if any), including the decision made as a result of profiling and the logic used to make such decisions, as well as its impact on data processing and the expected / likely outcome of processing.

5.3. In case of termination of the business activities by the Contractor and/or termination of the Agreement concluded between the Bank and the Contractor, the contractor shall immediately return to the bank and delete/destroy the personal data transferred to the contractor and their copies without the possibility of recovery. The Bank is entitled to request confirmation of data deletion from the party. This provision shall not apply to information which the Party is obliged to maintain under the effective Law or is entitled to do as stipulated by legislation.

5.4. In case of local laws applicable to the Contractor prohibit return or deletion of the personal data, the Contractor warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law.

5.5. Obligations related to personal data processing remain in force following the completion of the contractual relationship up to the date to which the Contractual Party maintains access to personal data transferred to it. This provision shall not be construed as the Contactor's right to maintain access to personal data transferred to it under the Agreement after the completion of contractual relationship. To the extent permitted under this Policy, the Contactor shall return and destroy/delete permanently personal data transferred to it by the Bank and copies thereof within a reasonable period after the completion of contractual relations but not later than 30 days.

6. INFORMATIONAL SYSTEM INFRASTRUCTURE SECURITY OBLIGATIONS

6.1. The Contractor is obliged to strictly observe the requirements of the Information System Infrastructure indicated below. The Contractor must be equipped with the following capability.

6.1.1. In order to store and process personal data of the Bank, there must be an isolated space that will be separated from the main infrastructure by an independent Firewall. Access to the Firewall of the space shall be

controlled by relevant authorized persons. Access to the information contained in the isolated space shall be allowed through Jump Server;

6.1.2. Integrity/accessibility of the space shall be monitored and controlled;

6.1.3. Any update on the servers contained in the space shall be monitored;

6.1.4. If possible, the personal data shall be encrypted via means of a complex algorithm;

6.1.5. Access to the isolated space shall be made through secured channel, via encrypted communication and in accordance with the security protocol;

6.1.6. Password policy shall be in place for the isolated space, defining the complexity, changing period and history of passwords;

6.1.7. Admin user passwords for the servers of the isolated space shall be divided into at least two parts and stored with different owners through secure channel;

6.1.8. Admin user passwords for the servers of the isolated space shall be managed through the privileged access management system (PAM);

6.1.9. Access to the space shall require Two Step Authentication;

6.1.10. The isolated space shall not be accessible via internet. Server log shall be maintained for isolated environment. Server log shall be stored in one place. Server log data may be used for investigation of an accident or a bug;

6.1.11. Remote storage/Cloud Service may not be used for storing, processing or transferring personal data.

6.1.12. The personal data processed during development or testing shall be defaced so that it would be impossible to directly or indirectly identify an individual;

6.1.13. A shredder or fire must be used for the destruction of information because of its aging or due to a special request. The process of destruction must be attended by a pre-selected representative of the Bank.

7. MISCELLANEOUS

7.1. The transfer of personal data by the bank to the Contractor shall be performed in accordance with the purposes and grounds provided for by the legislation.

7.2. The bank shall store and process personal data in accordance with the bank's internal procedures and the terms and conditions stipulated by the legislation in force.

7.3. In the event of any dispute between the parties, upon the bank’s request, the Contractor will transfer the data to the bank being in its possession.

7.4. In case of reasonable doubts, the Bank is authorized to check the performance of tools and systems used for processing personal data transferred to the Contractor, as well as their compliance with technical and administrative specifics under safety requirements set forth herein.

7.5. Depending on the gravity of the breach of the aforementioned guarantees, for the purpose of the inspection, the Bank is authorized to require of the contracting party the submission of relevant information and documents to the Bank.

7.6. The Bank fully releases the responsibility for any damage and cost resulting from deliberate or negligent breach of any of the obligations under this policy.