Personal Data Proccessing Policy

The provisions regarding the processing of personal data of subjects defined in this document establishes the values, principles and regulations, used by the person being in a business relationship with the Bank during the processing of personal data.

The term „Contractor“ defined by the policy, refers to natural and /or legal person being in a contractual relationship with the Bank Provided that the signed agreement makes a corresponding reference to this Policy. The policy is an integral part of the contract. Being in compliance with each provision set forth in the policy is mandatory for the contractor, and its violation leads to the consequences provided for in the contract.

Personal Data Proccessing Policy

1. Contractor\Processor represents and warrants that it will:

1.1. Process the data transferred to it in compliance with this Agreement and the Law of Georgia solely for the purpose indicated herein and defined by the Law of Georgia;

1.2. 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);

1.3. Works with the Bank with a view to protecting the rights and privacy of data subjects;

1.4. Should be on the lookout for any practices that violate the Requirements established by the legislation of personal data protection and international regulations and should immediately notify the bank promptly;

1.5. Should work with the bank to resolve subject access requests;

1.6. Act in such a manner that processing will meet the requirements established by the legislation of personal data protection and international regulations and ensure the protection of the rights of the data subject;

1.7. Makes available to the bank all information necessary to demonstrate compliance with the obligations laid down by the regulations on personal data protection;

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

1.9. 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:

1.9.1. Which personal data are being processed;

1.9.2. The purpose of data processing;

1.9.3. The legal grounds for data processing;

1.9.4. The ways in which the data were collected;

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

1.9.6. 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;

1.9.7. 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.

1.10. 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.

1.11. shall keep records of data processing activities;

1.12. 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.

1.13. In the event of accidental or unauthorized access to personal data, destruction, loss, alteration or disclosure of such data, 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, 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 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.

1.14. Should assist the bank in data protection impact assessments where applicable;

1.15. 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;

1.16. 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.- 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 organisation;

1.17. the processor shall immediately inform the bank if, in its opinion, an instruction infringes the Regulations on data protection or the obligations of other state;

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

1.19. In case of the approval of the transfer 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;

1.20. Shall not transfer personal data outside of Georgia. In the event if the activities of contractor requires the transfer of personal data outside of Georgia, it will immediately notify the bank about this via e-mail, at the e-mail address privacycommitee@tbcbank.com.ge, and wait for the bank's instructions regarding the mentioned. In any case, the transfer of the 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 the so-called White list countries.

1.21. may not transfer or authorize the transfer of 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;

1.22. 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;

1.23. In the case of involving sub-contractors in the process of personal data processing, 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;

1.24. In case of termination of the business activities by the Contractor and/or termination of the agreement by the bank, 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.

1.25. 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. 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;

1.26. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer 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;

2. 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;

3. 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;

4. 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;

5. The party processing the data is obliged to strictly observe the requirements of the Information System Infrastructure indicated below. The Party which temporarily or permanently processes the personal data provided by the Bank must be equipped with the following capability:

5.1. 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 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.

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

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

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

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

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

5.7. 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.

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

5.9. Access to the space shall require Two Step Authentication.

5.10. 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. Servel log data may be used for investigation of an accident or a bug.

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

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

5.13. 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.