TBC Bank JSC proposes the following amendments /additions to Standard Terms and Conditions of the E-Commerce Agreement (hereinafter referred to as "Standard Terms") in compliance with Paragraph 1.4 of Key Terms and Conditions of the E-Commerce Agreement, published on the Bank's website https://www.tbcbank.ge/web/ka/web/guest/card-payments

- **Annex #4 be added to Standard Terms to read as follows:**

"**Annex #4**

Personal Data Processing Policy

1.1. The Merchant represents and warrants that it will:

1.1.1. 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;

1.1.2. 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);

1.1.3. Limit an access to personal data to a narrow circle of users/administrators and only grant the authority to those who have a direct need to access the data and are aware of non-disclosure and security requirements related thereto;

1.1.4. In case of an accidental or unauthorized access to personal data, and destruction, loss, modification or disclosure thereof, inform the Bank immediately or not later than 2 (two) working days therefrom regarding the nature of the incident, indicating the data destroyed/lost/modified/disclosed;

1.1.5. Take immediate measures to ensure timely response to an incident and elimination of the causes, and inform the Bank about these measures;

1.1.6. 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;

1.1.7. Assign personal data processing to subcontractors only on special occasions and upon the Bank's written approval. These subcontractors shall be subject to requirements envisaged hereunder, without any limitations. Assignment of personal data processing to subcontractors does not relieve the Merchant of the obligations assumed or limit the Merchant's responsibilities in case of damages resulting from the breach of the obligations;

1.1.8. If it exercises the right set forth in Article 1.1.7 herein, 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 Merchant. Unless the disagreement is resolved through negotiations, the Bank is authorized to terminate the Agreement with the Party prematurely, without incurring any compensation liabilities;

1.1.9. If the Bank terminates the Agreement on the grounds set forth in Article 1.1.8 herein, return the Bank and destroy/delete permanently the personal data transferred to it as well as copies thereof within a reasonable period of time. The Bank is authorized to require confirmation of deletion from the Merchant. This provision shall not apply to information which the Party is obliged to maintain under the effective Law.

1.1.10. 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 Merchant's right to maintain access to personal data transferred to it under the Agreement after the completion of contractual relationship. The

Merchant 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;

1.2. 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 Merchant, as well as their compliance with technical and administrative specifics under safety requirements set forth herein;

1.3. 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;

1.4. 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;

1.5. The party processing the data is obliged to strictly observe the requirements of the Information System Infrastructure indicated in the annex to this Agreement.

Annex: Information System Infrastructure Requirements

The following measures shall be taken with respect to the space of a contracting party, where the personal data supplied by the Bank is temporarily or continuously found:

1. An isolated space must exist for the storage and the processing of the personal data, which will be separated by an independent Firewall.
2. Relevant authorized persons must control the access to the space Firewall.
3. The information stored in the isolated space must be accessed via the so called Jump Servers;
4. The integrity/accessibility of the space must be controlled and monitored;
5. Updates on the servers placed in the space must be monitored;
6. Personal data must be encrypted by using strong programming algorithms where possible;
7. Access to the isolated space must be ensured by using a protection method, via encrypted communication and safe protocol;
8. Password policy must exist for the isolated space to define the complexity, change period and history of passwords;
9. The admin user passwords for isolated space servers must be divided at least into two parts and stored with various owners, by using a safe method;
10. The so called two step authentication of users must be carried out for giving access to the space;
11. The isolated space must not be accessible via internet;
12. Logging must be carried out onto the isolated space servers; log must be kept in a centralized way and if necessary, it can be used in the process of incident or defect investigation;
13. Remote Storage (Cloud Service) must not be used for the storage, processing and the transfer of personal data;
14. When using personal data within the development or testing, the information must not be falsified in a way that it becomes impossible to directly or indirectly identify a person;
15. 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."