Bronto, Venda and Monexa Services Data Security Addendum

**Access Control to Processing Areas (Physical Controls)**

Data importer implements the following measures to prevent unauthorized persons from gaining access to the data processing equipment where the personal data is processed or used:

- **Physical Security Staffing:**
  - each data importer data center is staffed by onsite security personnel and monitored by a security organization responsible for continuous physical security functions;
  - procuring 24-hour security service at data centres;

- **Physical Security Access Procedures:**
  - establishing security areas
  - requiring all doors to be locked before and after entry;
  - restricting and protecting access paths;
  - securing the data processing equipment;
  - establishing access authorizations for staff and third parties, including the respective documentation;
  - restricting issuance of card-keys;
  - regulating card-keys once issued;
  - logging, monitoring and tracking all access to the data centre; and
  - securing the data centre with a security alarm system, and other appropriate security measures.

**Access and Input Control of Data Processing Systems, Including Specific Areas of the Data Processing Systems (Technological Controls)**

Data importer implements the following measures to prevent unauthorized persons from gaining access to the data processing systems, including specific areas of the data processing systems. Input and removal of personal data is also controlled by:

- **Industry Standard Data Handling:**
  - issuing and securing staff identification codes;
  - authenticating authorized personnel use at the individual level requiring authentication credentials such as user IDs that cannot be re-assigned to another person;
  - assigning individual terminals and/or terminal users and host identification characteristics exclusive to specific functions;
  - access control and privilege management, whereby data importer employs systems and processes to limit physical and logical access based on least privileges and segregation of duties to protect personal data from unlawful or unauthorized processing;
  - limiting staff access to only that personal data relevant to the scope of each individual’s role or responsibility. Personal data cannot be read, copied or modified or removed without authorization;
  - employing electronic access control systems in the data centres that are linked to a system alarm, in which unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate;
  - identifying and tracking terminal use at the user level;
  - encrypting database fields designated for credit card data information and social security numbers, encryption of such media consistent with standard industry practice, a documented retention period, applicable deletion procedures and reasonable physical and environmental controls. Please note: data at rest will not be encrypted.
Industry Standard Data Storage:
- using storage medium (or any equipment with storage capability) to be used to store personal data that will be secured and hardened in accordance with industry standard practices;
- maintaining a reasonable asset management policy to manage the life cycle (commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of such media;
- destroying decommissioned media containing personal data in accordance with NIST 800-88 Revision 1 at the Moderate level of sensitivity (or similar data destruction standard);
- logically segmenting personal data from data importer corporate data and other data importer customers’ data;
- regularly re-using and destroying tape back-up copies in a manner that renders the personal data unreadable; and
- employing backup processes and procedures for personal data, including storage of physical media in a secure location, encryption of such media consistent with standard industry practice, a documented retention period, applicable deletion procedures and reasonable physical and environmental controls.

Segregation of Personal Data (Technological Controls)
Data importer implements the following measures to process personal data gathered for unrelated purposes separately:
- segregating personal data through the use of application security measures and then assigning access to the appropriate users;
- separating personal data into modules within the data processing system. Each module is created for the specific purpose for which the personal data was gathered, i.e. by functionality and function; and
- storing personal data in different areas at the database level on a per module or function basis.

Transmission Control (Technological Controls)
Data importer implements the following measures to prevent unauthorized persons from reading, copying, altering or deleting personal data during personal data transmission:
- using firewall and encryption technologies to protect the gateways and pipelines through which personal data travels;
- logging, monitoring and tracking transmissions in a manner that is commercially reasonable;
- giving Customer control over the creation, deletion and suspension of user roles within the Applicable Services, including without limitation, allowing Customer to configure multi-factor authentication and IP address restriction, as documented in the User Guides for such Applicable Services;
- allowing Customer to apply its own password and authentication policies via the Applicable Services’ configurable policy settings and when using the single sign on functionality in the Applicable Services, as documented in the User Guides for such Applicable Services; and
- maintaining network connectivity security requirements that protect data importer’s infrastructure with multiple levels of secure network devices.

Availability Control (Process Controls)
Data importer implements the following measures to ensure that personal data is protected from accidental destruction or loss:
- implementing infrastructure redundancies to ensure data access is restored within seven days and backup performed at least weekly;
- storing back-ups off-site and ensuring they are readily available for restoration in case of failure of storage infrastructure for relational database server;
• employing Intrusion Detection Systems to look for known attacks against commonly installed software and implementing corrective action or remediating identified vulnerabilities and security concerns, if any, in a timeframe commensurate with the risk;
• recording any detected Security Incident, deploying data recovery procedures as needed, including, if possible, identification of the person who carried them out, and if applicable given the nature of the Security Incident, having a third party penetration test performed after corrective actions are implemented;
• performing a risk assessment of the Applicable Services every year, which will include an evaluation of risks to the confidentiality, integrity and availability of personal data which resides on the Applicable Services and a documented plan to correct or mitigate such risks in data importer’s security policies.

Roles, Responsibilities and Policy Controls
Data importer implements the following measures to ensure personal data is processed only in accordance with instructions provided by data exporter:
• binding policies and procedures for data importer’s employees and sub-processors. Policies clearly informing staff of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation;
• individual appointment of system administrators;
• maintaining a current list with system administrators’ identification details (e.g. name, surname, function or organizational area);
• correcting any inaccuracies, and deleting personal data as instructed;
• implementing compliance audits;
• maintaining applicable third-party certifications that include audit reporting that can be produced upon request of data exporter; and
• establishing processes for the destruction or return of personal data to data exporter at the expiration or termination of Customer’s Commercial Agreement.

Additional Safeguards
• **Data Importer Security Policy.** Data importer has, and will maintain, a security policy for its security organization that requires security training and privacy training as part of the training package for applicable security personnel, as documented in data importer’s applicable compliance audits and third-party certifications.

• **Data Importer Security Organization.** Data Importer has, and will continue to have, a dedicated security organization that is responsible for the ongoing maintenance of data importer’s security infrastructure, the review of Applicable Services, and for responding to Security Incidents.

• **Change Management.** Data importer maintains a change management policy to ensure changes to the organization, business processes, information processing facilities and systems that affect information security are controlled, as further described and audited in data importer’s applicable compliance audits and third-party certifications.

• **Server Operating Systems.** Data importer servers will use a hardened operating system implementation customized for the Applicable Services and data importer will maintain a risk-based prioritized patch management policy.

• **Redundancy.** Data importer’s disaster recovery plan is described in its applicable compliance audits and third-party certifications. Data importer’s data centres are designed with resiliency and redundancy with infrastructure systems designed to eliminate single points of failure. Personal data in the Applicable Services is continually replicated within the primary data centre. Additionally, data importer has in place a procedure for
recovering personal data and the Applicable Services to a secondary data centre in the event the primary data centre is declared by data importer to be inoperable due to a catastrophic disaster.

- **Power.** The data centre electrical power systems are designed to be fully redundant and maintained without interruption to continuous operations. Backup power is provided by various mechanisms, including, but not limited to, UPS batteries. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage and out-of-tolerance frequency conditions. Diesel engine generators are in place to provide power to critical equipment and customer loads.