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:

- establishing security areas;
- procuring 24-hour security service at data centres;
- 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:

- 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;
- 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;
- electronic recording of input entries.
- identifying and tracking terminal use at the user level;
- regularly re-using and destroying tape back-up copies in a manner that renders the personal data un-readable; and
- using industry standard encryption technologies. Please note: data at rest will not be encrypted.

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; and
- logging, monitoring and tracking transmissions in a manner that is commercially reasonable.
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; and
- recording any detected security incident and deploying data recovery procedures as needed, including, if possible, identification of the person who carried them out.

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 will clearly inform 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 Customer’s services agreement.