Technical and Organisational Measures

Confidentiality (Article 32(1) lit. (b) GDPR)

Physical Access Control

- No unauthorised access to data Processing facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems;

Electronic Access Control

- No unauthorised use of the data Processing and data storage systems, e.g.: passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media;

Internal Access Control (permissions for user rights of access to and amendment of Personal Data)

- No unauthorised reading, copying, changes or deletions of Personal Data within the system, e.g.: rights authorisation concept, need-based rights of access, logging of system access events; and

Isolation Control

- The isolated Processing of Personal Data, which is collected for differing purposes, e.g. multiple client support, sandboxing.

Integrity (Article 32(1) lit. (b) GDPR)

Data Transfer Control

- No unauthorised reading, copying, changes or deletions of Personal Data with electronic transfer or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature; and

Data Entry Control

- Verification, whether and by whom Personal Data is entered into a data Processing system, is changed or deleted, e.g.: logging, document management.

Availability and Resilience (Article 32(1) lit. (b) GDPR)

Availability Control

- Prevention of accidental or wilful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning.

Rapid Recovery

Procedures for regular testing, assessment and evaluation (Article 32(1) lit. (d) GDPR)

- Data Protection Management;
- Incident Response Management;

- Data Protection by Design and Default (Article 25(1) GDPR);
- Order or Contract Control; and
- No third-party data Processing as per Article 28 GDPR without corresponding instructions from WTG, e.g.: clear and unambiguous contractual arrangements, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.

Security measures

1. Data Importer/Processor has implemented and will maintain a security program in accordance with industry standards.
2. More specifically, Data Importer/Processor's security program will include:

Access Control of Processing Areas

Data Importer/Processor implements suitable measures to prevent unauthorised persons from gaining access to the data Processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data are Processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- Establishing access authorisations for employees and third parties, including the respective documentation;
- All access to the data centre where Personal Data are hosted is logged, monitored, and tracked; and
- The data centre where Personal Data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data Importer/Processor implements suitable measures to prevent their data Processing systems from being used by unauthorised persons, including:

- Use of appropriate encryption technologies;
- Identification of the terminal and/or the terminal user to the Data Importer/Processor and Processing systems;
- Automatic temporary lock-out of user terminal if left idle, identification and password required to reopen; and
- Automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts).

Access Control to Use Specific Areas of Data Processing Systems

Data Importer/Processor commits that the persons entitled to use their data Processing system are only able to access the Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied, modified or removed without authorization. This will be accomplished by various measures, including:

- Employee policies and training in respect of each employee's access rights to the Personal Data;
- Release of Personal Data only to authorised persons, including allocation of differentiated access rights and roles; and
- Use of encryption technologies where appropriate; and
- Control of files, controlled and documented destruction of Personal Data.

Availability Control

Data Importer/Processor implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss, including:

- Infrastructure redundancy; and
- Backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data Importer/Processor implements suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the Personal Data travels; and
- As far as practicable, all Personal Data transmissions are logged, monitored and tracked.

Input Control

Data Importer/Processor implements suitable input control measures, including:

- An authorisation policy for the input, reading, alteration and deletion of Personal Data;
- Authentication of the authorised personnel;
- Protective measures for the Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data;
- Utilisation of unique authentication credentials or codes (passwords);
- Providing that entries to data Processing facilities (the rooms housing the computer hardware and related equipment) are kept locked; and
- Automatic log-off of user sessions that have not been used for a substantial period of time.

Separation of Processing for different Purposes

Data Importer/Processor implements suitable measures to ensure that Personal Data collected for different purposes can be Processed separately, including:

- Access to Personal Data is separated through application security for the appropriate users; and
- Modules within the Data Importer/Processor's database separate which Personal Data is used for which purpose, i.e. by functionality and function.

Documentation

Data Importer/Processor's will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data Importer/Processor will take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Schedule 2.

Monitoring

Data Importer/Processor will implement suitable measures to monitor access restrictions to Data Importer/Processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- Individual appointment of system administrators; and
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Data Exporter upon request.