APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The following technical and organizational measures are performed on the processes taken by WorldAPP:

Physical access controls
Employed for preventing unauthorized persons from gaining access to Data Center processing systems within which Personal Data is processed or used.

- Electronic access card reading system
- Management of keys / documentation of key holders
- False entrances
- Vehicle blockades
- Customized parking lot designs
- Bulletproof glass/walls and unmarked buildings 24x7x365 staffed security guards
- Security service, front desk with required sign in for all visitors
- Burglar alarm system
- Internal and external infrared pan, tilt, zoom CCTV Monitored building management system
- Biometric scanners
- Portals and person-traps that authenticate only one person at a time
- Physical keys to locked cages containing the servers

Admission controls
Measures taken for preventing data processing systems from being used without authorization.

- Personal and individual user log-in when entering the system and / or the corporate network
- Administrative accounts passwords requirements:
    - must contain at least 8 characters
    - must contain a mix of alpha and numeric characters
    - must be changed every 90 days
    - the history of the last 3 passwords is kept to make sure that the new password does not repeat one of the previous 3 passwords.
    - user accounts will be suspended for 5 minutes after 5 unsuccessful log in attempts.

- Password procedures for standard users minimum of 8 characters, with a mix of alpha and numeric symbols.
- Application session times out after 40 minutes of inactivity
- Upon verification of the username and password, the application uses session-based token authentication.
- Remote access for maintenance requires IP-restricted remote access (SSH)
- Automated screen locks after a 10 minutes of inactivity
- Password protected screen savers

Virtual access controls
Measures taken to ensure that persons entitled to use a data processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of processing or use and after storage.

- User authentication is based on username and strong password
- All transactional records contain identifiers to distinguish Pilkington records
- System processing uses a rule-based mechanism to tailor data access to specific users and roles
- Data access, insert, and modification are logged
- ISO certifications are maintained at the datacenter

Transmission controls
Measures taken to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.

- All data are encrypted in flight using TLS
- Access to reports is logged
- Removable storage is not used

Input controls
Measures taken to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed.

- Application provides an option to restrict record entry to a defined set of roles
- Application provides an option to date/time stamp the entries and include identifiers for entering party
- Firewalls and intrusion prevention systems are in place to prevent unauthorized access

Assignment controls
Measures employed to ensure that, in the case of commissioned Processing of Personal Data, the data are processed strictly in accordance with the instructions of the principal.

- Confidentiality agreements are in place for all individuals with data access

- Training is conducted during onboarding and on a regular basis
- No third parties used for the processing of data other than as described in this Agreement
- Privacy policy describes rights and obligations of agent and principle

Availability controls
Measures taken to ensure that Personal Data are protected from accidental destruction or loss.

- Systems employ redundancies such as RAID arrays and redundant equipment
- Backups are stored in alternate equipment from primary processing
- Multiple air conditioning units are installed to provide redundant capacity in a N+1 configuration.
- Fire protection including "sniffer" systems, augmented by heat detection and dry-pipe sprinkler systems
- Multiple firewall layers and hardening on all servers
- UPS backed by N+1 generators
- Diverse fiber routing and multiple carriers

Separation controls
Measures taken to ensure that Personal Data collected for different purposes can be processed separately.

- Three-tier systems are used to physically separate presentation, business processing and storage
- Separation of duties is used internally to ensure functions pass through change control processes
- Discrete development, staging and production environments are maintained
- All routing of data for processing is controlled through automated rules engines
- Computing and storage is on equipment owned by Processor