DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is made between:

(1) **Customer**

and

(2) **IT-CO Hungary Kft.**
seat: 1024 Budapest, Fény utca 16., 2nd Floor
company registration number: 01-09-283374
as processor
("**IT-CO**")

This DPA forms part of the agreement between IT-CO and Customer for the licensing by IT-CO to Customer of IT-CO's proprietary package courier fleet management application generally described as "Packageez delivery software license" (the "**Agreement**").
The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

1. DEFINITIONS

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which Customer is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which Customer is subject to any other Data Protection Laws;

1.1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Agreement;

1.1.3 "**Contracted Processor**" means IT-CO or a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Restricted Transfer**" means:

1.1.8.1 a transfer of Customer Personal Data from Customer to a Contracted Processor; or

1.1.8.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 5.4.3 or 12 below;

1.1.9 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 4, amended as indicated (in square brackets and italics) in that Annex and under section 12.4; and

1.1.10 "**Subprocessor**" means any person (including any third party, but excluding an employee of IT-CO or any of its sub-contractors) appointed by or on behalf of IT-CO to Process Customer Personal Data on behalf of Customer in connection with the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word “include” shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 IT-CO shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the Customer’s documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case IT-CO shall to the extent permitted by Applicable Laws inform the relevant Customer of that legal requirement before the relevant Processing of that Customer Personal Data. The signing by Customer of the Order Form shall be considered a documented instruction.

2.2 Customer:

2.2.1 instructs IT-CO (and authorises IT-CO to instruct each Subprocessor) to:

2.2.1.1 Process Customer Personal Data; and

2.2.1.2 in particular, transfer Customer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1 on behalf Customer.

2.3 Annex 1 to this DPA sets out certain information regarding the Contracted Processors’ Processing of the Customer Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Customer may make reasonable amendments to Annex 1 by written notice to IT-CO from time to time as Customer reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this DPA.

3. IT-CO PERSONNEL

IT-CO shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual’s duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, IT-CO shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. The technical and organizational measures are described in Annex 2.

4.2 In assessing the appropriate level of security, IT-CO shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. SUBPROCESSING

5.1 Customer authorises IT-CO to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.

5.2 IT-CO may continue to use those Subprocessors already engaged by IT-CO as at the date of this DPA, subject to IT-CO in each case as soon as practicable meeting the obligations set out in section 5.4. A list of existing Subprocessors is set forth in Annex 3.

5.3 IT-CO shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within ten (10) Days of receipt of that notice, Customer notifies IT-CO in writing of any objections (on reasonable grounds) to the proposed appointment, IT-CO shall not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken.

5.4 With respect to each Subprocessor, IT-CO shall:

5.4.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) IT-CO, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including

terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA and meet the requirements of Article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) IT-CO, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with Customer; and

5.4.4 provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

5.5 IT-CO shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of IT-CO.

6. DATA SUBJECT RIGHTS

6.1 Taking into account the nature of the Processing, IT-CO shall assist Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 IT-CO shall:

6.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Contracted Processor is subject, in which case IT-CO shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. PERSONAL DATA BREACH

7.1 IT-CO shall notify Customer without undue delay upon IT-CO or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 IT-CO shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

IT-CO shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. DELETION OR RETURN OF CUSTOMER PERSONAL DATA

9.1 Subject to sections 9.2 and 9.3, IT-CO shall promptly and in any event within thirty (30) Days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Customer Personal Data.

9.2 Subject to section 9.3, Customer may in its absolute discretion by written notice to IT-CO within fifteen (15) Days of the Cessation Date require IT-CO to (a) return a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to IT-CO; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by any Contracted Processor. IT-CO shall comply with any such written request within sixty (60) Days of the Cessation Date.

9.3 Each Contracted Processor may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that IT-CO shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 IT-CO shall provide written certification to Customer that it has fully complied with this section 9 within ninety (90) Days of the Cessation Date.

10. AUDIT RIGHTS

10.1 Subject to sections 10.2 to 10.3, IT-CO shall make available to Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including

inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws (including, where applicable, Article 28(3)(h) of the GDPR).

10.3 Customer shall give IT-CO reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit has given notice to IT-CO that this is the case before attendance outside those hours begins; or

10.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

10.3.3.1 Customer reasonably considers necessary because of genuine concerns as to IT-CO's compliance with this DPA; or

10.3.3.2 Customer is required or requested to carry out by Data Protection Laws, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Customer has identified its concerns or the relevant requirement or request in its notice to IT-CO of the audit or inspection.

11. RESTRICTED TRANSFERS

11.1 Subject to section 11.3, Customer (as "**data exporter**") and each Contracted Processor, as appropriate, (as "**data importer**") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Customer to that Contracted Processor.

11.2 The Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

11.3 Section 11.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Laws.

11.4 IT-CO warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor, IT-CO's entry into the Standard Contractual Clauses under section 11.1, and agreement to variations to those Standard Contractual Clauses made under section 12.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.

12. GENERAL TERMS

Governing law and jurisdiction

12.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

12.1.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

12.2 Nothing in this DPA reduces IT-CO's obligations under the Agreement in relation to the protection of Customer Personal Data or permits IT-CO to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.3 Subject to section 12.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement

and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Changes in Data Protection Laws, etc.

12.4 Customer may:

12.4.1 by at least 30 (thirty) Days' written notice to IT-CO from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 11.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

12.4.2 propose any other variations to this DPA which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

12.5 If Customer gives notice under section 12.4.1:

12.5.1 IT-CO shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 5.4.3; and

12.5.2 Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by IT-CO to protect the Contracted Processors against additional risks associated with the variations made under section 12.4.1 and/or 12.5.1.

12.6 If Customer gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

12.7 Neither Customer nor IT-CO shall require the consent or approval of any Customer Affiliate or IT-CO Affiliate to amend this DPA pursuant to this section 13.5 or otherwise.

Severance

12.8 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEXES:

Annex 1: Description of Processing activities

Annex 2: Technical and organizational measures

Annex 3: List of existing Subcontractors

ANNEX 1
DESCRIPTION OF PROCESSING ACTIVITIES

Data exporter

The data exporter is the Customer who purchases IT-CO's Services that allows Authorized Users to enter, amend, use, delete or otherwise process Customer Personal Data in the Software.

Data importer

The data importer is IT-CO (and its Subprocessors) that provide the Services, including the following:

- correction of Software errors
- backup and restoration of Customer Data stored in the Software
- release and development of fixes and upgrades of the Software
- monitoring, troubleshooting and administering the underlying Services infrastructure and database
- security monitoring, network-based intrusion detection support, penetration testing

Data subjects

Employees, contractors, business partners, customers of Customer entered into and stored in the Services.

Data categories

[Provide list of Customer Personal Data submitted to / created in the Services.]

Special categories of data (if appropriate)

The importer does not process any special categories of data.

Processing operations

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Services
- provision of consulting services or other Custom Services specified in the Order Form
- communication Customer and with Authorized Users
- storage of Personal Data in data centers
- uploading any fixes or upgrades to the Service
- backing up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement

ANNEX 2
TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define IT-CO Hungary Ltd.'s current technical and organizational measures. IT-CO Hungary Ltd. may change these at any time without notice so long as it maintains a comparable or better level of security.

Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. Physical Access Control

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- In general, buildings are secured through access control systems (e.g., smart card access system).
- Guests and visitors to IT-CO Hungary Ltd. buildings must register their names at reception and must be accompanied by authorized IT-CO Hungary Ltd. personnel.
- IT-CO Hungary Ltd. employees and external personnel must wear their ID cards at all IT-CO Hungary Ltd. locations.

2. System Access Control

Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. The personnel access IT-CO Hungary Ltd.'s systems with a unique identifier (user ID).
- In case personnel leaves the company, their access rights are revoked.
- IT-CO Hungary Ltd. has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form.
- Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- IT-CO Hungary Ltd. uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Full remote access to IT-CO Hungary Ltd.'s corporate network and critical infrastructure is protected by strong authentication.

3. Data Access Control

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. IT-CO Hungary Ltd. uses authorization concepts that document grant processes and assigned roles per account (user ID).

4. Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from IT-CO Hungary Ltd.'s data processing systems.

Measures:

- IT-CO Hungary Ltd. only allows authorized personnel to access Personal Data as required in the course of their duty.
- IT-CO Hungary Ltd. has implemented a logging system for input, modification and deletion, or blocking of Personal Data by IT-CO Hungary Ltd. or its subprocessors within the Cloud Service to the extent technically possible.

5. Job Control

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- As part of the IT-CO Hungary Ltd. Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the IT-CO Hungary Ltd. Information Classification standard.
- All IT-CO Hungary Ltd. employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of IT-CO Hungary Ltd. customers and partners.

6. Availability Control

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- IT-CO Hungary Ltd. employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- IT-CO Hungary Ltd. has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services.

7. Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

- IT-CO Hungary Ltd. uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.

ANNEX 3
LIST OF EXISTING SUBPROCESSORS

Microsoft Inc.	Microsoft Azure web hosting
Moon42 Kft.	Mobile application developer
Rocket Science Group LLC	Mandrill email client provider
Twilio Inc.	SMS client provider
Google Inc.	Maps and other service provider

APPENDIX 1
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 organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. Physical Access Control

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- In general, buildings are secured through access control systems (e.g., smart card access system).
- Guests and visitors to data importer buildings must register their names at reception and must be accompanied by authorized data importer personnel.
- Data importer employees and external personnel must wear their ID cards at all data importer locations.

2. System Access Control

Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. The personnel access data importer's systems with a unique identifier (user ID).
- In case personnel leaves the company, their access rights are revoked.
- Data importer has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form.
- Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Data importer uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Full remote access to data importer's corporate network and critical infrastructure is protected by strong authentication.

3. Data Access Control

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Data importer uses authorization concepts that document grant processes and assigned roles per account (user ID).

4. Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from data importer's data processing systems.

Measures:

- Data importer only allows authorized personnel to access Personal Data as required in the course of their duty.
- Data importer has implemented a logging system for input, modification and deletion, or blocking of Personal Data by data importer or its subprocessors within the Cloud Service to the extent technically possible.

5. Job Control

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- As part of the data importer Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the data importer Information Classification standard.
- All data importer employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of data importer customers and partners.

6. Availability Control

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Data importer employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- Data importer has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services.

7. Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

- Data importer uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its controllers) has access only to its own data.