CONTROLLER-CONTROLLER DATA PROTECTION ADDENDUM

This DATA PROCESSING ADDENDUM (this "**Addendum**") shall apply to all agreements between **SCOOT PTE. LTD.** ("**Scoot**") and you (the "**Agent**" or "**Supplier**"), whether existing or future (each an "**Agreement**", and collectively referred to as the "**Agreements**"). This Addendum shall be deemed incorporated into and shall take effect from the effective date of each Agreement.

To the extent that any of the terms or conditions contained in this Addendum may contradict or conflict with any terms or conditions regarding the processing of personal data in any Agreements, it is expressly understood and agreed that the terms of this Addendum shall take precedence and supersede those other terms or conditions.

Scoot and the Agent shall hereafter be collectively known as the "**Parties**" and individually known as a "**Party**".

The Parties agree as follows:

1. Definitions

1.1 For the purposes of this Addendum, the following expressions bear the following meanings unless the context otherwise requires:

"**Business Day**" means any day other than a Saturday, Sunday or public holiday in Singapore;

"**California Personal Data**" means all personal information (as defined in the CCPA) of individual customers of each Party who reside in the State of California, or any personal information of each Party's employees/ Company Personnel employed and/or residing in the State of California;

"**China Personal Data**" means all personal information (as defined in the PIPL) of individual customers of each Party who reside in mainland China, or any personal information of each Party's employees/ Company Personnel employed and/or residing in mainland China;

"**Company Personnel**" means Scoot's employees, employee dependents and/or beneficiaries and job applicants;

"**Controller to Controller Clauses**" means (i) in respect of transfers of EU Personal Data, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 1 (Controller to Controller); and (ii) in respect of transfers of UK Personal Data, the standard contractual clauses issued by the Commissioner under s119A(1) Data Protection Act 2018, in each case as amended, updated or replaced from time to time;

"**Data Protection Laws**" shall include but not be limited to:

(a) in respect of EU Personal Data, any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other

binding instrument of the Party's member state, including Regulation 2016/679 (the "**GDPR**"), Regulation (EU) 2017/003 (the "**e-Privacy Regulation**"), and Directive 2002/58/EC (the "**e-Privacy Directive**");

(b) in respect of California Personal Data, the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq (the "**CCPA**");

(c) in respect of China Personal Data, the Personal Information Protection Law of the People's Republic of China and related laws and regulations (the "**PIPL**");

(d) in respect of Personal Data, means the Singapore Personal Data Protection Act 2012 (the "**PDPA**");

(e) in respect of UK Personal Data, the UK Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (together with the DPA, the "**UK GDPR**"), and the Privacy and Electronic Communications Regulations 2003, and any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time ("**UK Data Protection Laws**");

(f) in respect of Shared Personal Data, all of the above.

(in each case as amended, consolidated, re-enacted or replaced from time to time);

"**EU Personal Data**" means all personal data (as defined in the GDPR or any national legislation implementing the GDPR) of individual customers of each Party who are offered goods and services in the European Economic Area ("**EEA**"), and Switzerland (the "**GDPR Countries**") or whose behaviour is monitored in the GDPR Countries, or any personal data of each Party's employees/ Company Personnel employed and/or residing in the GDPR Countries;

"**Personal Data**" means data, whether true or not, about an individual who can be identified either from that data or from that data when combined with other information to which an entity has access or is likely to have access;

"**Process**", "**Processed**", "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Purpose**" has the meaning given in Clause 2.2;

"**Representatives**" means, as applicable in relation to a Party, its directors, officers, employees, agents, consultants, advisers, subcontractors or other representatives and the directors, officers, employees, agents, consultants, advisers, subcontractors or other representatives of each of the Parties;

"**Shared Personal Data**" means the EU Personal Data, California Personal Data, UK Personal Data, China Personal Data and/ or Personal Data each Party provides to, or receives from the other; and

"**Third Countries**" means:

(i) in relation to personal data transfers subject to the GDPR, all countries outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for personal data by the European Commission from time to time, which at the date of this Addendum include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay and the UK; and

(ii) in relation to personal data transfers subject to the UK GDPR, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for personal data by UK adequacy regulations issued under Section 17A DPA or Paragraphs 4 and 5 of Schedule 21 of the DPA from time to time, which at the date of this Addendum include all the countries listed in (i) and all EEA countries and Gibraltar; and

"**UK Personal Data**" means all personal data (as defined by UK Data Protection Laws) of individual customers of each Party who are offered goods and services in the UK or whose behaviour is monitored in the UK, or any personal data of each Party's employees/ Company Personnel employed and/or residing in the UK.

2. Purpose of Data Sharing

2.1 The Parties Process Shared Personal Data for the purpose of their agreement(s) for the Agent to act as a sales agent of Scoot. Each Party shall in respect of EU Personal Data and UK Personal Data act as a data controller, subject to the terms of this Addendum. Such data sharing does not constitute joint control of the Parties under the PIPL.

2.2 Each Party agrees to only Process the Shared Personal Data in accordance with this Addendum, for the Agent to act as an appointed sales agent of Scoot and to enable customers to book through your network and travel on Scoot operated services, more particularly described in Schedule 1 (Processing Details):

(a) To issue tickets on the Scoot's flights or issue electronic miscellaneous charges orders or other documents in connection with sales made on behalf of Scoot;

(b) To provide pre-flight and post-flight customer service to Scoot's customers as necessary and/or requested, including in relation to refunds inquiry, reservations and general information.

and the Parties shall not Process Shared Personal Data in a way that is incompatible with the Purposes described in this Addendum (the "**Purpose**"). In no event shall either Party Process any Shared Personal Data for the purpose of direct marketing to customers/ employees of the Party from which it received the relevant Shared Personal Data.

2.3 The Parties shall ensure Shared Personal Data comprises only data or information of customers/ employees that is necessary for the Purpose, including the customer's/ employee's full name, title, suffix, date of birth, passport number, nationality, country, gender, contact details (including home phone, mobile phone, business phone, fax, email, address and emergency contact information), frequent flyer information, flight information, payment (including credit card) information, PNR and Ticket number,

and all other information contained in the Passenger Name Record (PNR) when making a booking.

2.4 Each Party shall comply with all applicable Data Protection Laws to the extent relevant to its Processing of Shared Personal Data or its obligations under the Agreement(s) and this Addendum.

3. **Protection of Shared Personal Data**

3.1 Each Party shall, and shall procure that its Representatives shall:

3.1.1 in relation to the Shared Personal Data, obtain consent (where necessary) and/or provide notice to customers/ employees/ Company Personnel in accordance with Data Protection Laws to enable Shared Personal Data to be provided to, and used by, the other Party as contemplated by the Agreement(s);

3.1.2 Process the Shared Personal Data for no longer than is necessary to carry out the Purpose and in any event not longer than any statutory or professional retention periods applicable under any Data Protection Laws, and shall return or delete any Shared Personal Data once the Processing of the relevant Shared Personal Data is no longer necessary for the Purpose;

3.1.3 where Shared Personal Data that constitutes EU Personal Data is transferred by a Party to a location outside of the EEA, the transferor shall comply with the data exporter's obligations in the Controller to Controller Clauses which are deemed to be incorporated into and forms part of this Addendum (the "**EU SCCs**"), and the transferee shall comply with the data importer's obligations in the Controller to Controller Clauses;

(i) For the purposes of Annex I of such Controller to Controller Clauses, the parties and processing details set out in Schedule 1 (Processing Details) shall apply;

(ii) For the purposes of Annex II of such Controller to Controller Clauses, the technical and organizational security measures set out in Schedule 3 (Technical and Organization Security Measures) shall apply;

3.1.4 where Shared Personal Data that constitutes UK Personal Data is transferred by a Party to a location outside of the UK, the Parties shall comply with the terms set out in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (which incorporates the Standard Data Protection Clauses issued by the Information Commissioner's Office under section 119A(1) of the Data Protection Act 2018), as updated from time to time, which are deemed to be incorporated into and forms part of this Addendum (the "**UK SCCs**").

(i) For the purposes of Table 1 of the UK SCCs, the parties and processing details set out in Schedule 1 (Processing Details) shall apply;

(ii) For the purposes of Table 2 of the UK SCCs (Selected SCCs, Modules and Selected Clauses), the clauses as set out in the EU SCCs, as read together with the UK SCCs, shall apply;

(iii) in relation to the appropriate standards of Technical and Organizational measures (including technical and organizational measures to ensure the security of the data) applicable, Schedule 3 shall apply;

3.1.5 where Shared Personal Data that constitutes Personal Data is transferred outside Singapore, the transferor shall (i) obtain all necessary consents for such transfer; (ii) ensure that the recipients of such Personal Data is (are) under contractual obligations to protect such Personal Data to the same or higher standards as those imposed under this Addendum and the PDPA; and (iii) only transfer or Process such Personal Data outside Singapore in the manner described in Schedule 2 (Approved Processing Outside Singapore), and on the condition that the transferor shall notify the other Party in writing of any intended changes concerning arrangements to transfer or Process such Personal Data outside Singapore;

3.1.6 where Shared Personal Data that constitutes China Personal Data is transferred outside China, the transferor shall comply with the data exporter's obligations under Chapter 3 of the PIPL (*Rules of Cross-Border Provision of Personal Information*) and satisfy one of the following conditions:

(i) it has passed the privacy security assessment by the Cyberspace Administration of China (the "**CAC**");

(ii) it has obtained the required privacy certification from the specialized organization designated by the CAC;

(iii) it has entered into the standard contract with the recipient in the form formulated and published by the CAC; or

(iv) where applicable Chinese laws and regulations otherwise allows.

3.1.7 comply with its obligations pursuant to Chapter 3 of the GDPR (Rights of the data subject),and Chapter IV of the PIPL (Individuals' Rights in Personal Information Processing Activities), and Part V of the PDPA (Access to and Correction of Personal Data), and pertaining to consumer rights under the CCPA, and where requested by the other Party in relation to any Shared Personal Data, assist the other Party to comply with the same rights to the extent necessary, including:

(i) assisting the other Party with any subject access requests which it may receive from individuals to whom any Shared Personal Data relates; and

(ii) carrying out any reasonable request from the other Party to amend, restrict, or delete any Shared Personal Data;

3.1.8 notify the other Party promptly and in any event within 24 hours after it learns of any misappropriation or unauthorized access to, or disclosure or use of, the Shared Personal Data, and take necessary acts and measures to mitigate any harmful effect to the data subjects; and

3.1.9 implement and maintain adequate technical and organisational measures against unauthorised or unlawful Processing of, accidental loss or destruction of, or damage to, the Shared Personal Data, including without limitation to:

(i) maintain the security and confidentiality of the Shared Personal Data; and

(ii) protect against reasonably anticipated threats or hazards to the security or integrity of the Shared Personal Data.

3.2 A Party shall permit the other Party at any reasonable time upon five (5) Business Days' notice, to be given in writing, to have access to the appropriate part of the data recipient's premises, systems, equipment, and other materials and data Processing facilities to enable the other Party to inspect the same for the purposes of monitoring compliance with the data recipient's obligations under the Agreement(s) and this Addendum. Such inspection shall not relieve the data recipient of any of its obligations under the Agreement(s) and this Addendum.

3.3 The Parties agree to negotiate in good faith modifications to this Addendum if changes are required for a Party to continue to Process the Shared Personal Data in compliance with Data Protection Laws or to address the legal interpretation of Data Protection Laws, including (i) to comply with any amendments to the PDPA; (ii) to comply with the GDPR or the UK Data Protection Laws and any guidance on the interpretation of its provisions; (iii) if changes to the membership status of a country in the European Union or the EEA require such modification or (iv) to comply with the CCPA and any guidance on the interpretation of its provisions; or (v) to comply with the PIPL and any guidance on the interpretation of its provisions.

3.4 Both Parties acknowledge and agree that nothing in this Agreement(s) or the Addendum creates or shall be interpreted as a joint data controller relationship under the PIPL between the Parties.

3.5 If one Party Processes any Shared Personal Data in violation of the Data Protection Laws or in breach of the terms and conditions of this Agreement(s), the other Party shall be entitled to (i) require the defaulting Party to stop the violation or the breach immediately; and (ii) to take (by itself and/or requiring the defaulting Party to do so) effective remedial or corrective measures to mitigate the risks or damages.

SCHEDULE 1

PROCESSSING DETAILS

A. LIST OF PARTIES

Data importer / exporter – Data Controller: [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

- Name: Scoot Pte. Ltd. ("Scoot")
- Address: 65 Airport Boulevard, Changi Airport Terminal 3, #B1-17, Singapore 819663
- Contact person's name, position and contact details: Christian Stenkewitz, Data Protection Officer (EU) / General Manager Benelux, privacy@flyscoot.com
- Activities relevant to the data transferred under these Clauses: Collection, Storage, Use, Transmission, Erasure
- Role (controller/processor): Controller

Data exporter / importer – Data Controller: [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

- Name: For IATA agents, please refer to "IATA Trading Name" / For non-IATA agents, please refer to "Agency Name in English" (the "**Agent**")
- Address: For IATA agents, please refer to "Address 1" and "Address 2" / For non-IATA agents, please refer to "Address 1" and "Address 2"
- Contact person's name, position and contact details: Please refer to "Full Name", "Job Title" and "Email Address"
- Activities relevant to the data transferred under these Clauses: Collection, Storage, Use, Transmission, Erasure
- Role (controller/processor): Controller

B. PROCESSING DETAILS/ DESCRIPTION OF TRANSFER

Categories of Data subjects whose personal data is processed/transferred

The personal data transferred concern the following categories of data subjects (please specify):

Customers who purchase the Scoot's air tickets and other Scoot products through the Agent.

Categories of data processed/transferred

The personal data transferred concern the following categories of data (please specify):

- Full name,
- Title,
- Suffix,
- Date of birth,
- Passport number,
- Nationality,
- Country,
- Gender,
- Contact details (including home phone, mobile phone, business phone, fax, email, address and emergency contact information),
- Frequent flyer information,

- Flight information,
- Payment (including credit card) information,
- PNR or ticket number
- All other information contained in the Passenger Name Record (PNR) when making a booking

Special categories of data (if appropriate) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The personal data transferred concern the following special categories of data (please specify):

- Meal preferences which would tend to show the customer's religious beliefs.
- Special handling requests which would tend to show medical information.
- Photographs or other biometric information

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
The data will be transferred on a continuous and regular basis throughout the operation of the Agreement(s).

Nature of the processing
The personal data transferred will be subject to the following basic processing activities (please specify):

- Collection by the Agent from customers of Scoot
- Storage, organisation and structuring in the Agent's systems
- Retrieval, consultation, use and alteration by the Agent's personnel
- Transmission to Scoot's reservation system via one or more of the following methods: electronic transmission via API or GDS; direct key-in into Scoot Agency Hub and/or GroupsRM portal; verbally providing data by calling Scoot's call centre, for the creation, fulfilment and management of Scoot bookings, and for the performance of the Agent's services under the Parties' agreement(s) such as issuing tickets or other documents in connection with the sales of Scoot's flights, facilitating group bookings and providing pre-flight and post-flight customer service to Scoot's customers.
- Storage in Scoot's reservation live systems for 18 months, and in the archives of the reservation systems for 7 years. The database servers are located in Australia.

Purpose(s) of the data processing/ data transfer and further processing
Processing is necessary for the purpose of the Parties' agreement(s) for the Agent to act as an appointed sales agent of Scoot, more particularly:

- to issue tickets on Scoot's flights or electronic miscellaneous charges orders or other documents in connection with sales made on behalf of the Scoot; and

- to provide pre-flight and post-flight customer service to the customers, including in relation to refunds, inquiry, reservations and general information.

Duration of the processing / the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data will be retained for as long as necessary for the legitimate business or legal purposes of the respective data controllers.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

SCHEDULE 2

1.

APPROVED PROCESSING OUTSIDE SINGAPORE

Location	Processing Details	How Personal Data is protected to the standard of the PDPA or higher
For IATA agents, please refer to "Country/Region" / For non-IATA agents, please refer to "Country & Postal Code"	Please see Data Protection Terms, Clause 2 (Purpose of Data Sharing) and Schedule 1 Annex B	Data Protection Principles according to GDPR, as set out in the European Commission's Standard Contractual Clauses incorporated into and forms part of this Addendum.

SCHEDULE 3

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Notices

Any notices regarding the day-to-day obligations should be communicated in writing via email or other written notice to each of the Data Protection Officers (or their designees).

2. General Security Practices

Parties have implemented and shall maintain appropriate technical and organizational measures to protect personal data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this document for its personnel, equipment, and facilities at the Data Importer locations providing services to the Data Exporter ("Services").

The Services are set forth in one or more agreements between the Data Importer and the Data Exporter.

3. Technical and Organizational Security Measures

3.1. Organization of Information Security

(a) **Security Ownership.** The Data Importer has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

(b) **Security Roles and Responsibilities.** The Data Importer personnel with access to personal data are subject to confidentiality obligations.

(c) **Risk Management.** The Data Importer performed a risk assessment before processing the personal data or offering the Services.

3.2. Human Resources Security

(a) **General**. The Data Importer informs its personnel about relevant security procedures and their respective roles. The Data Importer also informs its personnel of possible consequences of breaching its security policies and procedures. Employees who violate security policies may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker or contractor may result in the termination of his or her contract or assignment with the Data Importer.

(b) **Training.** The Data Importer personnel with access to personal data receive:

i. annual security awareness and training regarding privacy and security procedures for the Services to aid in the prevention of unauthorized use (or inadvertent disclosure) of personal data;

ii. training regarding effectively responding to security events; and

iii. training is regularly reinforced through refresher training courses, emails, posters, notice boards and other training materials.

(c) **Background Checks.** The Data Importer personnel are subject to criminal background checks.

3.3. Asset Management

(a) **Asset Inventory.** Assets associated with information and information-processing facilities are identified and an inventory of assets is maintained.

(b) **Information Classification.** The Data Importer classifies personal data to help identify it and to allow for access to it to be appropriately restricted.

(c) **Media Handling**

Importer personnel:

i. Use trusted devices/corporate laptops/servers with encrypted storage that are configured with anti-malware software. All software including operating system and the anti-malware software on the machines should be updated and patched frequently.

ii. Protect/Encrypt personal data stored on a mobile device and external media, including laptops, smartphones, USB drives and DVDs; and

iii. Take measures to prevent accidental exposure of personal data, e.g. using privacy filters on laptops when in areas where over-the-shoulder viewing of personal data is possible.

(d) **Data Disposal.** The Data Importer shall have a documented data disposal strategy that includes identification/detection and secured data removal/disposal of sensitive data in physical/electronic media. This includes degaussing of tapes/hard drives/electronic media.

3.4. Personnel Access Controls

(a) **Access Policy.** An access control policy is established, documented, and reviewed based on business and information security requirements.

(b) **Access Recordkeeping.** The Data Importer maintains a record of security privileges of its personnel that have access to personal data, networks and network services.

(c) **Access Authorization.**

i. The Data Importer must have data access policies which implements the following:
   a. Principle of least privilege access
   b. Regular reviews of personnel needing access to data
   c. Regular reviews of the rights of personnel to grant such access
   d. Traceability of every login to a single person.
   e. Lock-outs of accounts due to failed login attempts
   f. Locking access of unattended laptops/devices after a short predefined time (example 15 minutes)
   g. Secure password/credential storage
   h. Review and Detection of unauthorised access to data where data includes personal data, credentials storage, logs and audit trails.
   i. Logs of access to data and regular reviews of this access.

ii. The Data Importer must have password policies that follow industry best practices (example NIST) with password length/complexity requirements

3.5. Cryptography

(a) **Cryptographic controls policy**
   i. The Data Importer must have a policy on the use of cryptographic controls based on assessed risks.
   ii. The Data Importer must ensure that the cryptographic standards used adhere to industry standards adopted by US government/military or driven by internet leaders, e.g. Google and Amazon.

(b) **Key management**. The Data Importer must have measures for managing keys and detecting any compromise/unauthorised access in its key system.

3.6. Physical and Environmental Security

(a) **Physical Access to Facilities**
   i. The Data Importer limits access to facilities where systems that process personal data are located to authorized individuals.
   ii. Access is controlled through key card and/or appropriate sign-in procedures for facilities with systems processing personal data. Personnel must be registered and are required to carry appropriate identification badges.
   iii. A security alarm system or other appropriate security measures shall be in place to provide alerts of security intrusions after normal working hours.

(b) **Physical Access to Equipment.** The Data Importer equipment that is located off premises is protected using industry standard process to limit access to authorized individuals.

(c) **Protection from Disruptions.** The Data Importer uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

(d) **Clear Desk.** The Data Importer has policies requiring a “clean desk/clear screen” at the end of the workday.

3.7. Operations Security

(a) **Operational Policy.** The Data Importer must maintain policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to personal data and to its systems and networks.

(b) The Data Importer continues to update its operational processes, procedures and/or practices in a timely manner to ensure that they are effective against the latest threats discovered.

(c) **Mobile Devices.** Mobile devices should have access control measures and remote wipe capability turned on. Procedures should be in place to report and wipe data off lost mobile devices immediately after detection of loss.

(d) Backup recovery media, where possible, shall be kept in an encrypted format.

3.8. Communications Security and Data Transfer

(a) The Data Importer has network policies which implements the following:
   i. Segregation and Filtering of Traffic between Internet and Corporate Zones and between the different Corporate Zones
   ii. Intrusion Detection Capability
   iii. Access Control and Password Policies on Network Devices

iv. Regular Network vulnerability/Penetration tests conducted by an independent third party at least annually.

3.9. System Acquisition, Development and Maintenance

(a) **Security Requirements**. The Data Importer must adopt security requirements for the purchase or development of information systems, including for application services delivered through public networks.

(b) **Development Requirements**. The Data Importer has policies for secure development, system engineering and support. The Data Importer conducts appropriate tests for system/application security as part of acceptance testing processes.

3.10. Supplier Relationships

(a) **Policies.** The Data Importer has information security policies or procedures for its use of suppliers. The Data Importer has agreements with suppliers in which they agree to comply with Data Exporter's and/or the Data Importer's security requirements.

(b) **Management.** The Data Importer performs periodic audits on key suppliers and manages service delivery by its suppliers and reviews security against the agreements with suppliers.

3.11. Information Security Incident Management

(a) **Response Process.** The Data Importer maintains a record of information security breaches with a description of the breach, the consequences of the breach, the name of the reporter and to whom the breach was reported, and the procedure for recovering data. Further, the Data Importer should have robust incident handling and response processes that includes the containment of threat, investigation, recovery and restoration of services.

(b) **Reporting.** The Data Importer will report within 48 hours to a designated response center any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

3.12. Information Security Aspects of Business Continuity Management

(a) **Planning.** The Data Importer maintains emergency and contingency plans for the facilities in which the Data Importer information systems that process personal data are located.

(b) **Data Recovery.** The Data Importer's redundant storage and its procedures for recovering data are designed to attempt to reconstruct personal in its original state from before the time it was lost or destroyed.

3.13. Audit and Assessment

(a) The Data Exporter reserves the right to perform an onsite audit for the purpose of completing our due diligence in security matters.