DATA PROCESSING AGREEMENT ADDENDUM FOR SHOPFACTORY AND SANTU USERS

This Data Processing Agreement Addendum ("Addendum") applies to subscribers of services supplied via Santu, ShopFactory and GlobeCharge websites, including ShopFactory Cloud (“Services”), made and entered into by and between Santu Pty. Ltd. (SANTU) and the Subscriber specified in the table below ("Subscriber").

On behalf of:	**SANTU Pty. Ltd**	Subscriber Name:	W.C.J. van der Holst
Signed by:		Signed by:	W van der Holst
Name:	Steffan Klein	Title:	CEO
Title:	CEO	Business Name:	Outdoor & Travel Outfitters b.v. Full legal name used to perform business required
Date:	April 6, 2018	SANTU User Name:	VJ-9087-NX
Address:	5 Hampshire Rd Glen Waverley, Victoria Australia 3150	Date:	16 May 2018
		Address:	Rucphensebaan 24A 4706 PJ Roosendaal The Netherlands

This Addendum includes the Data Processing Terms and the attached Annexes 1-2 and supplements the SANTU terms and conditions, available at http://santu.com/en/terms, (as updated from time to time) between Subscriber and SANTU, or other agreement between Subscriber and SANTU governing Subscriber's use of the Service Offerings (the "Agreement**").** This Addendum will be effective as of the day SANTU receives a complete and executed Addendum from Subscriber in accordance with the instructions under paragraphs A. and B. below (the "Addendum Effective Date").

A. **Instructions.** This Addendum has been pre-signed on behalf of SANTU. To enter into this Addendum, Subscriber must:

a. complete the table above by signing, dating and providing the full name of the Subscriber, full legal entity name used to perform the business, account user name, address and signatory information and

b. deliver the completed and signed Addendum to SANTU as attachment via email to gdpr@santu.com.

B. **Effectiveness.**

a. This Addendum will be effective only if it is executed and submitted to SANTU in accordance with paragraph A. above and this paragraph B., and only if all items in the table are completed accurately and in full. If Subscriber makes any deletions or other revisions to this Addendum, then this Addendum will be null and void. This Addendum will only apply to Subscriber's (or its employees’ or subcontractors’) use of the SANTU account that includes the Subscriber's full legal entity name (matching the one provided in the table above) and only to the account accessed with the User Name listed above and only while the account is paid in full.

b. Subscriber signatory represents to SANTU that he or she has the legal authority to bind Subscriber and is lawfully able to enter into contracts (e.g., is not a minor).

c. This Addendum will terminate automatically upon termination of the Services subscription, or as earlier terminated pursuant to the terms of this Addendum.

C. Purpose.

In this Data Processing agreement SANTU is the Data Processor and you, as the Subscriber to SANTU services, are the Data Controller.

WHEREAS

(A) The Data Controller wishes to subcontract certain Services (as defined in Appendix 1), which imply the processing of Data, to the Data Processor.

(B) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement (including the recitals hereto) shall have the following meaning:

1.1.1. “Agreement” means this Data Processing Agreement and all Schedules, if any.

1.1.2. “Data Processor” or “Processor” or “SANTU” means us

1.1.3. “Data Controller” or “Controller” or “Subscriber” means you as subscriber to Services.

1.1.4. “GDPR” means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and any replacement directive or regulation imposing equivalent obligations.

1.1.5. “Data” means basic personal data as defined in the GDPR of the Subscriber as well as basic personal Data of Customers of the Controller, including name, address and contact details.

1.1.6. “Customer” means a person buying physical or digital goods or services from a Subscriber.

1.1.7. “Software Interfaces” means the interfaces provided as part of the Services to enable the Data Controller to interact with and to control and instruct our software.

1.1.8. “Third Party Processor” means a Processor separately contracted by the Data Controller for Services.

1.1.9. “Account” means a fully paid SANTU account.

1.1.10. "SANTU Network" means the data centre facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are used by SANTU to provide the Services.

1.1.11. “Processing" has the meaning given to it in the Directive and "process", "processes" and "processed" will be interpreted accordingly.

2. OBJECT OF THIS AGREEMENT

2.1. **Scope and Roles.** This Addendum applies when Data is processed by SANTU on behalf of the Subscriber.

2.2. **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including all statutory requirements relating to data protection.

2.3. **Instructions for Data Processing.** SANTU will process Data in accordance with Subscriber's instructions. The parties agree that this Addendum is Subscriber's complete and final instructions to SANTU in relation to processing of Data. Processing outside the scope of this Addendum (if any) will require prior written agreement between SANTU and Subscriber on additional instructions for processing, including agreement on any additional fees Subscriber will pay to SANTU for carrying out such instructions. Subscriber may terminate this Addendum if SANTU declines to follow instructions requested by Subscriber that are outside the scope of this Addendum.

2.4. **Access or Use.** SANTU will not access or use Data, except as necessary to perform the Services initiated by Subscriber.

2.5. **Disclosure.** SANTU will not disclose Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends SANTU a demand for Data, SANTU will attempt to redirect the law enforcement agency to request that data directly from Subscriber. As part of this effort, SANTU may provide Subscriber's basic contact information to the law enforcement agency. If compelled to disclose Data to a law enforcement agency, then SANTU will give Subscriber reasonable Notice of the demand to allow Subscriber to seek a protective order or other appropriate remedy unless SANTU is legally prohibited from doing so.

2.6. **SANTU Personnel.** SANTU restricts its personnel from processing Data without authorization by SANTU. SANTU will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

2.7. **Subscriber Controls.** The Service Offerings provide Subscriber with controls to enable Subscriber to process Data through the use of our Software Interfaces. Subscriber is responsible for properly (a) using the Services, (b) using the Software Interfaces controls available in connection with the Services (including the security controls), and (c) taking such steps as Subscriber considers adequate to maintain appropriate security, protection, deletion and backup of Data, which may include use of encryption technology to protect Data from unauthorized access and routine archiving of Data.

2.8. **Data Transfer**. Data will be processed within the SANTU Network, located in the European Union. SANTU will not transfer Data across borders unless instructed by the Data Controller or as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order) as described in Section 2.5. In all cases, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of Data and ensure compliance with the GDPR.

3. DATA PROTECTION

3.1 The Data Controller and the Data Processor shall comply with the GDPR.

3.2 The Processor shall process all Data lawfully, fairly and in a transparent manner in relation to the data subject.

4. DATA PROCESSING

4.1 The Data processor shall

4.1.1 not process the Data for any purpose other than to deliver the Services and to perform its obligations under the Agreement in accordance with the documented instructions of the Data Controller; if it cannot provide such compliance, for whatever reasons, it agrees to promptly inform the Data Controller of its inability to comply;

4.1.2 inform the Data Controller immediately if it believes that any instruction from the Data Controller infringes applicable data protection legislation and regulations;

4.1.3 not disclose the Data to any person other than to its personnel as necessary to perform its obligations under the Agreement and ensure that such personnel is subject to statutory or contractual confidentiality obligations;

4.1.4 take appropriate technical and organisational measures against any unauthorised or unlawful processing, and to evaluate at regular intervals the adequacy of such security measures, amending these measures where necessary; these security measures are described in Article 7 of this agreement.

4.1.5 ensure that processing of Data shall take place only in accordance with the need-to-know principle, i.e. information shall be provided only to those persons who require the personal data for their work in relation to the performance of the Services;

4.1.6 promptly notify the Data Controller about (i) any legally binding request for disclosure of the personal data by a data subject, a judicial or regulatory authority unless otherwise prohibited, such as the obligation under criminal law to preserve the confidentiality of a judicial enquiry, and to assist the Data Controller therewith (ii) any accidental or unauthorized access, and more in general, any unlawful processing and to assist the Data Controller therewith;

4.1.7 deal with all reasonable inquiries from the Data Controller relating to its processing of the Data or in connection with the Agreement within a reasonable timeframe;

4.1.8 make available to the Data Controller all information necessary to demonstrate compliance with the applicable data protection legislation and regulations within a reasonable timeframe;

4.1.9 refrain from engaging another data processors without either written consent of the Data Controller or specific consent given by the Data Controller via actions taken in our Software Interfaces.

4. 1.10 assist the Data Controller, subject to reasonable additional compensation, with the Data Controller's obligation under the GDPR.

4. 1.11 take all reasonable measures to assist the Data Controller to respond to request by data subjects, such as the provision of Software Interfaces to delete and modify Data when requested by Customers or to make the Data stored available to a Customer on request.

4.1.12 promptly notify the Data Controller by email of any unlawful access to Data stored on the Santu Network which results in loss, disclosure, or alteration of Data and to cooperate with the Controller as required to take reasonable steps to mitigate the effects and to minimize any damage resulting from the unlawful access. It is Data Controller’s sole responsibility to maintain accurate contact information via the SANTU or ShopFactory Cloud account settings at all times and to ensure deliverability of emails from SANTU.

4.1.12 ensure security of data during a transfer to a third Party Processor engaged by the Data Controller.

4.2. The Data Controller must not collect personal details from Customers which fall into Special Categories as referred to in Article 9 GDPR. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person’s sex life or sexual orientation.

4.3. The Data Controller acknowledges that SANTU's obligation to report unlawful access to Data is not and will not be construed as an acknowledgement by SANTU of any fault or liability of SANTU with respect to the unlawful access.

5. SERVICE DESCRIPTION

We provide Data processing services as described in Appendix 1 for Data Controllers who receive online orders through online eCommerce facilities.

6. DATA PROCESSING

6.1. We provide the Data Processing services listed in Appendix 1.

The categories of Data involved are personal data such as name, address and contact details. Special categories of data as referred to in Article 9 GDPR are excluded.

The data subjects are the Subscriber and the customers of the Subscriber who interact with the Customer via the Services.

Customer Data processing ends when the Subscriber terminates the Subscription. Subscriber Data will be retained for 8 years to comply with government regulations.

7. SUB-CONTRACTING

The Controller authorizes the use of all current and future sub-contractors by the Processor for the provision, securing and management of the SANTU Network as well as to provide support services to help the Controller manage und utilize the services provided by SANTU. Where SANTU uses or authorises any subcontractor, SANTU will:

> 7.1 restrict the subcontractor's access to Data only to what is necessary to maintain the Service Offerings or to provide the Service Offerings to Subscriber and any End Users in accordance with the Documentation and SANTU will prohibit the subcontractor from accessing Data for any other purpose;
>
> 7.2 impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this Addendum, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights.

7.3 remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the subcontractor that cause SANTU to breach any of SANTU's obligations under this Addendum.

7.4 inform the Controller before making any changes to its sub-contractor arrangements.

8. Audit of technical and organisational Measures

SANTU relies on external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which SANTU provides the Services. Organisational and technical security measures applied to Data and storage and processing systems by SANTU meet PCI DSS v3.2 standards, which exceed GDPR security specifications. The compliance with PCI standards is established by independent auditors and result in a PCI compliance report generated quarterly. The Controller agrees to accept a copy of the latest PCI report for auditing and inspecting as the reasonable and only response required by the Processor to comply with GDPR article 28 (j) and to treat the report as confidential material.

9. Nondisclosure

Subscriber agrees that the details of this Addendum are not publicly known and Subscriber will not disclose the contents of this Addendum to any third party except as required by law or to perform a legal review.

10. Entire Agreement; Conflict.

Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

Appendix 1 Description of services

The primary objective of Services is to process and secure Data on behalf of the Subscriber, so that the Subscriber can enter into contracts with customers to accept and process orders and to market products and services to Customers.

Data processing includes the performance of the following tasks:

- collecting
- delivering
- computing
- storing
- displaying
- manipulating
- editing
- exporting
- transferring
- searching
- analysing
- deleting

Appendix 2

1) **Description of Security measures.**

   The Data Processor has implemented the necessary technical and organizational measures to protect Data in compliance with the GDPR.

   All data processing is performed by the Data Processor under its own control on secure and GDPR compliant servers subcontracted from Amazon Web Services, Inc. (AWS) in Europe.

2) **Physical Security**
   a) Physical Access Controls. Physical components of the SANTU Network are housed in nondescript AWS facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
   b) Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.
   c) Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

3) **Digital Security**
   a) Firewalls control the transmission of data between our trusted internal networks and untrusted external networks, as well as traffic between sensitive areas of the internal networks themselves to protect against unauthorized access.
   b) The storage of Data is kept to a minimum and appropriate data retention and disposal policies, procedures and processes are in place. Without access to the proper cryptographic keys, encrypted data will be unreadable and unusable by hackers even if they manage to circumvent other security controls. Cryptographic keys are stored securely and access to them is restricted to the fewest custodians necessary.
   c) Strong cryptography and security protocols such as TLS, IPSEC and SSH are used to safeguard Data during transmission over open, public networks.

d) Regular scanning and updating of our systems ensures protection against emerging threats against all types of malware.
e) Security patches by vendors or providers of software used to offer our services are implemented regularly to protect our servers against any vulnerabilities
f) Server management access is limited by password control and IP addresses. Only trusted staff on a “Need to know” basis has access and only from dedicated IP numbers to our servers for management purposes. “Need to know” means access rights are granted to the smallest amount of Data and privileges required to perform a job.