A&K DATA PROCESSING ADDENDUM

Last Updated: September 10, 2024

This Abercrombie & Kent ("A&K") Data Processing Addendum, including its exhibits and appendices (the "**Addendum**"), applies to any and all Personal Data that Supplier accesses, receives, processes, and/or obtains from or on behalf of A&K in connection with the Agreement to the extent the Agreement incorporates by reference this Addendum or otherwise positions Supplier as a service provider or processor under Applicable Data Protection Laws.

1. Definitions

1.1. For the purpose of interpreting this Addendum, the following terms (and their applicable cognates) shall have the meanings set out below:

(a) "**A&K**" refers to Abercrombie & Kent and means the A&K entities contracting in the Agreement.

(b) "**A&K Personal Data**" means any Personal Data Processed by or on behalf of Service Provider to provide the Services in accordance with the Agreement.

(c) "**Affiliate**" means any entity within a controlled group of companies that directly or indirectly, through one or more intermediaries, is controlling, controlled by, or under common control with one of the Parties.

(d) "**Agreement**" means any agreement entered into between A&K and Supplier for the provision of the Services.

(e) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of A&K Personal Data, including but not limited to the laws and regulations identified in **Exhibit B** hereto as may be amended, modified, or supplemented from time to time, as applicable.

(f) "**Contracted Processor**" means any third party appointed by or on behalf of Service Provider to Process A&K Personal Data in connection with the Services.

(g) "**Data Exporter**" and "**Data Importer**" shall have the same meanings assigned to them in Part A of **Exhibit A**.

(h) "**GDPR**" means the EU GDPR and UK GDPR, as those terms are defined in **Exhibit B**, as applicable.

(i) "**Jurisdiction Specific Terms**" means all terms applicable to the Processing of A&K Personal Data that apply to the extent that Service Provider Processes A&K Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified in these terms. The Jurisdiction Specific Terms are included as **Exhibit B** to this Addendum.

(j) "**Parties**" means both A&K and Supplier.

(k) "**Party**" means either A&K or Supplier.

(l) "**Restricted Transfer**" means any transfer of A&K Personal Data protected by Applicable Data Protection Laws to a Third Country or an international organization in a Third Country (including data storage on foreign servers).

(m) "**Service Provider**" means Supplier.

(n) "**Services**" means the services and other activities carried out by or on behalf of Service Provider for A&K pursuant to the Agreement.

(o) "**Standard Contractual Clauses**" are the model clauses for Restricted Transfers adopted from time to time by the relevant authorities of the jurisdictions indicated in **Exhibit B**, insofar as their use is approved by the relevant authorities as an appropriate mechanism or safeguard for Restricted Transfers.

(p) "**Sub-Processor**" means a direct Processor of a Processor. For the avoidance of doubt, Contracted Processors are Sub-Processors.

(q) "**Supplier**" has the same meaning as given in the Agreement. If "Supplier" is not defined in the Agreement, then it means the Party contracting with A&K.

1.2. The terms "**Controller**", "**Data Protection Impact Assessment**", "**Data Subject**", "**Processor**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Personal Information**", "**Processing**", "**Supervisory Authority**", and "**Third Country**" shall have the same meanings as in the Applicable Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

1.3. Capitalized terms which are used but not defined herein shall have the meanings given to them in the Agreement. Except as modified or supplemented above, the definitions of the Agreement shall remain in full force and effect.

2. Duration and Scope

2.1. Duration. This Addendum shall continue concurrently for the duration that A&K Personal Data is Processed by Service Provider pursuant to the Agreement.

2.2. Scope. This Addendum will apply to the Processing of all A&K Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor. Processing of data by the Service Provider which does not constitute Personal Data or A&K Personal Data is outside the scope of this Addendum.

2.3. Exhibits and Appendices. This Addendum includes the following exhibits and appendices:

(a) Exhibit A – Details of Processing;

(b) Appendix I to Exhibit A – Technical and Organizational Security Measures;

(c) Exhibit B – Jurisdiction Specific Terms; and

(d) Exhibit C – Supplemental Clauses to the Standard Contractual Clauses.

3. Processing of A&K Personal Data

3.1. A&K acts as a Controller and Service Provider acts as a Processor.

3.2. Service Provider shall:

(a) comply with all Applicable Data Protection Laws in the Processing of A&K Personal Data;

(b) not Process A&K Personal Data other than on A&K's relevant documented instructions (including with regard to Restricted Transfers), unless such Processing is required by Applicable Data Protection Laws to which the relevant Processing activity(ies) are subject, in which case Service Provider shall, to the extent permitted by Applicable Data Protection Laws, inform A&K of that legal requirement before the respective act of Processing of that A&K Personal Data; and

(c) immediately inform A&K in the event that, in Service Provider's reasonable opinion, a Processing instruction given by A&K may infringe Applicable Data Protection Laws.

3.3. All necessary information relating to the details of the Processing is set out in **Exhibit A**. A&K shall be entitled to update **Exhibit A** from time to time by posting an updated version online or sending an updated version to Service Provider. Service Provider will be considered to have accepted any such update unless it provides A&K with written notice of non-acceptance within fourteen (14) days following receipt. If Service Provider issues such notice of non-acceptance, the Parties will cooperate and negotiate in good faith regarding any required updates to **Exhibit A**.

3.4. A&K instructs Service Provider (and authorizes Service Provider to instruct each Contracted Processor it engages) to Process A&K Personal Data and, in particular, transfer A&K Personal Data to any country or territory (subject to the requirements of Applicable Data Protection Laws governing Restricted Transfers), only as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum.

4. Service Provider Personnel

Service Provider shall ensure:

4.1. the reliability of any of its employees, agents, or contractors who may have access to A&K Personal Data;

4.2. that access to A&K Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfil the documented Processing instructions given to Service Provider by A&K or to comply with Applicable Data Protection Laws; and

4.3. that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality, which shall continue to endure after the termination of the Services.

5. Security of Processing

5.1. Service Provider shall implement and maintain appropriate technical and organizational security measures, such as those identified in **Appendix I to Exhibit A**, which ensure a level of security appropriate to the risk of Processing and take into account: (i) the state of the art, costs of implementation, and the nature and purposes of Processing; (ii) the risk of varying likelihood and severity to the rights and freedoms of natural persons; and (iii) the risks presented by the Processing activities, particularly those risks related to Personal Data Breaches.

5.2. Service Provider shall also assist A&K with regard to ensuring A&K's compliance with its own obligations related to security measures.

6. Sub-Processing

6.1. Authorization for Existing Contracted Processors: A&K authorizes Service Provider to use Contracted Processors, provided the obligations of this Section 6 (and the respective obligations of **Exhibit B**) are met.

6.2. Authorization for the Appointment of Additional Contracted Processors: To appoint additional Contracted Processors, Service Provider must provide A&K with prior written notice which will include the details of the Processing to be undertaken by that respective Contracted Processor.

6.3. Objection to Contracted Processors.

(a) If A&K does not explicitly notify Service Provider in writing of any objections to the proposed appointment within fourteen (14) days of the receipt of such notice, A&K shall be deemed to have consented to the proposed appointment. A&K may object to the appointment of a Contracted Processor by providing a written objection, which shall include the name of the objected-to Contracted Processor and a reasonable statement of objection.

(b) If an objection is received, the Parties will, for a period of no more than thirty (30) days from the date of A&K's objection, work together in good faith to attempt to find a commercially reasonable solution for A&K that avoids the use of the objected-to Contracted Processor. If no solution can be found, A&K, upon written notice to Service Provider, may terminate the Agreement immediately (or upon such date as A&K selects), with no further fees due, other than what has been accrued up to and including the date of termination. Upon termination of the Agreement, Service Provider shall cease to Process A&K Personal Data.

6.4. Requirements for Appointing Contracted Processors. With respect to each Contracted Processor, Service Provider shall:

(a) before the Contracted Processor first Processes A&K Personal Data (or, where relevant, in accordance with Section 6.1), carry out adequate due diligence to ensure that the Contracted Processor is capable of providing the level of protection and security for A&K Personal Data required by this Addendum, the Agreement, and Applicable Data Protection Laws;

(b) upon request of A&K, disclose the results of that due diligence, with documentation sufficient to support Service Provider's findings;

(c) restrict the Contracted Processor's access to A&K Personal Data only to what is necessary to assist Service Provider in providing or maintaining the Services, and prohibit the Contracted Processor from accessing A&K Personal Data for any other purpose; and

(d) ensure that the arrangement between Service Provider and the prospective Contracted Processor is governed by a written contract that includes terms which offer at least the same level of protection for A&K Personal Data as those set out in this Addendum, and that such terms meet the requirements of Applicable Data Protection Laws.

6.5. Service Provider shall agree to a third-party beneficiary clause with all Contracted Processors whereby, in the event the Service Provider has factually disappeared, ceased to exist in law, or has become insolvent, A&K shall have the right to terminate the arrangement with the Contracted Processor and to instruct the Contracted Processor to erase or return the A&K Personal Data.

6.6. Where any Contracted Processor fails to fulfil its data protection obligations under such written contract (or in the absence thereof, as the case may be), Service Provider shall remain fully liable to A&K for the performance of the respective Contracted Processors' data protection obligations under such contract and/or Applicable Data Protection Laws.

7. Rights of the Data Subjects

7.1. Taking into account the nature of the Processing, Service Provider shall assist A&K by implementing appropriate technical and organizational measures, insofar as possible, to

respond to requests to exercise rights of the Data Subjects under Applicable Data Protection Laws.

7.2. With regard to the rights of the Data Subjects within the scope of this Section 7, Service Provider shall:

(a) promptly notify A&K if it or any Contracted Processor receives a request from a Data Subject under any Applicable Data Protection Laws with respect to A&K Personal Data;

(b) not respond to that request, except on the documented instructions of A&K or as required by Applicable Data Protection Laws, in which case Service Provider shall, to the extent permitted by Applicable Data Protection Laws, inform A&K of that legal requirement before it or the Contracted Processor responds to the request; and

(c) promptly comply with any documented instructions from A&K regarding responding to a request to exercise rights of a Data Subject.

8. Personal Data Breach

8.1. Service Provider will maintain a reasonable and appropriate Personal Data Breach response program.

8.2. Breach Response. If Service Provider discovers, is notified of, or has reason to suspect a Personal Data Breach affecting A&K Personal Data under its or any of its Contracted Processors' control, Service Provider will: (i) immediately implement measures to stop the unauthorized access; (ii) secure the A&K Personal Data; and (iii) notify A&K without undue delay and, in any event, within twenty-four (24) hours of becoming aware of such suspected Personal Data Breach.

8.3. Breach Obligations. Immediately upon providing notice of a Personal Data Breach, Service Provider shall:

(a) describe to A&K in as much detail as reasonably possible: (i) the nature of the Personal Data Breach; (ii) where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (iii) the impact of such Personal Data Breach upon A&K and the Data Subjects; (iv) the measures taken or proposed to be taken by Service Provider to address the Personal Data Breach; and (v) relevant individuals who will be available (24 hours per day, 7 days per week) until the Parties mutually agree that the Personal Data Breach has been resolved;

(b) provide and supplement notifications as and when information becomes available;

(c) assist A&K in meeting its respective obligations pursuant to Applicable Data Protection Laws, including any obligations to notify Supervisory Authorities or Data Subjects of a Personal Data Breach; and

(d) in cooperation with A&K, use its best efforts (at Service Provider's expense) to investigate, mitigate, and remediate each such Personal Data Breach and prevent a recurrence of such Personal Data Breach.

8.4. Where a Personal Data Breach arises due to the negligence or wilful misconduct of Service Provider, Service Provider will promptly reimburse A&K for all costs reasonably incurred by A&K in connection with the Personal Data Breach, including, but not limited to, costs related to A&K's provision of notice of a Personal Data Breach to Supervisory Authorities, A&K's customers, or affected Data Subjects and costs related to offering credit monitoring services to affected Data Subjects (if determined appropriate by A&K or required by Applicable Data Protection Laws).

8.5. Service Provider represents and warrants that it is not, and has never been, subject to civil or criminal litigation, government investigation, or a consent decree, judgment, or order regarding data protection, privacy, or information security, and that it has not suffered any material security breach or, if it has, that it has disclosed information regarding such security breach(es) to A&K.

9. Data Protection Impact Assessment and Prior Consultation

9.1. Service Provider shall provide A&K with relevant information and documentation, and assist A&K in complying with its obligations with regard to any Data Protection Impact Assessments or prior consultations with Supervisory Authorities when A&K determines that such Data Protection Impact Assessments or prior consultations are required pursuant to Applicable Data Protection Laws, but in each such case solely with regard to A&K Personal Data Processed by Service Provider, and taking into account the nature of the Processing and information available to the respective Contracted Processors.

10. Deletion or Return of Personal Data

10.1. Service Provider shall promptly, following the date of cessation of Services, at the choice of A&K, delete or return all A&K Personal Data (including copies) to A&K. Service Provider shall provide A&K with the technical means, consistent with the way the Services are provided, to request the return or deletion of A&K Personal Data. In the event that A&K has not specified its choice, Service Provider shall return all A&K Personal Data to A&K.

10.2. Service Provider shall also cause all Contracted Processors that have received any A&K Personal Data to delete or return, as applicable, all such A&K Personal Data without undue delay.

10.3. Sections 10.1 and 10.2 shall not apply to the extent that applicable law requires Service Provider or its Contracted Processor, as applicable, to retain any A&K Personal Data. In those instances, Service Provider or Contracted Processor, as applicable, shall specify the applicable law requiring such retention and the period it shall retain A&K Personal Data. The Service Provider's obligations under this Addendum shall continue for the full period the A&K Personal Data is retained.

10.4. Sections 10.1 and 10.2 do not apply to A&K Personal Data that has been archived on back-up systems, which Service Provider or its Contracted Processors, as applicable, shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

11. Audit Rights

11.1. A&K may request, and Service Provider will provide (subject to obligations of confidentiality), a current SOC 2 Type II audit report, ISO 27001 certificate, or other substantially similar independent third-party audit report issued to Service Provider, and any related documentation that A&K may request, to confirm Service Provider's compliance with the Applicable Data Protection Laws.

11.2. If A&K, after having reviewed such audit report(s) and related documentation, still requires additional information (for example, Service Provider's policies and procedures regarding data protection, information from Service Provider's Contracted Processors, or any other relevant information), Service Provider shall further assist and make available to A&K all such additional information and/or documentation (including relevant provisions of contracts with Contracted Processors) necessary to demonstrate compliance with this Addendum and/or Applicable Data Protection Laws.

11.3. In addition, Service Provider shall allow for and contribute to audits, including remote and onsite inspections of the Services, by A&K (on behalf of itself or its clients) or an auditor mandated by A&K (on behalf of itself or its clients) with regard to the Processing of the A&K Personal Data by the Contracted Processor.

12. Jurisdiction Specific Terms

12.1. To the extent Service Provider Processes A&K Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction(s) ("**Jurisdiction Specific Terms**") shall apply in addition to the terms of this Addendum.

12.2. A&K may update **Exhibit B** from time to time to reflect changes in or additions to Applicable Data Protection Laws to which relevant Processing operations are subject. A&K shall be entitled to update **Exhibit B** from time to time by posting an updated version online or sending an updated version to Service Provider. Service Provider will be considered to have accepted any such update unless it provides A&K with written notice of non-acceptance within fourteen (14) days following receipt. If Service Provider issues such notice of non-acceptance, the Parties will cooperate and negotiate in good faith regarding any required updates to **Exhibit B**.

12.3. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will prevail.

13. Restricted Transfers

13.1. Restricted Transfers of A&K Personal Data within the scope of this Addendum shall be conducted in accordance with the applicable terms and requirements set out in **Exhibit B** and Applicable Data Protection Laws.

13.2. If the relevant authorities adopt a new version of Standard Contractual Clauses as a lawful mechanism for Restricted Transfers in a jurisdiction governing the processing of A&K Personal Data, the Parties are deemed to have agreed to the execution of the new version of the Standard Contractual Clauses by agreeing to this Addendum, and, if necessary, A&K shall be entitled to update **Exhibit A** and **Exhibit B** (and their appendices) accordingly.

13.3. If an alternative transfer mechanism is adopted by A&K during the term of the Agreement (an "**Alternative Mechanism**"), and A&K notifies Service Provider that some or all Restricted Transfers can be conducted in compliance with Applicable Data Protection Laws pursuant to the Alternative Mechanism, the Parties will rely on the Alternative Mechanism instead of the transfer mechanisms in **Exhibit B** for Restricted Transfers to which the Alternative Mechanism applies.

14. Updates to Exhibits to this Addendum

14.1. A&K may update **Exhibit A** and **Exhibit B** (and their appendices) from time to time to reflect changes in or additions necessary to Applicable Data Protection Laws. Without limiting the generality of the foregoing, if the execution of a new version of the Standard Contractual Clauses adopted by the relevant authorities in the jurisdiction governing the processing of A&K Personal Data is later required in order for the Parties to rely on the Standard Contractual Clauses as a lawful transfer mechanism for Restricted Transfers, the Parties are deemed to have agreed to the new version of the Standard Contractual Clauses by agreeing to this Addendum, and, if necessary, A&K shall be entitled to update **Exhibit A** and **Exhibit B** (and their appendices) accordingly.

14.2. A&K may update **Exhibit C** from time to time to provide for additional safeguards to A&K Personal Data subject to the requirements of Applicable Data Protection Laws for

Restricted Transfers. A&K shall be entitled to update **Exhibit C** by posting an updated version online or sending an updated version to Service Provider. Service Provider will be considered to have accepted any such update unless it provides A&K with written notice of non-acceptance within fourteen (14) days following receipt. If Service Provider issues such notice of non-acceptance, the Parties will cooperate and negotiate in good faith regarding any required updates to **Exhibit C**.

15. Liability

15.1. The liability of each Party under this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement. In no event does this Addendum restrict or limit the rights of any Data Subject under the Applicable Data Protection Laws.

15.2. Service Provider shall be fully liable to A&K for any breach of the Agreement or this Addendum, and the obligations set out therein (including by means of additional contract, as the case may be), by any Contracted Processor, without prejudice to the liability of Service Provider in accordance with Applicable Data Protection Laws.

16. Indemnification

16.1. Service Provider agrees to indemnify, defend, and hold harmless A&K and its officers, directors, employees, agents, Affiliates, successors, and permitted assigns against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind which A&K may sustain as a consequence of any breach by Service Provider (or the Contracted Processors, as the case may be) of the provisions of this Addendum.

17. General Terms

17.1. Notice. Notices to A&K under this Addendum shall be directed to privacy@abercrombiekent.com. Service Provider shall provide the contact details for the purpose of receiving notices under this Addendum to privacy@abercrombiekent.com.

17.2. Prior Existing Agreement. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations, and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Service Provider and A&K in connection with the Agreement.

17.3. Conflicts. All clauses of the Agreement that are not explicitly amended or supplemented by the clauses of this Addendum remain in full force and effect and shall apply, as long as this does not contradict compulsory requirements of Applicable Data Protection Laws. In the event of any conflict between the Agreement (including any annexures, exhibits, and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail, except in such cases where the applicable Jurisdiction Specific Terms listed in **Exhibit B** will apply and take precedence.

17.4. Severability. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision, and the remainder of this Addendum will continue in effect.

17.5. Non-Compliance. If Service Provider determines that it can no longer meet any of its obligations in this Addendum, Applicable Data Protection Laws, or the Standard Contractual Clauses (where applicable), it shall: (i) promptly notify A&K of that

determination and (ii) cease the Processing or immediately take other reasonable and appropriate steps to remediate the lack of compliance.

17.6. Signature. If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant to A&K that you have the authority to bind that entity and its Affiliates, where applicable, to the terms and conditions of this Addendum.

17.7. Disclosure to Supervisory Authority. Service Provider acknowledges that A&K may disclose this Addendum and any relevant privacy provisions in the Agreement to Supervisory Authorities, or any other judicial or regulatory body upon their request.

17.8. This Addendum shall be governed by the laws specified in the Agreement.

17.9. Any disputes arising out of or in connection with this Addendum shall be subject to the exclusive jurisdiction of the courts specified in the Agreement.

Exhibit A

Details of Processing

A. LIST OF PARTIES:

A&K:

United Kingdom of Great Britain and Northern Ireland

Legal entity:	Abercrombie & Kent Ltd.
Company No:	01082430
Name:	Data Compliance Officer
Email address:	privacy@abercrombiekent.com
Postal address:	St George's House, Ambrose Street, Cheltenham, GL50 3LG.

Data Protection Officer

Legal entity:	VeraSafe, LLC
Telephone:	+1 (617) 398-7067
Email address:	experts@verasafe.com
Postal address:	100 M Street S.E., Suite 600, Washington, D.C. 20003, USA
Web:	https://www.verasafe.com/about-verasafe/contact-us/

European Union

Legal entity:	Abercrombie & Kent Italy and Croatia
Name:	EU Data Protection Representative
Email address:	datacompliance@abercrombiekent.co.uk
Postal address:	Via Fattori 10, Florence, 50132, Italy
Supervisory body:	Garante Per La Protezione Dei Personali
Website URL:	garanteprivacy.it

United States of America, Canada and South/Central America

Legal entity:	Abercrombie & Kent USA LLC
Name:	Data Protection Manager
Email address:	datacompliance@abercrombiekent.com
Postal address:	1411 Opus Place Executive Towers West II, Suite 300, Downers Grove, IL 60515.

Australia and Asia

Legal entity:	Abercrombie & Kent Australia Pty. Ltd.
Name:	Data Protection Manager
Email address:	datacompliance@abercrombiekent.com.au
Postal address:	North Tower, Level 26/80 Collins Street, Melbourne VIC 3000, Australia

Activities Relevant to Processing of A&K Data:	Processing activities relating to the Services, as set forth in the Agreement.
Controllership Role:	A&K serves as the Controller.
Data Transfer Role:	A&K may serve one or more roles, according to the purposes of the Personal Data being Processed: • A&K serves as the Data Exporter when sending (exporting) the Personal Data to Service Provider. • A&K serves as the Data Importer when receiving (importing) the Personal Data from Service Provider

Service Provider:

Contact information set forth in the Agreement.

Activities Relevant to Processing A&K Data:	Processing activities relevant to the Services as set forth in the Agreement.
Controllership Role:	Service Provider serves as the Processor.

Data Transfer Role:	Service Provider may serve one or more role, according to the purposes of the Personal Data being Processed: ● Service Provider serves as the Data Exporter when sending (exporting) the Personal Data to A&K. ● Service Provider serves as the Data Importer when receiving (importing) the Personal Data from A&K.

B. DESCRIPTION OF PROCESSING:

Subject Matter of the Processing:	The subject matter of the Processing of A&K Personal Data pertains to the provision of Services pursuant to the Agreement.
Nature and Purpose of Processing:	The Processing is related to the provision of Services, namely, the delivery of the travel services, including the provision (where applicable) of accommodation, food, excursions, transport etc., to A&K, as further detailed within the Agreement, and Service Provider and its Contracted Processors (if applicable) will perform such acts of Processing of Personal Data as are necessary to provide those Services according to A&K's instructions, including but not limited to the transmission, storage, and other Processing of Personal Data submitted to the Services.
Further Processing:	Service Provider shall not carry out any further Processing of Personal Data beyond the provision of the Services under the Agreement.
Retention Criteria (Duration):	Generally, retention of Personal Data should not be required. In case Personal Data should be retained, any retention period will be limited to the duration necessary to perform the Services under the Agreement.
Categories of Data Subjects:	A&K may submit Personal Data to Service Provider to perform the Services pursuant to the Agreement and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects: ● Guests of A&K ● Employees of A&K ● Users of the Services
Categories of Personal Data:	A&K may submit Personal Data to the Service Provider to perform the Services pursuant to the Agreement and which may include, but is not limited to the following categories of Personal Data: ● Name, address, date of birth; ● Contact information, including phone number, email, and emergency contact information; ● Passport copy or details (if/where applicable); ● Travel insurance provider (if/where applicable).

Special Categories of Personal Data:	A&K may submit special categories of Personal Data to the Service Provider to perform the Services pursuant to the Agreement, which could include: ● Dietary requirements (if/where applicable) ● Medical requirements/health conditions (if/where applicable). It may be possible to infer additional special categories of Personal Data in connection with performing the Services, such as the following: ● Race or ethnicity (such as from the passport details) ● Religious or philosophical beliefs, political opinions, trade union membership, and/or sex life or sexual orientation, if the nature of the trip reveals such information (such as a group booking from a specific religious association).
Frequency of the Transfer:	Regular and repeating for as long as A&K uses the Services.
Subject Matter, Nature, and Duration of Contracted Processors' Processing:	Any Processing of A&K Personal Data by Contracted Processors will be only as strictly required to perform the Services pursuant to the Agreement. Upon request, Service Provider will provide to A&K a description of Processing for any Contracted Processor(s), including the subject matter, nature, and duration of Processing.
Technical and Organizational Measures of Contracted Processors:	When Service Provider engages a Contracted Processor under this Addendum, Service Provider and the Contracted Processor must enter into an agreement with data protection terms substantially similar to those contained in this Addendum. Service Provider must ensure that the agreement with each Contracted Processor allows Service Provider to meet its respective obligations with respect to A&K. In addition to implementing technical and organizational measures to protect A&K Personal Data, Contracted Processors must: ● notify Service Provider in the event of a Personal Data Breach so that Service Provider may immediately notify A&K; ● delete A&K Personal Data when instructed by Service Provider in accordance with A&K's instructions to Service Provider; ● not engage additional Contracted Processors without Service Provider's authorization; and ● not process A&K Personal Data in a manner which conflicts with A&K's instructions to Service Provider.

Appendix I to Exhibit A

Technical and Organizational Security Measures

Throughout the term of the Agreement and for so long as Service Provider has access to any A&K Personal Data, Service Provider shall implement and maintain technical and organizational security measures ("**TOMs**") to safeguard such A&K Personal Data. Such TOMS may include the following:

Type of TOMs	Description of TOMs
Measures for pseudonymization and encryption of Personal Data:	● Secure implementation of the Transport Layer Security (TLS) protocol version 1.2 or higher for Personal Data in transit using a minimum of 128-bit encryption or 256-bit encryption if applicable ● Encryption of Personal Data in transit through SSH and VPN, with the use of a formal key management system (KMS) ● Encryption of all remote accesses for system maintenance or configuration relating to Personal Data ● Whole disc encryption, container-level encryption, or file-level encryption in portable workstations and portable mass storage media to secure Personal Data at rest using a minimum of 128-bit encryption or 256-bit encryption if applicable ● Pseudonymization capabilities for Personal Data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:	● Adherence to widely recognized standards including but not limited to ISO 27000, ISO 2230, and SOC 2 ● Implementation and enforcement of internal policies, including business continuity plans, high level data security policies, and incident response plans ● Implementation of an in-house detection system and intrusion prevention system to protect network infrastructure ● Firewall protection of external points of connectivity in network architecture ● Storage of Personal Data on servers with RAID 10 parity with regular back-up] ● Policies for classifying, identifying, and handling Personal Data ● Incident response and management ● Anti-virus and anti-malware programs ● Identity and Access Management (IDAM) that includes separation of duties and least privilege ● Expedited patching of known exploitable vulnerabilities in the software applications and IT systems

Type of TOMs	Description of TOMs
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident:	● Implementation and maintenance of procedures to create and maintain retrievable exact copies of Personal Data that Service Provider stores or otherwise maintains ● A business continuity plan that is reviewed, tested, and updated as needed ● A disaster recovery plan that is reviewed, tested, and updated as needed ● Data replication on multiple sites with high availability storage
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the Processing:	● Periodic (at least once annually) internal and external vulnerability scans on information technology systems, including software applications and networks that will be used for Processing Personal Data ● Formal patch management process for vulnerabilities ● Penetration testing at least once annually ● Maintenance of updated security audit certifications (SOC 2 or ISO 27000)
Measures for user identification and authorization:	● Role-based access authorization policy based on least privilege and need to know ● Configuration of systems and applications to restrict access to only authorized access ● Monitoring of all user access ● Password policies and password management procedures that require strong passwords ● Multi-Factor authentication ● Single sign-on (SSO) authentication ● Biometric authentication ● FOB key authentication ● Assignment of a uniquely identifiable ID to each user ● Period audits of active user accounts and associated access capabilities (at least twice annually and when there is a new user or system change)
Measures for the protection of Personal Data during transmission:	● Encryption of Personal Data during transmission using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption or 256-bit encryption if applicable ● Encryption of Personal Data during transmission with TLS and/or through SSH and VPN, with the use of a formal key management system (KMS) ● Secure authentication procedures for executing Personal Data transfers, including access credentials, specific user profiles, biometrics, tokens, etc.
Measures for the protection of Personal Data during storage:	● Encryption of Personal Data during storage (i.e., at rest) using a minimum of AES-256 ● Secure configuration for network devices, such as firewalls, routers, and switches] ● Encryption of Personal Data stored on all mobile devices, including laptops

Type of TOMs	Description of TOMs
Measures for ensuring physical security of locations at which Personal Data are Processed:	● Physical access controls to prevent unauthorized access to facilities (door locks, card readers, security cameras, etc.) ● Environmental controls in facilities storing Personal Data] ● Processes for ensuring that Personal Data is only hosted in facilities with the highest guarantees and certifications (ISO 27001:2013, SOC 2 Type II, etc.)
Measures for ensuring events logging:	● Active monitoring and logging of software application, network, and database security for potential security events at the system, platform, and application levels] ● Retention of audit logs in accordance with legal requirements
Measures for ensuring system configuration, including default configuration:	● Maintenance of documented security baselines for all authorized operating systems, software applications, and network devices ● Performing regular manual audits of all systems to ensure compliance with the organization's security baselines ● Maintenance of secure images or templates for all systems based on the organization's security baselines ● Storage of the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible ● Deployment of system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals] ● Use of a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur
Measures for internal IT and IT security governance and management:	● Dedicated IT governance team ● Dedicated CISO ● Implementation and maintenance of an information security management program based on generally accepted frameworks such as the ISO 27000, NIST Cybersecurity, and CIS Controls, including but not limited to, mobile device policies, incident response management policies, teleworking policies, acceptable use policies, asset management policies, and change management policies
Measures for certification/assurance of processes and products:	● Policies and procedures to ensure compliance with applicable legislative and regulatory requirements

Type of TOMs	Description of TOMs
	● Maintenance of relevant certifications such as ISO 27001 for Information Security management system (ISMS), ISO 22301 for Business Continuity Management System (BCMS), SOC 2 Certification, and/or PCI DSS for card holder environments
Measures for ensuring data minimization:	● An internal review process with relevant stakeholders (including the Data Protection Officer, where applicable) to ensure that Service Provider is only collecting Personal Data that it needs ● Ensuring that data minimization is embedded into the system configuration and change management procedure ● Internal processes to remove Personal Data from its systems as soon as that Personal Data is no longer required under the terms of the Agreement
Measures for ensuring data quality:	● Implement and maintain appropriate technical controls to prevent, detect, and correct data integrity violations in IT Systems, including but not limited to data loss prevention (DLP) tools, checksums, mirroring, ECC memory, RAID parity, and file integrity monitoring tools
Measures for ensuring limited data retention:	● Implementation of an internal retention schedule for Personal Data, including backups, based on legal and regulatory requirements ● Ensuring secure disposal of devices that store Personal Data
Measures for ensuring accountability:	● Implementation and maintenance of a security and awareness program that includes at least an annual privacy and security training for all individuals responsible for Processing Personal Data] ● Ensuring that personnel responsible for Processing Personal Data are bound to confidentiality obligations (e.g., through a non-disclosure agreement) ● Procedures for discipline and sanctions when personnel violate security policies, non-disclosure agreements, and other policies relating to Personal Data] ● Enforcement of internal IT and IT security governance and management in accordance with the TOMs entitled “Measures for internal IT and IT security governance and management” above
Measures for allowing data portability and ensuring erasure:	● Maintenance of an updated data inventory (i.e., a data map or a record of processing) that identifies all locations where a Data Subject’s Personal Data is stored ● Creation of a self-service portal or a ticketed system for Data Subjects to access, export, correct, or delete their Personal Data ● Segregation of Personal Data in IT systems and databases ● Processes for assuring that Personal Data can be deleted from backup media if legally required
Information about Contracted Processors’ TOMs:	Set forth in **Part B of Exhibit A**.

Exhibit B

Jurisdiction Specific Terms

1. Australia

1.1. When applicable, the Processing of A&K Personal Data shall be compliant with the Australian Privacy Principles, the Australian Privacy Act (1988), or any other applicable law, regulation, or decree of Australia pertaining to the protection of such information.

2. Brazil

2.1. When applicable, the Processing of A&K Personal Data shall be compliant with Brazil's Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018 and any corresponding decrees, regulations, or guidance.

3. Canada

3.1. When applicable, the Processing of A&K Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable Canadian privacy or data protection laws.

4. European Economic Area

4.1. Definitions.

(a) "**EEA**" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(b) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of A&K Personal Data.

(c) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as may be amended from time to time.

(d) "**EU 2021 Standard Contractual Clauses**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

4.2. Restricted Transfers. With regard to any Restricted Transfer subject to EEA Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision adopted by the European Commission on the basis of Article 45 of the EU GDPR;

(b) The appropriate Standard Contractual Clauses adopted by the European Commission from time to time; or

(c) Any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws, as the case may be.

4.3. Standard Contractual Clauses.

(a) This Addendum hereby incorporates by reference the Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The Parties agree that any references to clauses, annexures, modules, and choices within the Standard Contractual Clauses shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated Standard Contractual Clauses as may be applicable from time to time pursuant to this Addendum.

(c) For the purposes of the EU 2021 Standard Contractual Clauses and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future:

i. The Parties agree to apply the following modules, as applicable:

(A) Module Two with respect to Controller-to-Processor Restricted Transfers; and

(B) Module Four with respect to Processor-to-Controller Restricted Transfers;

ii. Clause 7: The Parties choose not to include the optional docking clause.

iii. Clause 9(a): The Parties choose Option 2, "General Written Authorization," and the time period set forth in Section 6.3 of this Addendum. The procedures for designation and notification of new Contracted Processors are set forth in more detail in Section 6 of this Addendum.

iv. Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.

v. Clause 13 (Annex I.C): The competent Supervisory Authority is the Irish Data Protection Commission.

vi. Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.

vii. Clause 18: The Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland.

viii. Annex I(A and B): The content of Annex I(A) is set forth in **Part A of Exhibit A**.

ix. Annex II: The content of Annex II is set forth in **Appendix I to Exhibit A**.

4.4. The terms contained in **Exhibit C** to this Addendum supplement the Standard Contractual Clauses.

4.5. In cases where the Standard Contractual Clauses apply and there is a conflict between the terms of this Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail with regard to the Restricted Transfer in question.

5. South Africa

5.1. When applicable, the Processing of A&K Personal Data (as identified in Exhibit A) shall be compliant with the Protection of Personal Information Act (POPIA). For the sake of clarity, Service Provider's obligations to A&K under the DPA are those that POPIA requires that Service Provider as "Operator" have in place with A&K as the "Responsible Party", and "Personal Data" means "personal information".

5.2. Service Provider will further establish and maintain the security measures referred to in section 19 of POPIA and will notify A&K immediately where there are reasonable grounds to believe that the Personal Data of a data subject has been accessed or acquired by any unauthorized person.

5.3. Service Provider shall ensure that no Personal Data of data subjects is transferred outside of the Republic of South Africa unless:

(a) the data subject provides its prior written consent to the transfer;

(b) the recipient is subject to a law, code of conduct or contract which provides comparable protection for the Personal Data as the protections contained in this Addendum, including similar provisions relating to the further transfer of the Personal Data;

(c) the transfer is necessary for the performance of a contract between the data subject and A&K, or a contract between the data subject and Supplier which is in the interest of the data subject; or

(d) the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject, and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

6. Switzerland

6.1. Definitions.

(a) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

(b) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection as amended ("**FADP**") and the Ordinance to the Federal Act on Data Protection.

6.2. Restricted Transfers. With regard to any Restricted Transfer subject to Swiss Data Protection Laws between the Parties one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision adopted by the FDPIC on the basis of Article 6 of the FADP;

(b) The Standard Contractual Clauses adopted by the FDPIC; or

(c) Any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

6.3. Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the EU 2021 Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The Parties incorporate and adopt the EU 2021 Standard Contractual Clauses for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be the FDPIC. Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Data Subjects in Switzerland from applying to the FDPIC for relief.

ii. Clause 18: The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.

iii. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there any Restricted Transfers subject to Swiss Data Protection Laws.

6.4 In cases where the Standard Contractual Clauses apply and there is a conflict between the terms of this Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail with regard to the Restricted Transfer in question.

7. United Kingdom

7.1. Definitions.

(a) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(b) "**UK Data Protection Laws**" (as used in this Section) includes the Data Protection Act 2018 and the UK GDPR (as defined below).

(c) "**UK GDPR**" (as used in this Section) means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

(d) "**UK ICO**" (as used in this Section) means the UK Information Commissioner's Office.

(e) "**UK IDTA**" (as used in this Section) means the International Data Transfer Agreement issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

(f) "**UK Transfer Addendum**" (as used in this Section) means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

7.2. Restricted Transfers. With regard to any Restricted Transfer subject to UK Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) a valid adequacy decision adopted pursuant to Article 45 of the UK GDPR;

(b) the UK IDTA;

(c) the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under UK Data Protection Laws, and the Processing activities of the Data Importer are not subject to the UK GDPR by virtue of application of Article 3(2) of the UK GDPR), as they have been adopted for use by the relevant authorities within the United Kingdom, including the UK ICO, using the UK Transfer Addendum; or

(d) any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

7.3. EU 2021 Standard Contractual Clauses and UK Transfer Addendum

(a) The Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses, which have been adopted for use by the UK ICO with certain modifications and the addition of the UK Transfer Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(b) For the purposes of the tables to the UK Transfer Addendum:

i. Table 1: The content of Table 1 is set forth in **Part A of Exhibit A**.

ii. Table 2: The content of Table 2 is incorporated and adopted as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms. To the extent Module 4 is

applicable, Personal Data received from the Data Importer may be combined with personal data collected by the Data Exporter.

iii. Table 3: The content of Table 3 (Annexes 1A, 1B, II, and III) is set forth as follows:

(A) *Annex 1*: The content of Annex 1 is set forth in **Exhibit A**.

(B) *Annex II*: The content of Annex II is set forth in **Appendix I to Exhibit A**.

iv. Table 4: The Parties agree that the Data Exporter may terminate the UK Transfer Addendum.

(c) The Parties incorporate and adopt the EU 2021 Standard Contractual Clauses as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms, with the following distinctions:

i. Clause 13 (Annex I.C): The competent authority shall be UK ICO.

ii. Clause 17: The EU 2021 Standard Contractual Clauses, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.

iii. Clause 18: The Parties agree that any dispute arising from the Standard Contractual Clauses or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The terms contained in **Exhibit C** to this Addendum supplements the EU 2021 Standard Contractual Clauses.

(e) In cases where the EU 2021 Standard Contractual Clauses, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of this Addendum and the terms of the EU 2021 Standard Contractual Clauses, in conjunction with the UK Transfer Addendum, the terms of the EU 2021 Standard Contractual Clauses, in conjunction with the UK Transfer Addendum, shall prevail with regard to the Restricted Transfer in question.

7.4. UK IDTA.

(a) This Addendum hereby incorporates by reference the UK IDTA. The Parties are deemed to have accepted, executed, and signed the UK IDTA where necessary in its entirety.

(b) For the purposes of the tables to the UK IDTA:

i. Table 1: The information required by Table 1 appears within **Part A of Exhibit A**.

ii. Table 2:

(A) The UK IDTA, shall be governed by the laws of England and Wales.

(B) The Parties agree that any dispute arising from the UK IDTA shall be resolved by the courts of England and Wales.

(C) The Parties' controllership and data transfer roles are set out in **Part A of Exhibit A**.

(D) The UK GDPR may apply to the Data Importer's Processing of the Personal Data.

(E) This Addendum and the Agreement set out the instructions for Processing Personal Data.

(F) The Data Importer shall Process Personal Data for the time period set out in **Part B of Exhibit A**. The Parties agree that the Data Exporter may terminate the UK IDTA before the end of such time period with one month's written notice.

(G) The Data Importer may only transfer Personal Data to authorized Contracted Processors (if applicable), as set out within Section 6 of this Addendum, or to such third parties that the Data Exporter authorizes in writing or within the Agreement.

(H) Each Party must review this Addendum at regular intervals, to ensure that this Addendum remains accurate and up to date and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews as frequently as at least once each year or sooner.

iii. Table 3: The content of Table 3 is set forth in **Part B of Exhibit A**.

iv. Table 4: The content of Table 4 is set forth in **Appendix I to Exhibit A**.

(c) Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK IDTA are noted throughout this Addendum.

(d) The terms contained in **Exhibit C** to this Addendum supplement the UK IDTA.

(e) In cases where the UK IDTA applies and there is a conflict between the terms of this Addendum and the terms of the UK IDTA, the terms of the UK IDTA shall prevail.

8. United States of America

8.1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of United States Data Protection Laws (defined below), the provisions of the Addendum and this Section shall apply to such Processing.

8.2. Definitions.

(a) "**United States Data Protection Laws**" include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the Processing of Personal Data, as may be amended from time to time. Such laws include, without limitation:

i. the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 *et seq.*), and the California Consumer Privacy Act Regulations, together with all implementing regulations;

ii. the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 *et seq*., together with all implementing regulations;

iii. the Connecticut Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015;

iv. the Oregon Consumer Privacy Act, Senate Bill 619;

v. the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code Ann. § 541.001 *et seq.*;

vi. the Utah Consumer Privacy Act, Utah Code Ann. S 13-61-101 *et seq.*; and

vii. the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 *et seq*.

(b) "**Personal Data Breach**" (as used in the Addendum) includes "Breach of Security" and "Breach of the Security of the System" as defined under applicable United States Data Protection Laws.

(c) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sell**", and "**Share**" shall have the same meanings as under applicable United States Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

8.3. Processing of A&K Personal Data.

(a) A&K discloses A&K Personal Data to Service Provider solely for: (i) valid Business Purposes; and (ii) to enable Service Provider to perform the Services.

(b) Service Provider shall not: (i) Sell or Share A&K Personal Data; (ii) retain, use, or disclose A&K Personal Data for a Commercial Purpose other than providing the Services specified in the Agreement or as otherwise permitted by United States Data Protection Laws; (iii) retain, use, or disclose A&K Personal Data except where permitted under the Agreement; or (iv) combine A&K Personal Data with other information that Service Provider Processes on behalf of other persons or that Service Provider collects directly from the Data Subject, with the exception of Processing for permitted Business Purposes. Service Provider certifies that it understands these prohibitions and agrees to comply with them.

8.4. Termination. Upon termination of the Agreement, Service Provider shall, as soon as reasonably practicable, destroy all Personal Data it has Processed on behalf of A&K after the end of the provision of Services relating to the Processing and destroy all copies of the Personal Data unless applicable law requires or permits storage of such Personal Data.

Exhibit C

Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit C** (this "**Exhibit**"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred to the importing Party pursuant to Standard Contractual Clauses. This Exhibit supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted Transfer.

1. Definitions

1.1. For the purpose of interpreting this Exhibit, the following terms shall have the meanings set out below:

(a) "**EO 12333**" means the U.S. Executive Order 12333.

(b) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(c) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.

2. Applicability of Surveillance Laws to Data Importer and its Contracted Processors

2.1. U.S Surveillance Laws.

(a) Data Importer represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II judgment.

(b) Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

i. No court has found Data Importer to be an entity eligible to receive legal process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4); or (ii) an entity belonging to any of the categories of entities described within that definition.

ii. If Data Importer were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II judgment.

(c) EO 12333 does not provide the U.S. government the ability to order or demand that Data Importer provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to EO 12333.

3. Backdoors

3.1. Data Importer certifies that:

(a) It has not purposefully created backdoors or similar programming for governmental agencies that could be used to access Data Importer's systems or A&K Personal Data subject to the Standard Contractual Clauses.

(b) It has not purposefully created or changed its business processes in a manner that facilitates governmental access to A&K Personal Data or systems.

(c) National law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to A&K Personal Data or systems.

3.2. Data Exporter will be entitled to terminate the contract on short notice in cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

4. Information About Legal Prohibitions

4.1. Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under this Exhibit. Data Importer may choose the means to provide this information.

5. Additional Measures to Prevent Authorities from Accessing A&K Personal Data

5.1. Notwithstanding the application of the security measures set forth in this Addendum, Data Importer will implement internal policies establishing that:

(a) Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred A&K Personal Data;

(b) Data Importer's Data Protection Officer shall be notified upon receipt of each request or order for transferred A&K Personal Data;

(c) Data Importer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

(d) if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

(e) if Data Importer receives a request from public authorities to cooperate on a voluntary basis, A&K Personal Data transmitted in plain text may only be provided to public authorities with the express agreement of Data Exporter.

6. Termination

6.1. This Exhibit shall automatically terminate with respect to the Processing of A&K Personal Data transferred in reliance of the Standard Contractual Clauses if the European Commission or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted Transfers covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Exhibit will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Exhibit.