**SCHEDULE “B” – DATA PRIVACY AND ONWARD TRANSFER AGREEMENT**

* + 1. **Definitions**. Capitalized terms used in this Schedule and not otherwise defined have the meanings ascribed to them in the Agreement. For the purposes of this Schedule, the following terms shall have the following meanings:

1. “**Process**” or “**Processing**” means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
2. “**Privacy Shield Framework**” means the Swiss-U.S. Privacy Shield Framework.
   * 1. Background. Service Provider acknowledges that in order to carry out its duties and obligations under the Agreement, Service Provider may gain access to Personal Information. In such cases, Service Provider will operate as processor (or “**agent**” as defined by the Privacy Shield Framework for Priceline for the limited purposes of using, storing, and otherwise processing Personal Data pursuant to the Agreement and this Schedule.
     2. **Obligations of Service Provider**. Service Provider shall:
3. only use applications and systems within Priceline’s System to Process Personal Data. Service Provider shall only have remote read-only access to Personal Data with no ability to copy or capture such data, unless agreed otherwise in advance and in writing;
4. designate a security official responsible for the development, implementation, and maintenance of its Information Security Program (as defined below) and Service Provider shall inform Priceline as to the person responsible for security;
5. Process the Personal Data only for the purpose of fulfilling its obligations under the Agreement or as otherwise instructed in writing by Priceline, and in accordance with all applicable Privacy Laws, the terms of this Schedule, and the Privacy Shield Framework;
6. notify Priceline in writing immediately upon making a determination that it has not met, or can no longer meet, its obligations under Section 3 of this Schedule, and, in such case, will abide by Priceline’s written instructions, including instructions to cease further Processing of the Personal Data, and take any necessary steps to remediate any Processing of such Personal Data not in accordance with this Section 3;
7. submit its data processing facilities, data files and documentation needed for Processing the Personal Data to auditing and/or review by Priceline or any independent auditor or inspection entity reasonably selected by Priceline to ascertain compliance with this Schedule upon the request of Priceline, with reasonable notice and during normal business hours;
8. obtain the prior written approval of Priceline to disclose Personal Data to any third party or otherwise allow any third party to access Personal Data; and, in such an event, it shall: (i) impose the no less equivalent privacy and security requirements on any such third party to which Service Provider is subject under this Schedule; (ii) remain responsible for any such third party’s actions with respect to the Personal Data; and (iii) provide to Priceline, at least 60 days before disclosing or allowing access to any such Personal Data, a list detailing the name and address of all such third parties to which it discloses or allows access to Personal Data, including the locations of such third party’s servers hosting or Processing Personal Data, in order to allow Priceline to evaluate whether supplemental data processing agreements or other controls are needed to protect Personal Data and/or to decide whether to decline approval for subcontracting to any such third parties;
9. without limiting the generality of any of the obligations of Service Provider set out under the Agreement, with respect to the Personal Data transferred to Service Provider or received by Service Provider under the Agreement, Service Provider has implemented, and will maintain, a comprehensive written information security program (“**Information Security Program**”) that includes administrative, technical, and physical safeguards to ensure the confidentiality, security, integrity, and availability of Personal Data and to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. In particular, the Information Security Program shall include, but not be limited to, the following safeguards where appropriate or necessary to ensure the protection of Personal Data:
   * 1. Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access and will maintain the confidentiality of the Personal Data, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt and decrypt Personal Data where appropriate;
     2. Security Awareness and Training – a security awareness and training program for all members of workforce (including management), which includes training on how to implement and comply with its Information Security Program;
     3. Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes;
     4. Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan;
     5. Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of a facility, and the movement of these items within a Service Provider’s facility, including policies and procedures to address the final disposition of Personal Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use, and Service Provider shall ensure that no Personal Data is downloaded or otherwise stored on laptops or other portable devices;
     6. Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith;
     7. Data Integrity – policies and procedures to ensure the confidentiality, integrity, and availability of Personal Data and protect it from disclosure, improper alteration, or destruction;
     8. Storage and Transmission Security – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt Personal Data in electronic form while in transit and in storage on networks or systems to which unauthorized individuals may have access;
     9. Storage Media - policies and procedures to ensure that prior to any storage media containing Personal Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, will irreversibly delete such Personal Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media such that it is impossible to recover any portion of data on the media that was destroyed;
     10. Disposal – an auditable program implementing the disposal and destruction requirements set forth in this Section for all storage media containing Personal Data;
     11. Testing – policies and procedures regarding the regular testing of key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified, with tests being conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs; and
     12. Adjust the Program – the monitoring, evaluation, and adjustment, as appropriate, of the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Personal Data, internal or external threats to or the Personal Data, and Service Provider’s own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems,
10. provide assistance to Priceline as may be reasonably necessary for Priceline to comply with Applicable Laws relating to data protection, including, but not limited to, (i) assisting Priceline in responding to data subject requests for exercising data subject rights under Applicable Law; (ii) assisting Priceline in responding to data protection authority or other regulatory requests for information related to Processing; and (iii) providing all information necessary related to Processing for Priceline to demonstrate compliance with Applicable Laws relating to data protection;
11. submit to the investigatory and other jurisdiction of the U.S. Federal Trade Commission and/or data protection Governmental Authorities in the European Union with respect to the Processing of the Personal Data, to the same extent that such investigatory and other jurisdiction would apply to Priceline under the Privacy Shield Framework;
12. without limiting the generality of any of the obligations of Service Provider set out under the Agreement, in the event of a Security Incident: (i) reimburse Priceline for any and all damages, losses, fees or costs incurred as a result of such incident; (ii) remedy, to the extent reasonably possible, any harm or potential harm caused by such incident; and (iii) to the extent that a Security Incident arises from network and/or to the extent the breach arises from breach of this Schedule gives rise to a need, in Priceline’s sole judgment to provide (A) notification to public authorities, individuals, or other persons, or (B) undertake other remedial measures (including, without limitation, notice, credit monitoring services and the establishment of a call center to respond to inquiries (each of the foregoing a “**Remedial Action**”)), at Priceline’s request, Service Provider shall, at Service Provider’s cost, undertake such Remedial Actions, with the timing, content and manner of effectuating any notices being determined by Priceline in its sole discretion; and
13. promptly notify Priceline if it receives a request for subject access, rectification, cancellation, objection or any other data protection related requests, and, should any Governmental Authority contact Service Provider with a demand for Confidential Information, Service Provider will direct such Governmental Authority to request such information directly from Priceline. As part of this effort, Service Provider may provide Priceline’s basic contact information to such Governmental Authority. If compelled to disclose the Confidential Information to law enforcement, then Service Provider will promptly, and without any undue delay, notify Priceline and deliver a copy of the request (except where Service Provider is legally prohibited from doing so) to allow Priceline to seek a protective order or any other appropriate remedy.
    * 1. **Cross-Border Transfers from European Economic Area (EEA).** Service Provideragrees that this Schedule incorporates by reference the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU) (“**Model Processor Contract**”), where Service Provider shall be deemed for the purposes of this Schedule to be the “data importer,” each of Priceline’s affiliates established in the EU shall be deemed for the purposes of this Schedule to be the “data exporter,” and the data processing activities in Appendix 1 to the Model Processor Contract shall be such activities as necessary for to perform its services for Priceline as described in this Schedule, and the data security measures in Appendix 2 to the Model Processor Contract shall be those identified in Section 3 of this Schedule.
      2. **Further Assurances**. Service Provider shall, upon Priceline’s request, promptly execute supplemental data processing agreement(s) with Priceline or any of its Affiliates or take other appropriate steps to address cross-border transfer and other applicable requirements if Priceline concludes, in its sole judgment, that such steps are necessary to address data privacy, data protection, and/or data security laws applicable to Priceline.
      3. **Termination**.
14. This Schedule shall remain in full force and effect for so long as the Agreement remains in effect, unless earlier terminated pursuant to Section 6(b).
15. Priceline may, in its sole and unfettered discretion, terminate this Schedule and/or the Agreement immediately, without judicial notice or resolution and without prejudice to any other remedies, in the event that: (i) compliance with the terms of this Schedule by Service Provider would put in breach of its legal obligations; (ii) Service Provider is in breach of any representations or warranties given by it under this Schedule and fails to cure such breach with thirty (30) days’ notice from Priceline; (iii) Service Provider provides notice to Priceline pursuant to Section 3(g) of this Schedule; (iv) a data protection or other regulatory authority or other tribunal or court in the countries in which Priceline or its Affiliates operate finds that there has been a breach of any Applicable Law in that jurisdiction by virtue of Service Provider or Priceline’s processing of the Personal Data; or (v) if either party makes an assignment for the benefit of creditors, becomes subject to a bankruptcy proceeding, is subject to the appointment of a receiver, or admits in writing its inability to pay its debts as they become due.
16. This Schedule shall immediately terminate if the Agreement is terminated for any reason.
17. Upon termination of this Schedule for any reason, Service Provider shall return all Personal Data and all copies of the Personal Data subject to this Schedule to Priceline or, at Priceline’s request, shall destroy (i.e., render the information permanently unreadable and not reconstructable into a usable format in accordance with the then-current U.S. Department of Defense, or similar data destruction standard or CESG standards, as applicable) all such Personal Data and shall certify to Priceline that it has done so.
    * 1. **Withholding**. Under no circumstance shall Service Provider be entitled, and Service Provider hereby forever waives any and all right, to withhold any Personal Information from Priceline to enforce any alleged payment obligation or in connection with any dispute relating to the terms of the Agreement or any other matter between Priceline and Service Provider.
      2. **Paramountcy**. If there is a conflict between the provisions of the Agreement and the provisions of this Schedule, the provisions in this Schedule shall govern.