

UPS DATA PROCESSING EXHIBIT
UPSDPE02/2022

This UPS Data Processing Exhibit (the “Exhibit”) contains requirements for Vendor with respect to the privacy and protection of Personal Information that Vendor accesses or acquires from UPS or its Affiliates, that UPS or its Affiliates provide to Vendor, or that Vendor collects or acquires on behalf of UPS or its Affiliates. Capitalized terms used without definition in this Exhibit are defined in Section 4 (Definitions) of this Exhibit.

1. PROCESSING OF PERSONAL DATA

- (a) General Obligations. Vendor will Process Personal Data in compliance with Applicable Law at all times and will provide at least the same level of privacy protection for all Personal Data as required by Applicable Law. Vendor will not disclose Personal Data to any third party without first obtaining UPS’s written consent. Vendor shall ensure that, at all relevant times during the term of the Agreement, all Vendor personnel engaged in the Processing of Personal Data are subject to enforceable obligations to maintain the confidentiality of the Personal Data and to comply with the relevant terms and conditions of this Exhibit.
- (b) Processing Only on Instructions from UPS. Vendor will Process Personal Data solely on behalf of UPS for the purpose of performing the Services and in accordance with UPS’s instructions as issued from time to time in writing. Vendor acknowledges that, with respect to the Personal Data, Vendor will act only as a data processor as defined under Applicable Law. The duration of Vendor’s Processing of Personal Data will be the term of the Agreement, except as provided in the Agreement, and subject to Section 1(e) (Retention and Deletion) of this Exhibit. Vendor will Process only such Personal Data during the course of performing the Services as is strictly necessary for Vendor to perform the Services. Vendor shall not combine or commingle Personal Data with Personal Information that Vendor receives from or on behalf of any third party or collects from Vendor’s own interactions with Data Subjects, except to the extent necessary to Process the Personal Data in accordance with this Exhibit. If Applicable Law requires Vendor (or, for avoidance of doubt, any subcontractor) to conduct Processing that is or could be construed as inconsistent with UPS’s instructions, then Vendor shall notify UPS promptly and prior to commencing the Processing. If Vendor believes that any instruction from UPS is in violation of, or would result in Processing in violation of, Applicable Law, then Vendor shall notify UPS immediately.
 - (i) The Personal Data to be Processed by the Vendor consists of the following categories of information: names, physical addresses, email addresses, etc.
 - (ii) The Personal Data to be Processed by the Vendor involves the following categories of Data Subjects: shippers, consignees and package recipients, customers of customers of UPS and its Affiliates, current and former employees and job applicants, contractors, supplier and vendors, prospective customers, financial services customers, The UPS Store, The UPS Store customers, The UPS Store Owners.
- (c) Subcontractors. Vendor may subcontract the Processing of Personal Data only with prior written consent of UPS. For any proposed subcontractor, Vendor will disclose to UPS the geographic location(s) at which the proposed subcontractor will perform the Processing. All Processing by subcontractors must be subject to a written agreement between Vendor and the subcontractor that requires the subcontractor to comply with the same limitations, restrictions and other terms and conditions as provided in this Exhibit, including express guarantees by the subcontractor to implement technical and organizational measures to ensure that Processing satisfies all requirements of Applicable Law. Vendor shall remain responsible for the Processing of the Personal Data and for any acts and omissions of such subcontractors to the same extent as if such acts or omissions were performed by Vendor.

(d) Cooperation to Facilitate Data Subject Requests.

- (i) Vendor will at no additional charge cooperate fully with UPS with respect to, and facilitate UPS's authentication, recording, investigation, processing, execution and resolution of, all enquiries, complaints, requests and claims of Data Subjects relating to access, rectification, portability, restriction, erasure, objection or any other rights available to Data Subjects under Applicable Law with respect to Personal Data.
 - (ii) Vendor will notify UPS promptly if it receives any enquiry, complaint, request or claim from a Data Subject relating to Personal Data or the Processing thereof. Vendor will not respond to any such Data Subject request without UPS's prior written consent except to the extent required by Applicable Law or necessary to confirm the request relates to UPS.
- (e) Retention and Deletion. Vendor may retain Personal Data only for the period of time required for Vendor to perform the Services, or such longer period required by Applicable Law, required pursuant to the Agreement or requested in writing by UPS. Vendor will permanently delete all copies of Personal Data in its possession or control at the expiration of such time period in accordance with any standards provided for deletion of data in the main body of the Agreement or in the Security Exhibit or, if the Agreement does not provide such standards, then in accordance with applicable industry standards for secure deletion of Personal Data.

(f) Cross-Border Transfers.

- (i) Vendor may only transfer Personal Data across national borders upon the prior written consent of UPS and in compliance with Applicable Law.
- (ii) Vendor will follow UPS's instructions with respect to any transfer of Personal Data across national borders to adduce adequate safeguards for the privacy of all relevant Data Subjects and will require any applicable subcontractors to do the same. Without limiting the generality of the foregoing, transfers by Vendor (if any) of Personal Data from the European Economic Area, Switzerland or the United Kingdom to another location must be: (A) to a country providing adequate protection of privacy rights (as deemed by the European Commission, the UK Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner, as applicable, from time to time); (B) pursuant to Standard Contractual Clauses issued or approved by the European Commission, the UK Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner, as applicable, and which remain valid for use for transfers of Personal Data from the applicable jurisdiction at the time of the transfer, provided Vendor has secured any necessary approvals for the transfer from applicable governmental authorities; or (C) authorized by all applicable governmental authorities in the European Economic Area, Switzerland or the United Kingdom, as the case may be, such as through Binding Corporate Rules approved by all applicable governmental authorities.

2. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

- (a) Standards. Vendor will take all necessary technical and organizational security measures against the unauthorized or unlawful processing of Personal Data and against the loss, alteration or destruction of, or damage to, Personal Data. Such technical and organizational measures will include at a minimum: (i) compliance with the Security Exhibit or, if the Agreement does not include a Security Exhibit, (ii) compliance with applicable industry standards for information security. Vendor acknowledges that its duty to take security measures under this Section 2(a) is in addition to, and does not limit, Vendor's obligations to take appropriate technical and organizational security measures pursuant to Applicable Law.

(b) Privacy Breaches.

- (i) For the avoidance of doubt, Vendor agrees that any Privacy Breach will constitute a Data Breach as defined in the Security Exhibit. In the event of a Privacy Breach, Vendor will therefore comply with all requirements of the Security Exhibit that arise from or relate to a Data Breach.
- (ii) If the Agreement does not require Vendor to notify UPS of a Privacy Breach, then Vendor will comply with this Section 2(b)(ii).
 - (A) Vendor will maintain a documented Privacy Breach action and response plan. If Vendor discovers or is notified of a Privacy Breach, then Vendor will at its expense: (1) notify UPS immediately of the Privacy Breach; (2) investigate the Privacy Breach; (3) mitigate the effects of the Privacy Breach; and (4) perform post-incident assessments, including those reasonably requested by UPS, and report on the results of such assessment(s) to UPS.
 - (B) Vendor will promptly provide UPS with, at a minimum, information to assist UPS in its own reporting obligations relating to the Privacy Breach, including descriptions of the following: (1) the steps taken by Vendor to remedy the Privacy Breach; (2) when the investigation and mitigation has been completed, as well as material progress related to the foregoing; and (3) the details of the Privacy Breach.
 - (C) Vendor will be solely responsible for the costs incurred by UPS: (1) to remedy any Privacy Breach; (2) to notify all affected Data Subjects of the Privacy Breach; (3) to provide commercially reasonable identity theft protection services to affected Data Subjects; and (4) to establish and operate (directly or through a third party) call center and other support resources to provide information to Data Subjects inquiring about the Privacy Breach.
- (iii) Vendor agrees that, in addition to applicable requirements provided in the Security Exhibit or in Section 2(b)(ii):
 - (A) Vendor's notice to UPS of a Privacy Breach must contain the following: (1) a description of the categories and approximate number of Data Subjects, as well as the categories and approximate number of Personal Data records affected by the Privacy Breach; (2) the name and contact details of any Data Protection Officer appointed by Vendor; and (3) Vendor's assessment, developed through reasonable diligence, of the likely consequences of the Privacy Breach with respect to the affected Personal Data and Data Subjects.
 - (B) If UPS determines that any Privacy Breach must be disclosed to a third party, including Data Subjects or governmental authorities (including, but not limited to, any data protection authorities in the European Economic Area), then Vendor shall fully cooperate with and assist UPS in fulfilling UPS's reporting and disclosure obligations.
 - (C) Vendor shall not disclose the occurrence of any Privacy Breach to any third party without first obtaining UPS's written consent to do so, except to the extent Vendor is required by Applicable Law to make such disclosure prior to obtaining UPS's written consent. Vendor agrees that UPS has the sole right to determine: (1) whether to provide notice of the Privacy Breach to any individuals, regulators, consumer reporting agencies or other third parties; and (2) the contents of such notice, whether any type of remediation may be offered to affected Data Subjects, and the nature and extent of any such remediation.

3. AUDITS AND OVERSIGHT.

- (a) Audits. Vendor will provide to UPS, its auditors (including internal audit staff and external auditors), inspectors, regulators and other representatives access to any Vendor owned or managed facility or part of a Vendor owned or managed facility at which Vendor is providing the Services, to relevant Vendor personnel, and to computer systems, data and records relating to the Services for the purpose of performing audits of Vendor or any of its subcontractors to verify Vendor's compliance with this Exhibit. Vendor will provide full cooperation to UPS and its representatives in connection with any such audit. UPS may perform such audits no more than once in any calendar year unless UPS has a reasonable suspicion of a breach or potential breach of this Exhibit by Vendor, in which event UPS may perform an audit on a more frequent basis. Vendor will respond in writing within thirty (30) days to all recommendations UPS provides that result from such audits. Vendor will comply with all reasonable recommendations from UPS that result from such audits relating to Vendor's compliance with this Exhibit.
- (b) Documentation and Requests for Information. Vendor will:
 - (i) Document and provide to UPS upon request copies of all records of Personal Data Processing activities required to be maintained under Applicable Law;
 - (ii) Provide to UPS a copy of Vendor's then-most recent audit report or review that relates to any Processing of Personal Data, as conducted by Vendor's external auditors; and
 - (iii) Provide to UPS copies of the reports resulting from any audits performed by Vendor's internal personnel that include Processing of Personal Data within their scope.
- (c) Cooperation.
 - (i) If UPS determines that Applicable Law or UPS policy requires an assessment of the privacy impacts of any Processing of Personal Data by or on behalf of Vendor, then Vendor will cooperate fully with and facilitate UPS's conduct of the assessment.
 - (ii) If UPS determines that Applicable Law or a UPS policy requires UPS to notify, seek guidance from or consult with a third party, including any governmental authority or representative labor body, concerning Vendor's Processing of Personal Data, then Vendor will cooperate with UPS in connection with such advisory request or consultation.
 - (iii) Vendor will notify UPS promptly if Vendor becomes the subject of, or reasonably believes it may become the subject of, any claim, investigation, audit, suit or enforcement proceeding arising from or relating to Vendor's Processing of Personal Data; and will cooperate fully with UPS and assist UPS with any claim, investigation, audit, suit or enforcement proceeding arising from or relating to Vendor's Processing of Personal Data.
 - (iv) Vendor will fully cooperate with any reasonable and appropriate steps UPS takes, pursuant to Section 3(d) (Compliance with Exhibit), to stop and remediate any unauthorized use of Personal Data.
 - (v) Vendor's cooperation pursuant to this Section 3(c) must include providing access to relevant information, records and personnel.

- (d) Compliance with Exhibit. Vendor certifies that Vendor understands the restrictions in this Exhibit and will comply with them. Vendor must notify UPS immediately if Vendor determines it can no longer meet its obligations under this Exhibit. Any failure of Vendor to comply with this Exhibit constitutes a material breach of the Agreement. In such event, UPS may terminate the Agreement or the applicable Processing, effective immediately, at its sole option upon written notice to Vendor without liability or further obligation to Vendor and without prejudice to any other remedies under this Agreement, at law or in equity, and may take other reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

4. DEFINITIONS

- (a) "Affiliate" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.
- (b) "Agreement" means the contract between UPS and Vendor that references this Exhibit, including all Schedules, Exhibits, Appendices and other attachments to the contract.
- (c) "Applicable Law" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, reporting or licensing requirements, ordinances and other pronouncement having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority. References to "Applicable Law" mean the Applicable Law as may be amended, modified, supplemented, or restated.
- (d) "Data Subject" means an identified or identifiable natural person.
- (e) "Personal Information" means information that identifies or relates to an identifiable individual (i.e., a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person physical, physiological, mental, economic, cultural or social identity) or such person's computer system or mobile device, and other similar information regulated by Applicable Law.
- (f) "Personal Data" means Personal Information that Vendor accesses or acquires from UPS or its Affiliates, that UPS or its Affiliates provide to Vendor, or that Vendor collects or acquires on behalf of UPS or its Affiliates.
- (g) "Privacy Breach" means any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to PII.
- (h) "Process" means any operation or set of operations which is performed upon PII, whether by automatic or manual 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.
- (i) "Security Exhibit" means the UPS Information Security Agreement for Vendors or such other exhibit, schedule or appendix to the Agreement or provisions set forth within the main body of the Agreement that set forth information security standards for Vendor.
- (j) "Services" means the services Vendor is obligated to perform pursuant to the Agreement.