DESIGNER BRANDS

THESHOECOMPANY.CA DSW.CA

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") is between Designer Brands Inc. ("Company") and Vendor (as defined in the Agreement). All capitalized terms not otherwise defined in this Addendum will have the meaning given to them in the Agreement. In the event of any inconsistency or conflict between this Addendum and the Agreement, this Addendum will govern. This Addendum will survive termination or expiration of the Agreement.

1. Definitions. For the purposes of this Addendum, the following terms shall have the following meanings:

"Applicable Privacy Laws" means all applicable current and future federal, provincial, and local laws, ordinances, regulations, and orders relating to privacy, data security, and the processing, storage, protection, and disclosure of Personal Data, including, but not limited to, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), Personal Information Protection Act (Alberta), Personal Information Protection Act (British Columbia), and Act Respecting the Protection of Personal Information in the Private Sector (Quebec).

"Data Subject Rights Request" means a request by a natural person to exercise one or more rights provided to such person under Applicable Privacy Laws, including, but not limited to, a right to access, correct, amend, transfer, or delete Personal Data or restrict or object to the Processing of such data.

"Personal Data" means any information Vendor Processes on behalf of Company in connection with the services it provides to Company under the Agreement that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable person. The specific categories of Personal Data Processed by Vendor are set forth in **Attachment A ("Scope of Processing")**.

"Process" or "Processing" means any operation or set of operations that are performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary or other valuable consideration. A "sale" does not include disclosure of Personal Data to a third party when the applicable data subject uses or directs Company or Vendor, as applicable, to (i) intentionally disclose their Personal Data or (ii) intentionally interact with one or more third parties. "Sale" and its variants may be used uncapitalized in this Addendum for ease of reading.

"Share" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party when such disclosure does not meet the definition of a Sale. "Share" does not include disclosure of Personal Data to a third party when the applicable data subject uses or directs Company or Vendor, as applicable, to (i) intentionally disclose their Personal Data or (ii) intentionally interact with one or more third parties. "Share" and its variants may be used uncapitalized in this Addendum for ease of reading.

2. Obligations of Vendor.

Vendor represents, warrants and covenants that:

a. It will Process Personal Data only for the purpose of fulfilling its obligations under the Agreement and in accordance with Company's written instructions, which are documented in this Addendum, the Agreement and any other writing provided by Company, unless Vendor is required to do otherwise by law. Vendor will inform Company of any legal obligation to Process Personal Data in a manner that differs from Company's instructions prior to such Processing. It will cooperate with and timely respond to all requests to provide an accounting of collection, use and disposal requests made by the Company or its customers, including the implementation and use of Company's data subject access request technology.

b. It will not sell Personal Data.

c. It will Process Personal Data in accordance with all applicable laws and regulations, including but not limited to Applicable Privacy Laws, and will not, by any act or omission, place Company in breach of any applicable law or regulation.

d. If Vendor sells or shares Personal Data to/with Company, Vendor will not sell or share Personal Data for which the applicable data subject has not provided consent for, or has exercised any right to opt out or object to, the sale or sharing of their Personal Data under Applicable Privacy Laws.

e. All Personal Data will be deemed to be owned by the Company and is Company's Confidential Information. Company and all Vendor personnel and permitted subcontractors that Process Personal Data are under a binding obligation to protect the confidentiality and integrity of such Personal Data.

f. It will submit its facilities, networks and systems and its data files and documentation related to the Processing of Personal Data to auditing and/or review by Company or any independent auditor or inspection entity reasonably selected by Company to ascertain compliance with this Addendum upon the request of Company. If such audit or inspection determines that Vendor has not or is not Processing Personal Data in compliance with Applicable Privacy Laws or this Addendum, Company may take actions that, in its sole discretion, are appropriate to stop and/or

remediate Vendor's noncompliant Processing of Personal Data including but not limited to, at Company's sole discretion, immediately terminating the Agreement.

g. It will be fully responsible for any loss or unauthorized access, use, disclosure, alteration or destruction of Personal Data (each, a **"Security Incident"**). Vendor will implement appropriate technical, administrative, organizational and physical safeguards to protect Personal Data against Security Incidents, including but not limited to by taking the following security measures:

(i) Access Controls – policies, procedures, and physical and technical controls: (a) to limit physical access to Vendor's information systems and the facility or facilities in which they are housed to properly authorized persons; (b) to ensure that all members of Vendor's workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; and (c) to authenticate and permit access only to authorized individuals and to prevent members of Vendor's workforce from providing Personal Data or information relating thereto to unauthorized individuals.

(ii) Security Awareness and Training – a security awareness and training program for all members of Vendor's workforce (including management), which includes training on how to implement and comply with the Information Security Program.

(iii) 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.

(iv) 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 Vendor facility, and the movement of these items within a Vendor 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.

(v) 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.

(vi) 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 electronic information while in transit through networks or systems to which unauthorized individuals may have access.

(vii) Secure Disposal – policies and procedures regarding the disposal of Personal Data, and tangible property containing Personal Data, taking into account available technology so that Personal Data cannot be practicably read or reconstructed.

(viii) Assigned Security Responsibility – Vendor shall designate a security official responsible for the development, implementation, and maintenance of its Information Security Program. Vendor shall inform Company as to the person responsible for security.

(ix) Adjust the Program – Vendor shall monitor, evaluate, and adjust, as appropriate, 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 Vendor or the Personal Data, requirements of applicable work orders.

(x) Background Checks – Vendor will perform commercially reasonable criminal background checks on all personnel who will have access to Personal Data prior to hiring such personnel and require such personnel to certify at least annually that they have not been convicted, pled guilty, or pled nolo contendere to any criminal law violation since their background check or prior certification (whichever is later). To the fullest extent permitted by applicable laws and regulations, Vendor will not permit access to Personal Data by personnel who have been convicted, pled guilty, or pled nolo contendere to (i) a felony/indictable crime at any time or (ii) a misdemeanor/summary crime involving fraud, dishonesty, theft, identity theft, embezzlement, or other acts of moral turpitude in the prior seven (7) years.

h. It hereby expressly agrees to submit to the investigatory and jurisdiction of the Office of the Privacy Commissioner of Canada and/or data protection authorities having jurisdiction over the Processing of Personal Data, to the same extent that such investigatory and other jurisdiction would apply to Company.

i. It shall notify Company immediately in writing: (i) in the event that any Personal Data is disclosed by Vendor in violation of the Agreement, this Addendum or Applicable Privacy Laws; and (ii) within twenty-four (24) hours in the event that Vendor discovers, is notified of, or suspects that a Security Incident has occurred, may have occurred, or may occur. Such notice must provide sufficient information to allow Company to report the Security Incident or notify affected individuals as required under applicable law, and must include, at minimum: (a) a description of the Security Incident, a summary of the event(s) that caused the Security Incident, and the date and time of the relevant event(s); (b) the categories and approximate numbers of individuals and Personal Data records concerned; (c) the nature and content of the Personal Data affected; (d) contact information of the data protection officer or other contact point where more information can be obtained; (e) the likely consequences of the Security Incident; and (f) any measures taken to address the Security Incident. Vendor shall cooperate fully in the investigation of the Security Incident, indemnify and reimburse Company for any and all damages, losses, fees or costs (whether direct, indirect, special or consequential) incurred as a result of such incident, and remedy any harm or potential harm caused by such Security Incident. To the extent that a Security Incident gives rise to a need, in Company's sole judgment to provide (i) notification to public authorities,

individuals, or other persons, or (ii) 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 Company's request, Vendor shall, at Vendor's cost, undertake such Remedial Actions. The timing, content and manner of effectuating any notices shall be determined by Company in its sole discretion.

j. Vendor will notify Company immediately in writing in the event that it determines it is no longer able to meet its obligations under Applicable Privacy Laws or this Addendum. Upon receipt of such notice, Company may take actions that, in its sole discretion, are appropriate to stop and/or remediate Vendor's noncompliant Processing of Personal Data including but not limited to, at Company's sole discretion, immediately terminating the Agreement.

k. Vendor will not transfer or Process, or cause to be transferred or Processed, any Personal Data from one jurisdiction to another without Company's prior written consent. Upon Company's request at any time and for any reason, Vendor will immediately stop Processing Personal Data or stop using a subcontractor to Process Personal Data.

l. Vendor shall, upon Company's request, promptly execute supplemental data processing agreement(s) with Company or any of its affiliated companies or take other appropriate steps to address cross-border data transfer requirements or other applicable data protection or privacy laws concerning Personal Data.

m. Vendor will not disclose Personal Data to any third party (including subcontractors) without the prior written consent of Company. Company consents to Vendor's disclosure of Personal Data to subcontractors identified on **Attachment A (Scope of Processing).** Vendor will notify Company of any proposed changes to the subcontractors that it uses to Process Personal Data and give Company the opportunity to object to such changes. In connection with any authorized onward transfer of Personal Data and/or any delegation of Vendor's obligations under this Addendum to a third party, Vendor will (i) require by contract that the third party not disclose Personal Data to any other third party and only Process such Personal Data for the purpose of providing services to Vendor; (ii) contractually impose upon the third party the same data protection obligations that are set forth under this Addendum, including but not limited to the obligation to provide at least the same level of privacy and data security protection for such Personal Data as is required under the Principles; and (iii) be fully liable to Company for the acts or omissions of the third party.

n. Vendor will: (i) immediately notify Company in writing of any complaint or Data Subject Rights Request it receives from a third party with respect to the Processing of Personal Data, (ii) at the direction of Company, promptly cooperate and assist Company in responding to any Data Subject Rights Request; and (iii) upon Company's request, promptly correct, amend, delete or take any other action with respect to Personal Data. Vendor will not respond to any third-party complaint or Data Subject Rights Request unless directed to do so by Company; however, Vendor may refer data subjects to Company's privacy policy if they attempt to submit a Data Subject Rights Request.

o. Vendor will keep and provide to Company, upon request, accurate and up-to-date records relating to the Processing of Personal Data by Vendor.

p. At the direction of Company, cooperate and reasonably assist Company in conducting a data protection impact assessment and related consultations with any supervisory authority, if applicable, to ensure Company's secure Processing of Personal Data.

q. Upon termination of the Agreement, Vendor will return or destroy, at Company's option, all Personal Data in its possession or control unless retention of such Personal Data is required by laws or regulations applicable to Vendor or Company consents to the retention thereof.

r. Vendor will comply with all requirements, including contractual requirements, imposed by Applicable Privacy Laws upon its Processing of Personal Data even if such requirements are not enumerated herein such that Vendor will be deemed a service provider, data processor, or similar entity type under Applicable Privacy Laws with regard to such Processing.

s. Vendor will comply with all applicable information security laws, regulations and industry standards in performance of the Products. If Vendor directly or indirectly in any form whatsoever receives, transmits or retains any credit or debit card data for any reason, Vendor will employ safeguards that, at a minimum, comply with Company's policies and the PCI-DSS. Upon Company's request, Vendor will provide on an annual basis, a SSAE 16 / SOC 1 or 2 or equivalent successor report.

DESIGNER BRANDS

THESHOECOMPANY.CA DSW.CA

Attachment A
Scope of Processing

1. Subject Matter: The context for the Processing of Company Personal Data is Vendor's provision of the services under the Agreement.

2. Duration of Processing: Vendor will Process Company Personal Data until expiration or termination of the Agreement.

3. Nature and Purpose of Processing: Vendor will Process Personal Data for the purpose of providing services in accordance with the Agreement.

4. Categories of Data Subjects: Vendor will Process Personal Data that relates to any and all data subjects about whom Company transfers Personal Data to Vendor, or authorizes Vendor to collect Personal Data regarding, to provide services under the Agreement.

5. Types of Personal Data Processed:

☐ ***Contact Information*** *(e.g., name, email address, phone number, username, password)*

☐ ***Location Data*** *(e.g., postal address, IP address, etc.)*

☐ ***Transactional Data*** *(e.g., purchase history, returns, payment information, etc.)*

☐ ***Preference Data*** *(e.g., profile/account settings such as language, buying pattern, interest in specific topics, etc.)*

☐ ***Employment Data*** *(e.g., title, past/present employers, resume/CV, educational history, professional training, etc.)*

☐ ***Special Categories of Data / Sensitive Personal Data*** *(e.g., social security number, driver's license or other state ID number, passport number, financial account credentials, precise geolocation, data from a known child, content of a data subject's communications (mail, email, text message) when the Company is not the intended recipient of the communications, information revealing racial or ethnic origin, citizenship, immigration status, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation) - if applicable, please describe:* _____

☐ ***Other*** *(e.g., online identifiers, payroll data, system access data, compensation data, etc.) - if applicable, please describe:* _____

6. Contact Details of Vendor's Data Protection Officer or Chief Privacy Officer: [insert]

7. Approved Subcontractors and Data Transfers

Subcontractor Name	Purpose of Subcontracting	Countries where Personal Data is Processed by Subcontractor	Data Transfer Mechanism (if applicable)