<div align="center">

EXHIBIT A
AGREEMENT ON CONFIDENTIALITY - PERSONAL INFORMATION ADDENDUM

</div>

This Personal Information Addendum to Agreement on Confidentiality ("Addendum") is made as of the date of later signature below ("**Addendum Effective Date**"), by and between _____, a _____, having its principal place of business at_____ (hereinafter "**Vendor**") and **DAVID'S BRIDAL, LLC,** a Florida limited liability company, having its principal place of business at 1001 Washington Street, in Conshohocken, Pennsylvania 19428 (hereinafter the "**Company**") and amends that certain Agreement on Confidentiality between the parties ("**Agreement**"). All initially capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Agreement.

WHEREAS, the Parties desire to establish terms governing Personal Information (as hereinafter defined) that may be disclosed by or on behalf of Company;

NOW THEREFORE, in consideration of the covenants and agreements herein contained, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, mutually agree as follows:

1. For purposes of this Addendum, Personal Information means information relating to an identified or identifiable natural person, including without limitation with respect to employees and customers of Company or its affiliates, made available to or accessed by Vendor, whether intentionally or unintentionally, whether through "cookies", Web bugs or other electronic or non-electronic means, whether non-aggregated or aggregated, and whether in written, oral or other form, and any copies thereof. An identifiable person is a person who can be identified, directly or indirectly, by reference to an identification number or factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Examples of Personal Information include, but are not limited to, the following: account number (bank account, credit card, etc.), address, zip code, biometric identifier, certificate or license number, date of birth, government identifiers (such as social security numbers or tax ID numbers), name, personnel number, photograph or video identifiable to an individual, vehicle identifier or serial number, and may also include other information related to an individual that may directly or indirectly identify the individual (e.g. salary, performance rating, purchase history, call history, etc.) or similar information that is otherwise required by applicable law to be protected or secured by Company.

2. The exceptions to the obligations of confidentiality in Section 4 of the Agreement shall not apply to Personal Information.

3. Notwithstanding any expiration or termination of the Agreement, all of the Parties' rights and obligations regarding the Confidential Information that includes Personal Information shall survive any such expiration or termination, and remain in effect.

4. Vendor shall have the following additional obligations with respect to Personal Information.

    a. Vendor shall use Personal Information only for the specific purpose it was provided or made available to Vendor or as otherwise authorized in writing by Company and in compliance with: (i) the Agreement, as amended by this Addendum; (ii) Company's privacy policies; and (iii) all applicable laws, policies and regulations (including but not limited to applicable laws, policies and regulations related to privacy, data security and consumer protection), including without limitation those laws, policies and regulations and standards required thereby that are applicable to Company, but that may not otherwise be directly binding on Vendor, including without limitation the Massachusetts data security regulations (201 Mass. Code Regs. §§ 17.01-17.05).

    b. Vendor will implement and maintain reasonable and appropriate (and in no event less than prevailing industry standard), administrative, technical, and physical safeguards to (i) ensure the security and confidentiality of Personal Information; (ii) protect against anticipated threats or hazards to the security or integrity of Personal Information; and (iii) protect against loss, theft, disposal, unauthorized access, disclosure, copying, use, or modification of Personal Information (except to the extent copying, use or disposal is required under this Agreement or in connection with use of the Personal Information to fulfill Vendor's obligations to Company in connection with the Purpose). These safeguards shall include, without limitation, a written

information security program (to include without limitation information access controls and system protection requirements) and physical, technical, administrative and organizational safeguards for (A) protection of business facilities, paper files, servers, computing equipment, including without limitation all mobile devices and other equipment with information storage capability, and backup systems containing Personal Information; (B) network application (including without limitation databases) and platform security; (C) business systems designed to optimize security and proper disposal of Personal Information; (D) secure storage of data; (E) authentication and access control mechanisms over Personal Information and media, applications, operating systems and equipment used in storing or processing Personal Information; (F) personnel security and integrity, including background checks as consistent with applicable law; and (G) training (at least annually) of Vendor's employees, personnel and/or subcontractors on how to comply with Vendor's physical, technical and administrative information security safeguards. Vendor shall be responsible for all obligations regarding Personal Information contained in this Agreement and may not delegate any obligations with respect to collection, use, disclosure, storage, handling or processing of Personal Information. Vendor shall ensure at all times that Personal Information and all records or other information containing Personal Information that are in the possession of Vendor (in any medium) are kept logically isolated and separate from any information, data, databases or other records stored, handled or processed by Vendor for itself or third parties.

c. Vendor shall limit disclosure of, and access to, the Personal Information solely to such portion thereof and solely to such of its employees on a strict "need to know" basis as required for such employee's performance of his or her duties to Vendor for the performance of Vendor's obligations in connection with the Purpose, and shall not otherwise disclose, transfer, release, sell or otherwise make available Personal Information to any other person or entity. Vendor shall collect, use, process and reproduce Personal Information only to the extent reasonably required for the Purpose. In the event that Vendor receives a request from a third party to access any Personal Information in Vendor's possession, Vendor will promptly forward a copy of such request to Company.

d. Vendor will notify Company in writing immediately after Vendor learns of an actual or suspected loss, misappropriation or unauthorized access to, disclosure, use or modification of Personal Information or PCI DSS Data or other compromise of the security, confidentiality or integrity of Personal Information or PCI DSS Data (collectively, "**Security Breaches**"). Vendor will, at its expense, promptly investigate each actual or suspected Security Breach and assist Company (or third parties engaged by Company for such purpose) in connection with any investigation that Company may desire to conduct with respect to such Security Breach. Vendor will take all reasonable steps, including those requested by Company, to limit, stop or otherwise remedy any actual or suspected Security Breach. Except as otherwise required by law, in the event of an actual or suspected Security Breach, Vendor shall obtain the prior written consent of Company before notifying any third party or any individuals whose Personal Information may have been affected by a Security Breach. PCI DSS Data means any Cardholder Data or Sensitive Authentication Data, as each term is used in the English language Payment Card Industry Data Security Standards.

e. Vendor shall: (i) immediately refer to Company any individual who contacts Vendor seeking access or correction to or with any inquiries or complaints about his or her Personal Information; (ii) immediately notify Company regarding any such request, inquiry or complaint; and (iii) provide, in a timely manner, all reasonable co-operation, assistance, information and access to Personal Information in its possession, custody or control as is necessary for Company to promptly (and, in any event, within any timeframe required by applicable privacy laws) respond to such request, inquiry or complaint.

f. Any Security Breach or any other breach of Vendor's obligations under this Addendum shall constitute a material breach by Vendor of the Agreement.

g. Upon Company's request, Vendor will correct Personal Information in its possession in accordance with Company's instructions.

h. Vendor shall regularly (but in no event less than annually) test and monitor the effectiveness

of its security practices and procedures relating to the Personal Information and will evaluate and adjust its information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Vendor knows or reasonably should know may have a material effect on its information security program. In addition, at any point during the term of the Agreement, upon Company's request, Vendor shall provide to Company a copy of Vendor's security standards, policies and guidelines related to Personal Information.

i.   Vendor shall use encryption or other secure technologies in connection with any transfer, communication or remote access connectivity involving Personal Information, if and as may be permitted or authorized under any applicable agreement with Company. Vendor agrees that Company is the owner of all Personal Information and has the right to direct Vendor in connection with the collection, use, disclosure and retention of Personal Information. Vendor shall not obtain any proprietary rights in any of the Personal Information.

j.   Vendor shall, upon request, provide, in a timely manner, all necessary and reasonable information and co-operation to Company with respect to Vendor's compliance with its obligations under this Addendum and to any regulatory or other governmental bodies or authorities with jurisdiction or oversight over applicable data privacy laws (each, a "**Privacy Regulator**") in connection with any investigations or inquiries made by any such Privacy Regulator under such legislation, including without limitation making available the results of any audits or tests performed on Vendor's information systems or security controls or on any components thereof. Vendor shall permit Company (or a third party chosen by Company) and any Privacy Regulator to audit Vendor's records, procedures, technology implementations and systems, privacy, confidentiality and security controls, and data retention and destruction policies upon reasonable advance written notice and during regular business hours, at Vendor's offices and data centers for the purpose of verifying Vendor's compliance with this Addendum and with such additional data privacy and data security obligations as it may have under any other agreement with Company, and shall, in connection therewith, provide to Company, or any such Privacy Regulator, in a timely manner, all necessary and reasonable information and co-operation. Such audit will be at Company expense unless it reveals a material deficiency or discrepancy, in which case Vendor shall pay for the reasonable expense of such audit and for correction of such deficiency or discrepancy. Upon request by Company, but not more frequently than once per calendar year during the term of the Agreement, Vendor shall deliver to Company a statement signed by Vendor certifying in writing that Vendor has, in respect of the previous twelve month period: (i) developed privacy compliance processes designed to ensure its compliance with the terms of the Agreement, as amended by this Addendum or that such processes previously developed remain in effect; and (ii) complied in all material respects with the requirements of the Agreement, as amended by this Addendum.

k.   Vendor will retain any Personal Information only for so long as necessary for Vendor to fulfill its obligations to Company, and shall thereafter promptly return or (if so instructed by Company in writing) destroy all originals and copies of such Personal Information and certify such destruction in writing to Company. The deletion of such Personal Information shall result in the complete destruction or erasure thereof, so that such Personal Information cannot be practicably read or reconstructed.

l.   Vendor shall designate and identify to Company an individual responsible for the handling of all Personal Information.

m.   Vendor shall comply with the English language Payment Card Industry Data Security Standards in effect from time to time, as issued by the PCI Security Standards Council and with all applicable laws and regulations governing the collection, storage and use of PCI DSS Data furnished or made available to Vendor.

n.   Vendor will collect, store and use solely in the United States all Personal Information and PCI DSS Data furnished or made available to it, and will not transfer such Personal Information or PCI DSS Data to any other country for any purpose without the prior written authorization of Company.

o. Vendor hereby agrees to defend, indemnify and hold harmless Company and its affiliates and subsidiaries from and against any and all damages, losses, liabilities, settlements and expenses (including without limitation costs and attorneys' fees) in connection with any third-party demand, claim or action that arises from an alleged breach by Vendor of the Agreement, as amended by this Addendum, in connection with or relating to any Personal Information or PCI DSS Data furnished or made available to Vendor or its obligations under this Addendum. This Section shall survive any expiration or termination of the Agreement.

p. Vendor represents, warrants and covenants that as of the date hereof and at all times throughout the term of the Agreement, Vendor shall, with respect to all Personal Information and other data, however recorded, about an identified or identifiable individual that Vendor shall protect, maintain, process, store and delete such information in accordance with applicable laws, including but not limited to: the EU General Data Protection Regulation (including its iterations by virtue of adoption individual member states and former member states); the Standard Contractual Clauses; Personal Information and Protection and Electronic Documents Act; and the California Consumer Protection Act; and the California Privacy Rights Act.

5. This Addendum together with the Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and supersedes or replaces any prior similar understandings or agreements between the parties whether oral or written. Those provisions of the Agreement not explicitly changed or overridden by this Addendum shall remain in full force and effect. This Addendum may be amended or modified only in writing, signed by an authorized representative of each Party. This Addendum shall be binding upon and inure to the benefit the Parties and their respective successors and assigns. This Addendum may be executed in counterparts and delivered by facsimile or other electronic means, each of which shall be deemed to be an original and all of which when taken together shall constitute one and the same agreement.

IN WITNESS WHEREOF, the undersigned, representing that they have the requisite organizational power and authority on behalf of their respective entities, have caused this Addendum to Agreement on Confidentiality to be executed, as of the Addendum Effective Date, as the valid and binding act of their respective entities.

_____	**DAVID'S BRIDAL, LLC**

By: _____	By: _____

Name: _____	Name: _____

Title: _____	Title: _____