Data Processing Addendum

Last Updated: June 13, 2024

This Data Processing Addendum ("DPA") forms an integral part of the Halcyon Death Care Management System ("DCMS") Terms of Service and any Order Form (collectively, the "Agreement") between Batesville Casket Company, LLC, an Indiana limited liability company ("Provider"), and the funeral home, crematory, multi-funeral home or crematory entity, or other entity that enters into the Agreement with Provider (the "Company"). For purposes of this DPA, Company and Provider may each be referred to as a "party" and collectively as the "parties." This DPA applies only to the extent that: (i) Provider has access to, or otherwise Processes, Company PI for, or on the behalf of, Company pursuant to the Agreement; and (ii) Company is subject to a Data Protection Law. This DPA is intended to supplement the Agreement and in the event of a conflict between this DPA and the Agreement, the terms and conditions set forth in this DPA shall supersede and control with respect to the conflict. For the avoidance of doubt, the terms or conditions set forth in the Agreement that are not otherwise addressed herein shall remain in full force and effect.

1. Definitions. For purposes of this DPA, the following terms shall apply:

California Consumer Privacy Act (CCPA)	means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CPRA) and other applicable amendments thereto and includes all applicable implementing regulations.
Claim Costs	shall mean and include costs incurred by Company in respect of claims that allege injury or damage by reason of Provider's release, loss, or unauthorized use or disclosure of any Company PI.
Company PI	means Personal Information, in any form or format, that Provider has access to, or otherwise Processes, for, or on the behalf of, Company pursuant to the Agreement and Services rendered thereunder.
Data Protection Law	means all laws, statutes, and regulations applicable to the Processing of Company PI, including the CCPA, the Colorado Data Privacy Act, the Connecticut Data Privacy Act, the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.
Data Subject	means the natural person whose Personal Information is Processed by Provider.
Documented Instructions	means the Processing terms and conditions set forth in the Agreement and this DPA.
Information System	means any information or telecommunication system, network, equipment, hardware, or software employed or otherwise used with respect to the Processing of Company PI.
Notification Costs	shall mean and include any and all verifiable costs (including, without limitation, attorneys' fees) incurred by Company in investigating whether notification of individuals is required and the preparation and delivery of any appropriate notices to individuals and the provision of appropriate credit monitoring services.
Personal Information	means any information or data that, alone or in combination with other information or data, can be used to reasonably identify a particular individual, household, or device, and is subject to, or otherwise afforded protection under, an applicable Data Protection Law.
Process	means any action performed on Company PI, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure,

	transfer or otherwise making available, alignment or combination, restriction, deletion, or destruction.
Security Event	means any unauthorized access to, or unauthorized loss, use, acquisition, exfiltration, or disclosure of unencrypted Company PI. A Security Event does not include an Unsuccessful Security Incident.
Sell and Sale	shall be ascribed the meaning set forth in the CCPA.
Share or Sharing	shall be ascribed the meaning set forth in the CCPA.
Services	means the technology, or consulting services, or other products, goods, or services that Provider furnishes to Company pursuant to the Agreement.
Subprocessor	means any third party engaged by Provider to Process Company PI on its behalf.
Unsuccessful Security Incident	means an unsuccessful attempt or activity that does not compromise the security of Company Personal Information, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

2. Data Protection

2.1. General Obligations. As between the parties, Company shall, at any and all times, retain all rights, title, and interest in Company PI. Company hereby appoints Provider and its affiliates to Process Company PI on Company's behalf and grants Provider and its affiliates a worldwide, non-exclusive, sublicensable, royalty-free license to Process the Personal Information in accordance with the Documented Instructions and as otherwise set forth herein. In the event Provider is compelled by law to Process Company PI beyond, or in conflict with, the Documented Instructions, Provider shall notify Company of the same prior to such Processing, unless such prior notification is expressly prohibited by law. Additional Processing by Provider outside the Documented Instructions, if any, will require prior written agreement between Provider and Company.

2.2. CCPA/CPRA Disclaimer. Each party acknowledges and agrees that the disclosure of Company PI to the other does not constitute, and is not the intent of either party for such disclosure to constitute, a Sale or Sharing of Company PI, and if valuable consideration, monetary or otherwise, is being provided by either party, such valuable consideration, monetary or otherwise, is being provided for the rendering of Services and not for the disclosure of Company PI. Provider (i) shall not collect, retain, use, or disclose Company PI for any purpose (including for any commercial purpose) other than for the specific purpose of performing the Services, unless otherwise required by law, (ii) shall not Sell or Share Company PI, except as necessary to satisfy its obligations under the Agreement, (iii) shall not collect, retain, use, or disclose Company PI outside the direct business relationship between Provider and Company, unless expressly permitted by law, (iv) shall not combine the Company PI that the Provider receives from, or on behalf of, Company with Personal Information that Provider receives from, or on behalf of, another party, or collects from its own interaction with a Data Subject, except to the extent reasonably necessary to provide the Services and as expressly permitted by law, and (v) shall, at Company's reasonable request, cease any unauthorized Processing of Company PI and grant Company authorization to assess and remediate any such unauthorized Processing. This DPA is Provider's certification, to the extent the CCPA or any other applicable Data Protection Law requires such a certification, that Provider understands and will comply with the Processing limitations with respect to Company PI that are set forth in the Documented Instructions. The parties acknowledge and agree that Provider shall Process Company PI only for the specific "business purpose" of performing the Services set forth in the Agreement.

3. Confidentiality and Information Security

3.1. Confidentiality. Provider shall maintain the confidentiality of all Personal Information and ensure that individuals who are authorized to Process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2. Information Security. Provider shall implement and maintain commercially reasonable technical and organizational security controls to protect and safeguard Personal Information, which shall include written policies describing its security controls and measures and the relevant procedures and responsibilities of Provider personnel who have access to Personal Information (**"Information Security Program"**). Provider shall designate a senior employee to be responsible for the overall management of Provider's Information Security Program. The Information Security Program shall include the security controls set forth in Security and Privacy Documentation.

3.3. Updates. Provider may update, amend, or otherwise alter its Information Security Program at any time and without notice to Company, provided that any such update, amendment, or alteration does not increase the likelihood of a Security Event or cause the Information Security Program to not meet the minimum standards set forth herein.

4. Cooperation and Assistance; Return of Company PI

4.1. General Assistance. Provider shall provide reasonable assistance to Company to assist Company to (i) comply with its obligations and responsibilities under any applicable Data Protection Law, including with respect to Data Subjects exercising their rights and privileges under applicable Data Protection Laws, (ii) upon Company's request and at Company's sole cost and expense, undertake data protection impact assessments, and (iii) comply with requests or demands from supervisory authorities.

4.2. Data Notice and Response. Provider shall, to the extent legally permitted, promptly refer to Company any correspondence, inquiry, complaint, request, or demand (collectively or individually, a "Data Notice") concerning the Processing of Company PI and shall not respond to any such Data Notice unless otherwise required by law. Notwithstanding the foregoing, in response to any such Data Notice, Provider may furnish Company's email contact information and request the Data Notice be submitted directly to Company. Upon written request from Company, Provider shall promptly amend, correct, delete, or cease Processing, Company PI in its custody or control. Company shall be responsible for any costs arising from Provider's provision of such assistance described herein. For the avoidance of doubt, Company shall be fully responsible and liable for timely and appropriately responding to a Data Notice.

4.3. Return or Destruction of Company PI. On termination or expiration of the Agreement, Company may wish to instruct Provider to delete or return all Company PI (including copies) from Provider's systems in accordance with applicable Data Protection Law. Provider will, after a recovery period of up to thirty (30) days following expiry or termination of the Agreement, comply with this instruction as soon as reasonably practicable, where technically feasible. Company shall be responsible for retrieving any remaining Company PI it wishes to retain before the end of the recovery period. Provider shall not be required to delete or return Company PI to the extent that Provider is required by applicable law or order of a governmental or regulatory body to retain some or all of the Company PI or such Personal Information is required for Provider to enforce or defend its legal rights or interests. In addition, except to the extent required by applicable law, Provider shall not be required to delete or return Personal Information archived on back-up systems if Provider shall securely isolate it and protect it from any further Processing and such Personal Information is deleted in accordance with Provider's standard overwriting and deletion policies.

5. Security Event Procedures. Provider shall promptly provide any and all legally required notices to Company of any Security Event promptly after becoming aware of, or otherwise discovering, the Security Event, and this written notification shall, to the greatest extent possible,

include a description of (i) the nature of the Security Event, (ii) the categories of Company PI affected by the Security Event, (iii) the approximate number of individuals affected by the Security Event, (iv) any potential legal or regulatory consequences that may arise from the Security Event, and (v) the measures taken or proposed to be taken to address the Security Event. In the event of a Security Event, Provider shall designate a senior employee to serve as Provider's single point of contact from whom Company can obtain more information about the Security Event. Notwithstanding any other provision in the Agreement or herein, Provider shall reimburse Company for Notification Costs and Claim Costs as described herein arising from a Security Incident or other breach in the security of any Company PI. Any notification, assistance, or cooperation provided by Provider in accordance with this Section 5 shall not be interpreted or construed as an admission of liability, wrongdoing, or fault of Provider.

6. Audits. Provider shall (i) upon request (but not more frequently than annually) respond to questionnaires and similar requests for information provided by Company to demonstrate Provider's compliance with Provider's obligations under this DPA, and (ii) periodically use independent external auditors to verify the adequacy of its written Information Security Program.

7. Subprocessing; Localization

7.1. Subprocessors. Company hereby acknowledges and agrees that Provider may engage Subprocessors to assist with its provision of Services to Company, provided Provider executes with any such Subprocessor a written agreement that contains terms and conditions that are substantially the same as, and in any event no less stringent than, the terms and conditions set forth in this DPA. Provider shall undertake all reasonable efforts to ensure that any such Subprocessor can comply, and is in compliance, with the terms and conditions set forth in this DPA. Provider shall, at any and all times, remain liable to Company for any and all acts or omissions of a Subprocessor. For the avoidance of doubt, Provider shall ensure that any and all obligations and responsibilities applicable to Provider pursuant to this DPA shall apply to any and all Subprocessors.

7.2. Localization. Unless otherwise agreed to in writing by Company, Provider shall at any and all times retain Company PI on Information Systems that are located in the United States of America.

8. Limitation of Liability. Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement and the applicable cap (maximum) for the relevant party set forth in the Agreement. For the avoidance of doubt, Provider and its affiliates' total liability for all claims from Company and all of Client's affiliates and Authorized Users arising out of or related to the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA. To the extent required by law, (i) this section is not intended to modify or limit either party's liability for Data Subject claims made against a party where there is joint and several liability, or (ii) limit either party's responsibility to pay penalties imposed on such party by a regulatory authority.

9. Miscellaneous. This DPA will be governed by and construed in accordance with the governing law, venue, and jurisdictional provisions set forth in the Agreement. In the event no such provisions exist, then this DPA shall be governed by and construed in accordance with the laws of Indiana, any legal claim, action, or dispute arising from this DPA shall be made and resolved in the federal or state courts of Indiana. References in this DPA to "writing" or "written" include e-mail communications and certified mail.

****