ALLVUE

DATA PROTECTION ADDENDUM

Version Date: March 1, 2025

This Data Protection Addendum (this "**DPA**") forms a part of, and is subject to, the Master Subscription and Services Agreement or other written hosted services agreement (in each case, as amended, the "**Master Agreement**") between Allvue Systems, LLC ("**Allvue**") and the entity or entities defined as 'Customer' thereunder (collectively and individually referred to herein as "**Customer**", and together with Allvue, the "**Parties**", and each, a "**Party**") in which this DPA is referenced; the Master Agreement, together with the DPA and the other Subscription Contracts, may be collectively referred to as the "**Agreement**."

1. DEFINITIONS

1.1 Unless otherwise expressly set forth in this DPA: (a) all defined terms used in this DPA shall have the same meaning ascribed to such terms in the Master Agreement; and (b) terms and phrases defined in the GDPR or the CCPA (each as defined below) shall have the meanings ascribed to such terms therein when used in this DPA.

1.2 "**CCPA**" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations.

1.3 "**Data Breach**" means accidental or unlawful destruction, loss or alteration, or unauthorized disclosure, of or unauthorized access to Personal Data.

1.4 "**Data Protection Legislation**" means the GDPR, the Data Protection Act 2018, the CCPA, Other US Privacy Laws or any other applicable data protection laws applicable to the Processing of Personal Data under the Master Agreement, including any amendment, consolidation, replacement or re-enactment thereof.

1.5 "**Data Subject**" means: (a) where the GDPR is the Data Protection Legislation, a "data subject" as defined in the GDPR; or (b) where the CCPA is the Data Protection Legislation, "consumer" as defined in the CCPA; or (c) where any other Data Protection Legislation applies, a natural person to whom Personal Data relates.

1.6 "**GDPR**" means, as applicable: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**EU GDPR**"); or (b) EU GDPR as it forms part of the laws of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**").

1.7 "**Other US Privacy Laws**" means the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act and other similar laws of the United States regulating the Processing of Personal Data.

1.8 "**Personal Data**" means: (a) where the GDPR is the Data Protection Legislation, "personal data" as defined in the GDPR; (b) where the CCPA is the Data Protection Legislation, "personal information" as defined in the CCPA; or (c) where any other Data Protection Legislation applies, information that relates to an identified or identifiable natural person, but in each case only to the extent that such Personal Data, or any part thereof, is processed through the Processing Activities.

1.9 **"Processing"** or **"Processing Activities"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as 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 under the Agreement.

1.10 "**Supervisory Authority**" means: (a) where the GDPR is the Data Protection Legislation, a "supervisory authority" as defined in the GDPR; (b) where the CCPA is the Data Protection Legislation, the California Attorney General or such other governmental authority authorized to enforce the CCPA; or (c) where other Data Protection Legislation is applicable, the governmental body charged with the enforcement thereof.

2. APPLICABILITY; CONSTRUCTION

2.1 This DPA governs the processing of Personal Data on Customer's behalf in connection with the Agreement that Customer uploads, transmits, provides, or otherwise makes available to Allvue for processing on Customer's behalf in connection with the obligations, terms, and services under the Agreement.

2.2 For purposes of this DPA: (a) the words "include," "includes" and "including" (and all cognates) are deemed to be followed by the words "without limitation"; (b) the word "or" is not exclusive; (c) the words "herein," "hereof," "hereby," "hereto" and "hereunder" refer to this DPA as a whole; (d) words denoting the singular have a comparable meaning when used in the plural, and vice versa; and (e) words denoting any gender include all genders.

3. PROVISIONS OF GENERAL APPLICABILITY

3.1 **Customer's Instructions:** Customer hereby appoints Allvue to process the Personal Data as set forth below. The Parties hereby agree that the Agreement sets out the instructions to Allvue for all Processing of Personal Data. Customer shall limit the scope of the Personal Data processed hereunder as reasonably prudent.

Subject matter of processing	The subject matter of the Processing is Personal Data.
Duration	For the Term and as otherwise reasonably necessary to comply with the terms and conditions of the Agreement or applicable law, including the Data Protection Legislation.
Nature and purpose of processing	Processing of Personal Data as reasonably necessary to perform the services and obligations and exercise the rights described in the Agreement, and to comply with Customer's Processing instructions as provided in the Agreement, or as Customer may otherwise provide to Allvue from time to time.
Categories of Data Subjects	Categories of Data Subjects to which Personal Data relate are determined and controlled by Customer in its sole discretion, and may include Customer's employees, contractors, agents, end users or other third parties that use Allvue's products or services on behalf of or in connection with the business of the Customer (or employees, agents or customers of such third parties) (collectively, the "**Impacted Data Subjects**")
Categories of Personal Data	The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include contact information (name, business entity, address, telephone number (fixed and mobile), e-mail address, fax number), employment details (job title, employer), username, geographic location, area of responsibility and IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data).
Sensitive Data	Allvue does not intentionally collect or process any Special Categories of Personal Data or criminal offences Personal Data in the provision of the Processing Activities. The Parties agree that if, for any reason (including the provision, transmission, or making otherwise available of such Personal Data from Customer or its Authorized User to Allvue), Allvue does process any such Personal Data in the Processing Activities, Customer: (a) shall notify Allvue in writing that it will be providing or transmitting such Personal Data to Allvue; (b) shall ensure that it has in place all necessary lawful bases and conditions for such processing in accordance with the relevant Data Protection Legislation; and (c) undertakes that Allvue shall not be in breach of Data Protection Legislation in respect of such processing (provided that such processing is otherwise undertaken in accordance with this DPA). Schedule 2 of the DPA shall apply to all Processing Activities including those mentioned herein.

Restricted Transfers (as defined below) and Transfers to subprocessors:	Allvue shall conduct Restricted Transfers in accordance with Section 4.5 of the DPA, and Customer understands the frequency shall be continuous in connection with the Allvue's contractual obligations to Customer and for any additional period as is required by applicable law. Allvue shall utilize subprocessors with Restricted Transfers in accordance with Section 4.4 of the DPA.

3.2 Each Party shall comply with all laws, rules and regulations applicable to it in connection with the performance of its obligations set forth herein, including the Data Protection Legislation, and in the case of Customer: (a) any instructions Customer issues to Allvue under the Agreement shall comply therewith; and (b) Customer shall ensure that it has the right to transfer, or provide access to, the Personal Data to Allvue for the Processing Activities.

3.3 Allvue shall notify Customer in writing of a confirmed Data Breach impacting the Customer without undue delay after becoming aware of such Data Breach, and in any event within forty-eight (48) hours after becoming aware of such Data Breach. Such notification shall provide reasonable and timely information as required by Customer to fulfill any reporting obligations it may have under the Data Protection Legislation (and in accordance with the timescales required thereby), including to the extent available, the nature of the Data Breach, the approximate number of Data Subjects concerned, the categories of Personal Data affected thereby and the magnitude and likely consequences thereof. Allvue shall take all reasonable measures to remedy or mitigate the effects of the Data Breach and shall keep Customer reasonably informed of developments in connection therewith. Allvue's notification of, or response to, a Data Breach shall not constitute an acknowledgement by Allvue of any fault or liability with respect to the Data Breach.

3.4 Allvue shall (a) ensure that any person that it authorizes to process the Personal Data (including its or its Affiliates' staff, agents, subprocessors) (an "**Authorized Person**") shall be subject to a strict duty of confidentiality (whether a contractual, statutory or other professional duty), and (b) ensure that all Authorized Persons process, and have access to, the Personal Data only as necessary for the purposes permitted hereunder and in compliance with all obligations of Allvue as if such Authorized Persons were a party hereto.

3.5 Taking into account the nature of the processing, Allvue shall provide all reasonable and timely assistance to Customer to enable Customer to respond to: (a) any request from a Data Subject to exercise any of his or her rights under the Data Protection Legislation (including his or her rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, inquiry, order or complaint received from a Data Subject or Supervisory Authority in connection with the processing of its Personal Data. In the event that any such request, correspondence, inquiry, order or complaint is made directly to Allvue (or any subprocessor of Allvue of which Allvue becomes aware), Allvue shall promptly inform Customer thereof, providing details of the same and, to the extent legally permissible, refrain from, or use commercially reasonable efforts to cause the applicable subprocessor to refrain from, responding to the foregoing (unless for the limited purpose of informing the Data Subject that the request has been forwarded to Customer or to acknowledge receipt of the request) except upon written instructions from the Customer or as required under applicable laws (in which case, Allvue shall notify Customer of such requirement).

3.6 Promptly after termination or expiration of the Master Agreement and after written request by Customer, Allvue shall take reasonable measures to destroy or return all Personal Data in its possession or control except as otherwise required to comply with applicable laws, including the Data Protection Legislation.

3.7 The Parties hereby submit to the choice of law and jurisdiction set forth in the Master Agreement with respect to any disputes or claims howsoever arising under this DPA, including all contractual, non-contractual or other obligations arising out of or in connection herewith.

3.8 Any claims related to a breach of a term of this DPA or the Standard Contractual Clauses (or "**SCCs**", as defined below) shall be subject to the terms and conditions, including the exclusions, waivers and limitations (including all

limitations of liability and waivers of damages) set forth in the Master Agreement, which are hereby incorporated herein by reference. The Parties' execution of the Master Agreement shall constitute valid execution of this DPA.

3.9 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either: (a) deemed amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible; or (b) if this is not possible, construed in a manner as if the invalid or unenforceable part had never been included such that the remaining part may be enforceable.

4. GDPR PROVISIONS AND OBLIGATIONS

4.1 The Parties hereby agree that: (a) the terms and conditions set forth in this Section 4 apply where the GDPR is the governing Data Protection Legislation that applies to the Personal Data processed hereunder; and (b) the Customer shall be the "controller" and Allvue shall be the "processor" as defined in the GDPR.

4.2 Allvue shall, in relation to the Processing Activities, take all technical and organizational measures (together, the "**Processing Security Measures**"), as detailed in Schedule 2, required to comply with Article 32 of the GDPR, to protect the Personal Data from a Data Breach and to ensure a level of security in respect of the Personal Data that is appropriate to the risk associated with the Processing Activities. In order to ensure compliance with its obligations under this Section, Allvue shall throughout the Term, continuously monitor and evaluate the Processing Security Measures taking into account associated risks. Customer is, in relation to the Personal Data, responsible for and ensures the lawful basis of processing.

4.3 Allvue shall make available to Customer, or an auditor mandated by Customer, written information reasonably necessary to assess or demonstrate Allvue's (and its subprocessors') compliance with the Data Protection Legislation with respect to the Processing Activities, which shall be completed by written questionnaire to the extent commercially practicable. If an on-site audit or inspection is expressly required under the Data Protection Legislation or by the applicable Supervisory Authority with respect to the Processing Activities, Customer shall submit an advance written request with respect thereto (unless prohibited from doing so by the Data Protection Legislation), and after the Parties have agreed on the start date, scope and duration of, and security and confidentiality controls applicable to, such audit or inspection, Allvue shall allow and contribute to such audit or inspection, which shall be at Customer's sole cost and expense (at Allvue's then-current hourly professional services rate), except where any such audit or inspection is required due to a material breach by Allvue of its obligations under this DPA or the Master Agreement or reveals such a material breach, provided that:

(a) Customer shall: (i) give Allvue reasonable advance written notice of such audit or inspection to be conducted; and (ii) use (and ensure that each of its mandated auditors makes) commercially reasonable efforts to: (A) avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the applicable premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection; and (B) conduct the audit or inspection during normal business hours; and

(b) notwithstanding anything to the contrary: (i) Allvue shall only be required to grant access to physical locations or provide documentation to the extent that it controls such facilities or documentation or has the right to grant access thereto under its contracts with the relevant subprocessor (which Allvue shall use commercially reasonable efforts to facilitate); and (ii) in no event shall Allvue be contractually required to permit any audit or other activity that may compromise, jeopardize or otherwise adversely impact the security, confidentiality, operability or integrity of services that Allvue provides to other customers or disclose any internal accounting or financial information or trade secrets of Allvue.

4.4 **Subprocessors**: Customer and Allvue agree that Allvue shall have a general authorization to engage subprocessors for the processing of Personal Data under the Agreement, subject to this Section 4.4, including Allvue's current subprocessors listed at https://www.allvuesystems.com/legal-terms/data-privacy/subprocessor-list.pdf ("**Subprocessor Site**"). Customer hereby agrees and consents to Allvue engaging additional subprocessors provided

that Allvue provides advance notice to customer of the use of such subprocessor as further described on the Subprocessor Site. Customer has the right to reject any such additional subprocessor within fifteen (15) days of such notice. In respect of any subprocessor engaged by Allvue, Allvue shall: (a) impose data protection and processing terms on that subprocessor that protect the Personal Data and the processing thereof to the same standard provided for by this DPA and that otherwise meet the requirements of Article 28 of the GDPR; (b) if such contract will involve a Restricted Transfer, utilize a Permitted Measure (as defined below) for such Restricted Transfer; and (c) remain fully liable for any breach of this DPA that is caused by an act, error or omission of such subprocessor. If Customer refuses to consent to Allvue's appointment of a subprocessor on reasonable grounds relating to the protection of the Personal Data, then the Parties shall work together in good faith to make a commercially reasonable change in the provision of the Services which avoids the use of that proposed subprocessor.

4.5 **Cross-Border Transfers**: Customer hereby agrees that to the extent that Allvue and its Affiliates transfer Personal Data on a global basis as necessary to meet the terms under the Agreement, this Section 4.5 shall apply. With respect to transfers of Personal Data from Customer subject to the EU GDPR or the UK GDPR, Allvue shall only make transfers outside of the EEA or UK, respectively ("**Cross-Border Transfers**"), as follows:

(a) to a country that has been designated by the applicable Supervisory Authority or Data Protection Legislation as providing an adequate level of protection for Personal Data ("**Adequacy Decision**"), or

(b) to a country without an Adequacy Decision ("**Restricted Transfer**"):

(i) The Parties agree to abide by the terms of the EU Standard Contractual Clauses (as amended from time to time, "**EU SCCs**" for Personal Data subject to the GDPR) and the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (as amended from time to time, "**UK SCCs**" for Personal Data subject to the UK GDPR), collectively the "**SCCs**," which are incorporated by reference and form an integral part of this DPA and which shall apply in accordance with Schedules 1 and 2, with Allvue as the "data importer" and Customer as "data exporter"); or

(ii) Allvue will make such Restricted Transfer utilizing another lawful safeguard as permitted and defined under the applicable Data Protection Regulation (Article 46 of the GDPR and UK GDPR) (collectively with the SCCs, the "**Permitted Measures**").

4.6 **Impact Assessment**: Allvue shall upon Customer's reasonable request, and within an agreed time frame, provide reasonable assistance to Customer in the performance of a data protection impact assessment required by the GDPR. Allvue shall provide up to five (5) hours' worth of assistance under this Section 4.6. Any additional assistance shall be at Customer's sole cost and expense (at Allvue's then-current hourly professional services rate).

4.7 Where Allvue is required by applicable law to process any Personal Data, other than in accordance with Customer's instructions, Allvue shall inform the Customer of that legal requirement before undertaking such processing, unless prohibited by applicable law on important grounds of public interest.

5. US PRIVACY LAW OBLIGATIONS

5.1 **Personal Data subject to the CCPA**. With respect to Consumers under the CCPA, Customer is the "Business" and Allvue is the "Service Provider" as defined under the CCPA. Customer ensures and represents that all consumers' Personal Data were collected in accordance with the CCPA and that Customer has the lawful right to transfer such Personal Data to Allvue, and: (a) Allvue will not retain, use, combine or disclose Personal Data for any purpose other than for the limited and specific purposes outlined in Section 3.1, as otherwise agreed to in writing by Allvue and Customer or as permitted by CCPA; (b) Allvue shall not "sell" or "share" Personal Data, as such terms are defined by CCPA, or retain, use or disclose the Personal Data outside of the direct business relationship with Customer; (c) Allvue will only retain, use, or disclose Personal Data for "business purposes," as defined by CCPA, as authorized by the Agreement or as otherwise permitted by the CCPA; (d) Allvue will not retain, use, or disclose Personal Data for any "commercial purposes" other than the "business purposes" (as these terms are defined by CCPA) specified in the

Agreement, unless expressly permitted by CCPA; (e) Allvue will comply with applicable provisions of CCPA and provide the same level of privacy protection for Personal Data as required by CCPA; (f) Customer has the right to take reasonable and appropriate steps to help ensure that Allvue uses Personal Data in a manner consistent with Customer's obligations under CCPA as a Business; (g) Allvue will notify Customer if Allvue makes a determination that it can no longer meet its obligations under CCPA; (h) Customer will have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of its Consumers' Personal Data by Allvue; and (i) Allvue will take actions reasonably necessary for Customer to comply with privacy requests made pursuant to CCPA, including requests to delete, correct or access Personal Data.

5.2 **Other United States Privacy Laws**. Allvue and Customer agree to the following, to the extent required by such applicable Other US Privacy Laws: (a) Allvue shall make available to Customer such readily accessible information in its possession necessary to demonstrate compliance with its obligations under Other US Privacy Laws; (b) Allvue shall allow reasonable audits and inspections in connection with its obligations under this DPA and the Agreement in accordance with Section 4.3; and (g) Allvue may engage additional subprocessors in accordance with Section 4.4.

* * * * *

Schedule 1

The EU SCCs shall apply pursuant to Section 4.5 of the DPA as follows:

1. Module 2 shall apply.
2. Clause 7 and Option 2 (in accordance with Section 4.4. of the DPA) of Clause 9 shall apply.
3. The Irish Data Protection Commission, the law of Ireland, and Ireland shall apply accordingly in Clause 13(a), Clause 17 (Option 2 applies), Clause 18(b), and Section C of Annex I of the EU SCCs.
4. Section A of Annex I of the EU SCCs shall be populated with Party information from the Recitals, the contact information in the Agreement, and reference to the table in Section 3.1 of the DPA.
5. Section B (Description of Transfer) of Annex I of the EU SCCs shall be populated by the table in Section 3.1 of the DPA.
6. Annex II of the EU SCCs shall be populated with Schedule 2 of the DPA.

Part 1 of the UK SCCs shall apply pursuant to Section 4.5 of the DPA as follows:

1. Table 1 of the UK SCCs shall be populated with Party information from the Recitals and the contact information the Agreement, and the Start Date is the Effective Date of the Master Agreement.
2. In Table 2 of the UK SCCs, the version of the Approved EU SCCs and its related information in this Schedule 1 supplements the UK SCCs.
3. Table 3 shall be populated with the information regarding the EU SCCs in this Schedule 1.
4. In Table 4, both parties are selected.

The Parties' execution of the Master Agreement shall constitute valid execution of the SCCs.

Schedule 2

TECHNICAL AND ORGANISATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and Organizational Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Allvue leverages well-known encryption technologies and algorithms to protect data at rest and in transit. All underlying cloud systems are encrypted using one of many methods depending on the type and location of the system, to include Bitlocker full disk encryption (AES-128) and cloud-based encryption of all system volumes used, and certificate-based encryption of all database backups. All data in transit is encrypted using TLS 1.2 with only secure ciphers (128 bits or greater) for end user access to Allvue applications. Additionally, limited data masking is available for chosen fields.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Allvue's information security program has been created to align with general cybersecurity principles that focus on awareness and proactive data-driven detection vs. a traditional reactive security model. Allvue has a security awareness training program, phishing simulation and reporting capability, and a central information hub to facilitate awareness. Allvue has various measures to ensure it has the proper visibility into its employees, devices, systems, and networks to facilitate monitoring, detection, and action/response. Allvue has detailed disaster recovery and continuity procedures in place to ensure that its systems remain available and possibility of data loss is severely limited to facilitate recovery.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Allvue has Business Continuity and Disaster Recovery Plans in place to ensure all resources can adequately continue operations during an incident affecting their availability. Disaster Recovery testing is conducted annually, and all gaps identified during testing are documented for remediation, prioritized for remediation, assigned to a member of the IT team for resolution, and all documentation is updated accordingly.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Allvue undergoes various third-party and internal audits to include annual penetration test and vulnerability scans on its applications by a trusted third-party vendor and annual SSAE 18 SOC 1 and SOC 2 audits. Allvue also performs annual disaster recovery and incident response testing. Additional audits and reviews are performed as needed on an informal and ad-hoc basis.
Measures for user identification and authorization	Access to all applications is protected via unique usernames and passwords, with available MFA options.
Measures for the protection of data during transmission	All data in transit is encrypted using TLS 1.2 with only secure ciphers (128 bits or greater) for end user access to Allvue applications.

Technical and Organizational Measure	Details
Measures for the protection of data during storage	All underlying cloud systems are encrypted using one of many methods depending on the type and location of the system, to include Bitlocker full disk encryption (AES-128) and cloud-based encryption of all system volumes used, and certificate-based encryption of all database backups.
Measures for ensuring physical security of locations at which personal data are processed	All data is stored in our IaaS partner's data centers, and Allvue inherits their world-class physical security controls.
Measures for ensuring events logging	Allvue has a SIEM in place where all system and user logs are aggregated for storage, correlation, and analysis.
Measures for ensuring system configuration, including default configuration	The Allvue hosted offering abides by strict change management processes and policies where configuration changes, software upgrades, system/security patches, etc. are applied and tested in lower tier environments, prior to being released to production environments.
Measures for internal IT and IT security governance and management	Allvue has a dedicated infosec team responsible for all aspects of information security.
Measures for certification/assurance of processes and products	Allvue undergoes annual SOC 1 and SOC 2 audits. Allvue's product development team executes extensive manual and automated functional, unit, stress, and performance testing on major Allvue software releases prior to making those versions available for its client environments. Additionally, Allvue's Hosting and Implementation teams design, maintain and execute client-specific test scenarios to be executed prior to major Allvue software releases to address critical customer functionality that may be unique to a client's implementation.
Measures for ensuring data minimisation	Allvue acts as the data processor and only processes data provided directly by its customer.
Measures for ensuring data quality	Allvue acts as the data processor and only processes data provided directly by its customer. Once data is within the system, Allvue security controls ensure data confidentiality and integrity is maintained.
Measures for ensuring limited data retention	Allvue retains data while services are being delivered, and stores backups for a default of one year. Upon contract termination, Allvue follows its customer termination process, which includes full removal of all customer data within ninety (90) days unless otherwise instructed by its customer.
Measures for ensuring accountability	Allvue adheres to contractual obligations and commitments and aligns with industry practices.
Measures for allowing data portability and ensuring erasure	Upon termination, its customer is able to request and receive a data export in an industry-standard format (i.e., csv).

Technical and Organizational Measure	Details
Technical and organizational measures of sub-processors	Allvue has a comprehensive Risk Management Framework, which includes a Risk Assessment Methodology and Risk Assessment Policy. Third-party vendors/applications are included in scope.