OOMNITZA
DATA PROCESSING ADDENDUM

Last Updated: February 23, 2024

This Data Processing Addendum, including its Exhibits, ("**DPA**") forms part of the Enterprise Terms, SaaS Subscription Agreement, or other written or electronic agreement between Oomnitza, Inc. ("**Oomnitza**") and Customer for the purchase of online services from Company (identified as the "Services" in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**"), which involves the Processing of Personal Data subject to Applicable Data Protection Laws (each as defined below). The purpose of this DPA is to set forth the terms under which Company Processes Personal Data on behalf of Customer.

This DPA consists of the main body and Exhibits A and B.

HOW TO EXECUTE THIS ADDENDUM:

This Addendum has been pre-signed on behalf of Oomnitza.

To complete this Addendum, Customer must:

- Complete the information in the signature box and sign on page 5.
- Send the signed Addendum to Oomnitza by email to security@oomnitza.com
- Except as otherwise expressly provided in the Agreement, this Addendum will become legally binding upon receipt by Oomnitza of the validly completed Addendum at this email address.

1. Definitions. Capitalized terms used but not defined in this DPA have the meanings set forth in the Agreement. The terms controller, data subject, processor and supervisory authority have the meanings set forth in the Applicable Data Protection Laws.

a. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

b. "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws, UK GDPR and the United States including the CCPA.

c. "**CCPA**" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time, including the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.

d. "**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

e. "**EEA**" means the European Economic Area.

f. "**European Data Protection Laws**" means the GDPR and other data protection laws and regulations of the EEA and European Union, and the Member States of each of the foregoing, to the extent applicable to the Processing of Personal Data under the Agreement.

g. "**EU – US Data Privacy Framework**" or "**EU/US DPF**" means the Commission Implementing Decision dated July 10, 2023, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

h. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) which includes the EU/US DPF.

i. "**Information Security Incident**" means a confirmed breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Company's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

j. "**Personal Data**" means Customer Data that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Laws, or information of a similar character regulated thereby," provided that such data is electronic data and information submitted by or for Customer to the Services.

k. "**Processing**" or "**Process**" 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.

l. "**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

m. "**Security Measures**" are Company's security measures implemented and maintained as administrative, technical and physical safeguards designed to protect the security and integrity of Personal Data and prevent Information Security Incidents, further described in Exhibit A hereto.

n. "**Standard Contractual Clauses**" means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, currently located here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj and as amended from time to time due to changes in Applicable Data Protection Law.

o. "**Subprocessors**" or "**Sub-processor**" means any third-party processor that Company engages to Process Personal Data in relation to the Services.

p. "**UK GDPR**" means the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2019.

q. "**US Data Privacy Framework**" or "**US DPF**" collectively means the E.U.-US Privacy Shield as replaced by the Data Privacy Frameworks operated by the U.S. Department of Commerce.

2. **Duration and Scope of DPA**. This DPA will remain in effect so long as Company Processes Personal Data, notwithstanding the expiration or termination of the Agreement. Exhibit B to this DPA applies solely to Processing subject to the CCPA to the extent Customer is a "business" (as defined in CCPA) with respect to such Processing.

3. **Customer Instructions**. Company will Process Personal Data only in accordance with Customer's instructions to Company. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Company only pursuant to an amendment to this DPA signed by both parties. Customer instructs Company to Process Personal Data via the Services and as authorized by the Agreement. Company shall inform Customer immediately: (a) if, in its opinion, an instruction from Customer constitutes a breach of any Applicable Data Protection Laws; (b) if Company is unable to follow Customer's instructions for the Processing of Personal Data; or (c) if Company has reason to believe that Company is subject to changes in Applicable Data Protection Laws contrary to any Customer instructions or terms or requirements of this DPA.

4. **Security of Personal Data**.

   a. Company Security Measures. Company may update the Security Measures from time to time, so long as the updated measures do not materially decrease the overall protection of Personal Data.

   b. Information Security Incidents. Company will notify Customer without undue delay of any Information Security Incident of which Company becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Company recommends the Customer take to address the Information Security Incident. Company's notification of or response to an Information Security Incident will not be construed as Company's acknowledgement of any fault or liability with respect to the Information Security Incident.

   c. Audits of Compliance DPIAs. Customer uses external auditors to verify the adequacy of its security measures, including the security of the physical facilities from which Customer provides the Services. This audit: (i) will be performed at least annually; (ii) will be performed by independent third-party security professionals at Company's selection and expense; and (iii) will result in the generation of a SOC 2 audit report ("Audit Report"), which will be Company's Confidential Information. At Customer's written request, and provided that the parties have applicable confidentiality terms in place, Company will provide Customer with a copy of the Audit Report so that Customer can verify Company's compliance with its obligations under this DPA. Customer agrees that the Audit Report, together with any third-party certification maintained by Company, will be used to satisfy any audit or inspection requests by or on behalf of Customer and to demonstrate compliance with this DPA (including the SCCs, where applicable).

   d. Data Protection Impact Assessments (DPIAs). Upon Customer's written request, Company will provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Company.

5. **Customer's Responsibilities**.

   a. Customer Obligations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any data subject, including those that have opted out from sales or other disclosures of personal data to the extent applicable under Applicable Data Protection Laws. Without limitation of Customer's obligations under the Agreement, Customer: (a) agrees that Customer is solely responsible for its use of the Services, including (1) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data, (2) securing the account authentication credentials, systems and devices Customer uses to access the Services, (3) securing Customer's systems and devices that Company uses to provide the Services, and (4) backing up Personal Data; and (b) has given all notices to, and has obtained all consents from, including where the Customer is a processor by ensuring that the ultimate controller does so, individuals to whom Personal Data pertains and all other parties as required by applicable laws or regulations for Company to Process Personal Data as contemplated by the Agreement.

   b. Prohibited Data. Customer represents and warrants to Company that Customer Data does not and will not, without Company's prior written consent, contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Data of children, including, without limitation, all information about

children under 16 years of age; or any information that falls within any special categories of data (as defined in GDPR).

6. Compliance with Laws & Data Subject Rights.

a. Compliance with Laws. Each party will comply with all Applicable Data Protection Laws. In particular, Customer will comply with its obligations as controller (or on behalf of controller) and Company will comply with its obligations as processor.

b. Personal Data Disclosures & Government Requests. Company will not disclose Personal Data to any third party, including any Public Authority, except: (i) as otherwise permitted under the Agreement including this DPA; or (ii) as necessary to comply with Applicable Data Protection Laws including with respect to any valid and/or binding Public Authority court order (e.g., a law enforcement subpoena). If Company receives a binding order from a Public Authority requesting access to or disclosure of Personal Data, Company will notify Customer of the request unless otherwise legally prohibited.

c. Data Subject Request Assistance. Company will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("**Data Subject Requests**") with respect to Personal Data in Company's possession or control. Where permitted under Applicable Data Protection Laws, Customer will compensate Company for any such assistance at Company's then-current professional services rates, which will be made available to Customer upon request.

d. Customer's Responsibility for Requests. Company will not respond to a Data Subject Request itself, except where Customer authorizes Company to redirect the Data Subject Request as necessary to allow Customer to respond directly. If Company receives a Data Subject Request, Company will advise the data subject to submit the request to Customer and Customer will be responsible for responding to the request.

7. EU/US DPF; UK, Switzerland, Changes in Laws.

a. EU/US DPF. As of the Effective Date, Company is registered with the United States for, and complies with, the EU/US DPF (see Company's certification is located here: https://www.dataprivacyframework.gov/list). Customer may transfer Personal Data to Company, provided during the Term of this DPA Company: (i) maintains compliance with the EU/US DPF and US DPF; and (ii) will promptly notify Customer if at any time Company ceases to be EU/US DPF certified. If Company no longer complies with the EU/US DPF and/or the US DPF, or if changes in Applicable Law renders the EU/US DPF invalid, the parties agree to implement an alternative lawful transfer mechanism (e.g., the Standard Contractual Clauses) and if the parties cannot agree on such alternative mechanism, Customer may terminate this DPA.

b. The United Kingdom, Switzerland. The United Kingdom and Switzerland each adopted the EU/US DPF; therefore, for the purposes of Applicable Data Protection Laws for such countries, including for clarity with respect to UK GDPR, Customer may transfer Personal Data to Company from each such country during the Term of this DPA subject to Section 7(a)(i) and (ii) above.

c. Changes in Applicable Data Protection Laws. Company shall use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services, to facilitate compliance with changes in Applicable Data Protection Laws without unreasonably burdening Customer. If Company is unable to make available necessary changes promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Company in accordance with the changes in Applicable Data Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

8. Subprocessors.

a. Consent to Subprocessor Engagement. Customer authorizes the following Subprocessors to Process Personal Data: (i) Company's Affiliates; and (ii) the Subprocessors set forth at https://www.oomnitza.com/thirdpartyterms, as updated by Company from time to time, or such other website address as Company may provide to Customer from time to time) ("**Subprocessor Site**").

b. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Company will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Company shall be liable for all obligations under the Agreement subcontracted to, the Subprocessor or its actions and omissions related thereto.

c. Subprocessor Changes. When Company engages any new Subprocessor after the Effective Date of the Agreement, Company will update the Subprocessor Site (including the name and location of the relevant Subprocessor and the activities it will perform).

d. Opportunity to Object to Subprocessor Changes. If Customer objects to such engagement in a written notice to Company on reasonable grounds relating to the protection of Personal Data, Customer and Company will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Company.

9. **Return or Deletion of Personal Data**. Upon request by Customer made within 60 days after the effective date of termination or expiration of this DPA, Company will delete or return Customer Data within a reasonable period of time. After such 60-day period, Company will have no obligation to maintain or provide any Customer Data, and as provided in the Documentation will thereafter delete or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited.

10. **Miscellaneous**. Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. In the event of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Company's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Company to Customer under this DPA may be given: (a) in accordance with any notice clause of the Agreement; (b) to Company's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Services-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

IN WITNESS WHEREOF, the undersigned have executed this Agreement by their duly authorized representatives, with the intention to be legally bound.

CUSTOMER: _____	**OOMNITZA, INC.** DocuSigned by: E26CB171CF844F4...
By: _____	By: _____
Name: _____	Name: Jon Davis
Title: _____	Title: Chief Information Security Officer
Date: _____	Date: 2/23/2024

EXHIBIT A
SECURITY MEASURES

Company processes all Personal Data received from Controller under this DPA in conformity with the following technical and organizational measures:

Company will implement and maintain an information security program ("**Information Security Program**") that: (i) is consistent with industry standard practices, taking into consideration the sensitivity of the relevant Personal Data, and the nature and scope of the Services to be provided; (ii) includes reasonable administrative, technical and physical safeguards designed to protect Personal Data; and (iii) complies with Data Protection Laws. At a minimum, the Information Security Program shall include:

- Information Security Policy. Company shall maintain a written information security policy applicable to all authorized personnel.
- Training. Company will provide role-based information security training.
- Access Control. Company will maintain an access control policy, procedures, and controls consistent with industry standard practices. Company will limit access to Personal Data to those employees and Sub-processors with a need-to-know.
- Logical Separation. Company will ensure Personal Data is logically separated from other Company client data.
- Encryption. Company will utilize industry standard encryption technologies with respect to Personal Data. Personal Data will be encrypted in-transit and at rest.
- Password Management. Company will maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.
- Incident Response Plan. Company will maintain an incident response plan that addresses Information Security Incident handling. Upon request, Company will provide Customer with a copy of its incident response plan.
- Penetration Testing. At least once per year, Company will retain an independent third-party to carry out a penetration test of Company's key systems. Upon request, Company will make the penetration test results available to Customer.
- Backups of Personal Data. Company will maintain an industry standard backup system and backup of Personal Data to facilitate timely recovery in the event of a service interruption.
- Disaster Recovery and Business Continuity Plans. Company will maintain disaster recovery and business continuity plans consistent with industry standard practices**.**

EXHIBIT B
UNITED STATES EXHIBIT

A. The parties acknowledge that Customer discloses Personal Data to Company for the limited and specified purposes set forth in the Agreement and DPA, and as instructed by Customer.

B. Customer shall have the right to take the reasonable and appropriate steps set forth in the Agreement designed to stop and remediate unauthorized use of Personal Data.

C. Company will not retain, use, disclose, sell, or share the Personal Data other than providing the Services specified by Customer's documented instructions. Company will not combine Personal Data with information received from, or on behalf of other entities, except to perform the purpose of providing the Services specified by Customer's documented instructions. Company shall Process Personal Data in accordance with Data Protection Laws applicable to Company's provision of the Services to its customers generally (i.e., without regard for Customer's particular use of the Services), when the Services are used according to this DPA, the Agreement, the Documentation, and the applicable Order Form. Company shall inform Customer if Company determines it is unable to meet its obligations under the CCPA.

D. The parties acknowledge that Company's retention, use and disclosure of personal information authorized by Customer's instructions documented in the DPA are integral to Company's provision of the Services and the business relationship between the parties.