U.S. Privacy Law Data Processing Addendum

Pursuant to the Agreement, Provider and Customer (each a "**Party**" collectively, the "**Parties**") hereby adopt this U.S. Privacy Law Data Processing Addendum ("**U.S. DPA**") for so long as Provider Processes Personal Information on behalf of Customer pursuant to the Agreement. In the event of a conflict between this U.S. DPA and the Agreement with respect to the subject matter of this U.S. DPA, this U.S. DPA will prevail to the extent of such conflict. Capitalized terms used in this U.S. DPA and not defined herein will have the meanings given to them by the Agreement.

1. **Definitions**. For the purposes of this U.S. DPA--
    1. "**Consumer**" means a natural person. Where applicable, Consumer shall be interpreted consistent with the same or similar term under U.S. Privacy Laws.
    2. "**Controller**" means a person or entity that collects individuals' Personal Information and alone, or jointly with others, determines the purposes and means of the Processing of such Personal Information. Where applicable, Controller shall be interpreted consistent with the same or similar term under U.S. Privacy Laws.
    3. "**Customer Personal Information**" means Customer Data that constitute Personal Information.
    4. "**Personal Information**" means information 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 natural person. Where applicable, Personal Information shall be interpreted consistent with the same or similar term under U.S. Privacy Laws.
    5. "**Process**," means any operation or set of operations that are performed on Personal Information or on sets of Personal Information, whether or not by automated means. Where applicable, "Processing," "Process," and "Processed" shall be interpreted consistent with the same or similar term under the U.S. Privacy Laws.
    6. "**Processor**" means "Processor," "Service Provider," or "Contractor" as those terms are defined in U.S. Privacy Laws.
    7. "**Sale**" and "**Selling**" have the meaning defined in U.S. Privacy Laws.
    8. "**Share**," has the meaning defined in the CCPA.
    9. "**U.S. Privacy Laws**" means, collectively, all U.S. federal and state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Information and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information), in each case where applicable to the Processing of Customer Personal Information by Provider pursuant to the Agreement. U.S. Privacy Laws may include, but are not limited to, the following:
        1. California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("**CCPA**");
        2. Colorado Privacy Act;
        3. Connecticut Personal Data Privacy and Online Monitoring Act;
        4. Delaware Personal Data Privacy Act;
        5. Indiana Consumer Data Protection Act;
        6. Iowa Consumer Data Protection Act;
        7. Montana Consumer Data Privacy Act;
        8. Oregon Consumer Privacy Act;
        9. Tennessee Information Privacy Act;
        10. Texas Data Privacy and Security Act;
        11. Utah Consumer Privacy Act; and
        12. Virginia Consumer Data Protection Act.
    10. In the event of a conflict in the meanings of defined terms in U.S. Privacy Laws, the meaning from the law applicable to the state of residence of the relevant Consumer applies.

2. Scope, Roles, and Termination.

1. *Applicability* - This U.S. DPA applies only to Provider's Processing of Customer Personal Information pursuant to the Agreement.
2. *Roles of the Parties* - For the purposes of the Agreement and this U.S. DPA, Customer is the Party responsible for determining the purposes and means of Processing Customer Personal Information as the Controller and appoints Provider as a Processor to Process Customer Personal Information on behalf of Customer for the limited and specific purposes set forth in Appendix A.
3. *Obligations at Termination* - Upon termination of the Agreement, except as set forth therein or herein, Provider will discontinue Processing and destroy or return Customer Personal Information in its or its subcontractors' and sub-processors' possession without undue delay. Provider may retain Customer Personal Information to the extent required by law but only to the extent and for such period as required by such law and always provided that Provider shall take steps to ensure the confidentiality of all such Customer Personal Information.

3. Compliance.

1. *Compliance with Obligations* – Provider shall: (a) comply with applicable obligations of U.S. Privacy Laws, (b) provide the level of privacy protection for Customer Personal Information required by applicable U.S. Privacy Laws, and (c) provide Customer with reasonable assistance to enable Customer to fulfill its own obligations under applicable U.S. Privacy Laws. Upon the reasonable request of Customer, Provider shall make available to Customer information in Provider's possession necessary to demonstrate Provider's compliance with this subsection.
2. *Compliance Monitoring* – No more than once per calendar year, Provider will provide to Customer, upon Customer's written request, information and documentation necessary to demonstrate Provider's compliance with this US DPA.
3. *Compliance Remediation* – Provider shall notify Customer if Provider determines that it can no longer meet its obligations under applicable U.S. Privacy Laws. Upon receiving notice from Provider in accordance with this subsection, Customer may direct Provider to take commercially reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Information.

4. Restrictions on Processing.

1. *Limitations on Processing* – Except where otherwise required by law, Provider will Process Customer Personal Information solely pursuant to the Agreement. Except as expressly permitted by U.S. Privacy Laws, Provider is prohibited from (i) Selling or Sharing Customer Personal Information, (ii) retaining, using, or disclosing Customer Personal Information for any purpose other than for the specific purpose of performing the services specified in Appendix A, (iii) retaining, using, or disclosing Customer Personal Information outside of the direct business relationship between the Parties, and (iv) combining Customer Personal Information with Personal Information obtained from, or on behalf of, sources other than Customer, except as expressly permitted under applicable U.S. Privacy Laws.
2. *Confidentiality* - Provider shall take steps to ensure that its employees, agents, subcontractors, and sub-processors are subject to a duty of confidentiality with respect to Customer Personal Information.
3. *Subcontractors:* Provider shall attempt to notify Customer of any intended changes concerning the addition or replacement of subcontractors or sub-processors. Further, Provider shall take steps to ensure that Provider's subcontractors or sub-processors who Process Customer Personal Information on Provider's behalf agree in writing to the same or materially equivalent restrictions and requirements that apply to Provider in this U.S. DPA and the Agreement with respect to Customer Personal Information, as well as to comply with U.S. Privacy Laws.
4. *Right to Object* – Customer may object in writing to Provider's appointment of a new subcontractor or sub-processor on reasonable grounds by notifying Provider in writing within thirty (30) calendar days of receipt of notice. In the event Customer objects, the Parties shall discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution.

5. Consumer Rights.

1. Provider shall provide commercially reasonable assistance to Customer for the fulfillment of Customer's obligations to respond to U.S. Privacy Law-related Consumer rights requests regarding Customer Personal Information.
2. Where applicable, Customer shall inform Provider of any Consumer request made pursuant to U.S. Privacy Laws with which Provider must comply with. Customer shall provide Provider with the information necessary for Provider to comply with the request.
3. Provider shall not be required to delete any Customer Personal Information to comply with a Consumer's request directed by Customer if retaining such information is specifically permitted by applicable U.S. Privacy Laws; provided, however, that in such case, Provider shall not use Customer Personal Information retained for any purpose other than provided for by that exception.

6. Deidentified Data

1. In the event that either Party discloses or makes available Deidentified data (as such term is defined in the U.S Privacy Laws) to the other Party, the receiving Party shall: (i) take reasonable measures to ensure that the data cannot be associated with a Consumer or household; (ii) publicly commit to maintain and use the data in Deidentified form and not to attempt to reidentify the data, except as permitted by applicable U.S. Privacy Laws; and (iii) contractually obligate any recipients of the data to comply with all provisions of this paragraph.

7. Deletion of Company Personal Information

1. Upon direction by Customer, and in any event no later than thirty (30) days after receipt of a request from Customer, Provider shall promptly delete Customer Personal Information as directed by Customer, unless Provider is required by law to retain such data, in which case Provider shall, on ongoing basis, isolate and protect the security and confidentiality of such Personal Information and prevent any further processing except to the extent required by such law and shall destroy or return to Customer all other Personal Information not required to be retained by Provider by law.

8. Security

1. The Parties shall implement and maintain no less than commercially reasonable security procedures and practices, appropriate to the nature of the information, designed to protect Customer Personal Information from unauthorized access, destruction, use, modification, or disclosure. Without limiting the forgoing, the Parties shall comply with the Security Measures set forth at Appendix B, as applicable, when Processing Customer Personal Information.
2. Provider shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires necessary to confirm Provider's compliance with the U.S. Privacy Laws and this U.S. DPA.
3. Upon becoming aware of an actual or reasonably suspected unauthorized access, destruction, use, modification, or disclosure of Customer Personal Information ("**Security Incident**"), Provider shall notify Customer without undue delay (and in any event within seventy-two (72) hours of becoming aware of the Security Incident) and shall provide timely updates and information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Such information will include the nature of the Security Incident, the categories and number of Consumers affected, the categories and amount of Customer Personal Information affected, the likely consequences of the Security Incident, and the measures taken or proposed to be taken to address the Security Incident and mitigate possible adverse effects.

9. Consumer Rights

1. Upon direction by Customer, and in any event no later than thirty (30) days after receipt of a request from Customer, Provider shall promptly delete Customer Personal Information as directed by Customer.

2. Provider shall not be required to delete any Customer Personal Information to comply with a Consumer's request directed by Customer if it is necessary to maintain such information in accordance with applicable U.S. Privacy Laws, in which case Provider shall promptly inform Customer of the exceptions relied upon under applicable U.S. Privacy Laws and Provider shall not use Customer Personal Information retained for any other purpose than provided for by that exception.
3. The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this U.S. DPA.

10. Exemptions.

1. Notwithstanding any provision to the contrary in the Agreement or this U.S. DPA, the terms of this U.S. DPA shall not apply to Provider's Processing of Customer Personal Information that is exempt from applicable U.S. Privacy Laws.

11. Changes to Applicable Privacy Laws.

1. The Parties agree to cooperate in good faith to enter into additional terms to address any modifications, amendments, or updates to applicable statutes, regulations or other laws pertaining to privacy and information security, including, where applicable, U.S. Privacy Laws.

Appendix A - Processing Details

Nature of the Processing	Provision of the Services.
Purpose(s) of the Processing	Provision of the Services.
Types of Customer Personal Information Subject to Processing	Email addresses, IP addresses, location information (inferred from IP addresses), job title, and phone numbers.
Duration of Processing	For the term of the Agreement or as otherwise agreed to in writing by the Parties.

Appendix B – Security Measures

The Parties will apply at least the following types of security measures to Customer Personal Information:

1. **Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Personal Information are Processed, include:

[X] Access control system (ID reader, magnetic card, chip card);

[X] Key management, card-keys procedures;

[X] Door locking (electric door openers etc.); and

[X] Securing decentralized data processing equipment and personal computers.

2. **Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

[X] User identification and authentication procedures.

3. **Data access control**

Technical and organizational measures designed to ensure confidentiality and that persons entitled to use a data processing system gain access only to such Customer Personal Information in accordance with their access rights, and that Customer Personal Information cannot be read, copied, modified or deleted without authorization, include:

[X] Internal policies and procedures;

[X] Control authorization schemes;

[X] Differentiated access rights (profiles, roles, transactions and objects);

[X] Monitoring and logging of access; and

[X] Change procedure.

4. **Disclosure control**

Technical and organizational measures designed to ensure that Customer Personal Information cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Personal Information are disclosed, include:

[X] Transport security.

5. **Control of instructions**

Technical and organizational measures designed to ensure that Customer Personal Information are Processed solely in accordance with the instructions of the Controller include:

[X] Unambiguous wording of the contract.

6. **Availability control**

Technical and organizational measures designed to ensure the integrity, availability and resilience of the processing systems, and that Customer Personal Information are protected against accidental destruction or loss (physical/logical) include:

[X] Backup procedures;

[X] Mirroring of hard disks (e.g., RAID technology);

[X] Uninterruptible power supply (UPS);

[X] Remote storage;

[X] Antivirus/firewall systems; and

[X] Disaster recovery plan.

7. **Separation control**

Technical and organizational measures designed to ensure that Customer Personal Information collected for different purposes can be Processed separately include:

[X] Segregation of functions (production/testing); and

[X] Procedures for storage, amendment, deletion, transmission of data for different purposes.