SUPPLIER DATA PROCESSING AGREEMENT (DPA)

Client and Supplier agree that this Data Processing Agreement ("DPA"), including exhibits, sets out the data privacy, data protection, data transfer, and security requirements that apply to Supplier's and its Affiliate(s)' Processing of Personal Data for the purpose of providing Services to Client and its Affiliate(s).

Client and Supplier agree as follows:

1. **Definitions.** When used in this DPA, the following terms have the following meanings. All capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

   "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

   "**Client"** means Entity that is provisioning for the services under the DPA.

   "**DP Law**" means all laws and regulations that apply to Personal Data Processing under this DPA, including applicable international, federal, state, provincial, and local laws, rules**,** regulations, directives and governmental requirements currently in effect, and as they become effective, relating in any way to data privacy, data protection, data transfer, data security, and the Payment Card Industry ("**PCI**") Data Security Standards.

   "**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, which may include a "Business" as defined under the CCPA.

   "**Data Processor**" means the entity that Processes Personal Data on behalf of the Data Controller, which may include a "Service Provider" as defined under the CCPA.

   "**Data Security Measures**" means technical and organizational measures that are intended to secure Personal Data to a level appropriate for the risk of the Processing, which include measures protecting Personal Data from misuse; accidental or unlawful loss; and unauthorized access, disclosure, alteration, or destruction.

   "**Data Subject**" means an identified or identifiable natural person to which Personal Data relates.

   "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

   "**Instructions**" means this DPA and any further written agreement or documentation by way of which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data for that Data Controller.

   "**Personal Data**" means information that relates to a Data Subject and, directly or indirectly, enables the Data Subject to be identified or identifiable, in particular by reference to name,

identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person) that is collected, disclosed, stored, accessed or otherwise Processed under the Agreement.

"**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

"**Process**", "**Processing**", or "**Processed**" means to perform any operation or set of operations on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, as defined or described under applicable DP Law.

"**Standard Contractual Clauses**" means the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU).

"**Sub-processor**" means an entity engaged by the Data Processor (or any Sub-processor of the Data Processor) to Process Personal Data on behalf and under the authority of the Data Controller.

"**Supplier"** means Converge Technology Solutions US, LLC.

2. **Roles of the Parties.**

   a. **Supplier's role.** Supplier is acting as a Data Processor on behalf of Client; and

   b. **Client's role.** Client as a Data Controller has the sole and exclusive authority to determine the purposes and means of Processing Personal Data. If Client is acting as the Data Processor Processing Personal Data on behalf of the Client User or another third party Data Controller, Supplier is acting on behalf of Client, who is acting on behalf of the Client User.

3. **Supplier Obligations as a Data Processor.** The Supplier will:

   a. Process Personal Data on behalf of and in accordance with Client's Instructions. Supplier will inform Client if, in its opinion, the Instructions are inconsistent with DP Law;

   b. Supplier will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and to comply with applicable Law. Supplier will not sell, disclose, share or provide access to any Personal Data that Client provides to Supplier for monetary or other valuable consideration. Supplier represents and warrants that it will not transfer any Personal Data subject to this DPA in a way that constitutes a Sale of Personal Data under the CCPA. Supplier will not accept any Personal Data as consideration for any Services that Supplier provides to Client;

c. ensure that all persons Supplier authorizes to Process Personal Data in the context of the Services are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of Personal Data;

d. immediately, and under no circumstances later than within 3 business days, inform Client of all requests Supplier receives from Data Subjects (including Verifiable Consumer Requests under the CCPA) exercising their applicable rights under DP Law of access to (right to know to under the CCPA), or correction or erasure of, their Personal Data, their right to restrict or object to Supplier's Processing, or their right to data portability. Supplier will not respond to these requests unless Client instructs Supplier in writing to do so;

e. immediately, and under no circumstances later than within 3 business days, inform Client of each request Supplier receives from a public authority requiring Supplier to disclose Personal Data Processed in the context of the Services or to participate in an investigation involving that Personal Data;

f. provide reasonable assistance through Data Security Measures to Client, at Supplier's expense, to assist Client in complying with Client's obligations under DP Law, which assistance would include conducting data protection impact assessments and consulting with a supervisory authority, taking into account the nature of the Processing and the information available to Supplier;

g. implement, maintain, and comply with the Security Requirements set out in **Exhibit A** to this DPA. Supplier will respond to Personal Data Breaches in accordance with Clause 2 of Exhibit A. The response may include identifying key partners, investigating the Incident, providing regular updates, and liaising with regards to notice obligations. Supplier will not notify Client's affected Data Subjects about a Personal Data Breach without first consulting with and obtaining written authorization from Client.

h. engage Sub-processors (i.e., Amazon Web Services, Microsoft Azure, Google Cloud Platform) as necessary to perform the Services on the basis of having received authorization from Client in accordance with Exhibit A. Supplier will remain liable to Client for the Sub-processor's performances of any part of the Services;

i. make available to Client, within reasonable time upon Client's request, all information necessary to demonstrate compliance with the obligations set forth in this DPA and allow for, and contribute to, audits and inspections conducted by Client or another auditor appointed by Client.

j. To the extent applicable to the Services, Supplier certifies that it understands and will comply with the requirements in this DPA relating to CCPA.

EXHIBIT A – SECURITY REQUIREMENTS ADDENDUM

The Security Requirements Addendum ("**SRA**") provides the required technical and organizational measures, including Data Security Measures, that Supplier will take in order to safeguard Client Data during the term of the Agreement (the "**Security Requirements**"). The SRA is subject to the Agreement, and all capitalized terms not defined in the SRA have the meanings set forth in the DPA. In the event of a conflict or ambiguity between the Agreement and the SRA, the terms of the SRA will supersede and control.

1. **Definitions**.
    a. "**Personnel**" means any employees, contractors, agents, and Subcontractors of Supplier.
    b. "**Client Data**" means all data (including Personal Data) (a) collected, received, stored or maintained by the Supplier in connection with Supplier's performance of its obligations under this DPA (including data or information collected by or associated with any cookies), (b) provided by Client to Supplier, or (c) derived from (a) or (b).
    c. "**Subcontractors**" means any third-party vendors or service providers subcontracted by Supplier to perform Services.
    d. "**Term**" means the period of time during which Client and Supplier are performing under at least one active statement of work, order form, or other legal agreement executed between Client and Supplier.
    e. "**User Data**" means information that describes a Client user's business and its operations, products or services, and orders placed by the Client user's customers.
2. **Information Security Breach.** Supplier will notify Client within a commercially reasonable time period, after it becomes aware that an Information Security Breach has occurred in the Supplier Systems. Supplier will promptly take all necessary steps to mitigate the impact of the Information Security Breach, grant Client access to relevant systems and logs related to the Information Security Breach, and cooperatively share information with Client to address and remediate the Information Security Breach.
3. **Annual Security Awareness Training.** Supplier will ensure that every Personnel individual completes annual security awareness training on Supplier's security policy, which must include training on Supplier's data security and confidentiality practices relating to Client Data.
4. **Supplier Personnel Confidentiality.** Supplier will ensure that every Personnel individual executes a confidentiality agreement with Supplier that is at least as protective of Client Data as this Agreement.

5. **Security Policy.** Supplier represents and warrants that it has implemented, or will immediately implement and maintain, an industry-standard security policy.

6. **Security Updates.** Supplier will maintain a vulnerability management program and apply critical security updates and patches to the Supplier Systems. Supplier will apply critical patches immediately and apply routine security updates within commercially reasonable time period after release.

7. **Incident Response Plan.** Supplier represents and warrants that it has implemented or will immediately implement, maintain during the Term, and test at least once annually through a tabletop exercise, an incident response plan that identifies Supplier's procedures for managing an Information Security Incident that meets industry standards.

8. **Security Incident Training.** Supplier will ensure that each Personnel individual participates in annual security incident training and will assign only trained Personnel to detect and respond to suspected or actual Information Security Breaches.

9. **Supplier Personnel Conduct.** Supplier will ensure that each Personnel individual complies with Supplier's policy and guidelines on confidentiality, business ethics, appropriate usage, anti-harassment, and professional standards.