

This Data Processing Addendum (“DPA”) is part of the Master Services Agreement (the “MSA”) between Converge AI, Inc. (“Converge,” “we,” or “us”) and the customer named in the Order Form (“you”). It applies when an Order Form references it or the parties sign it, and remains in effect as long as we process Personal Data. “Personal Data” means personal information in Customer Data, such as nonpublic personal information of your clients and employees. “Privacy Laws” means the laws that apply to our processing of Personal Data for you, such as the Gramm-Leach-Bliley Act, state insurance data security and privacy laws, and state consumer privacy laws. Other capitalized terms have the meanings in the MSA.

1. ROLES AND COMMITMENTS

1.1 Roles. You are the controller (or “business”) and we are your processor (or “service provider”) under Privacy Laws. Each party will comply with the Privacy Laws that apply to it.

1.2 Our commitments. We will process Personal Data only to provide the Services and on your documented instructions (the MSA, Order Forms, and your use of the Services). We will not sell or share it, or retain, use, or disclose it outside our direct business relationship with you or for any other purpose, or combine it with other data, except as Privacy Laws allow. We will tell you if we believe an instruction violates Privacy Laws or if we can no longer meet our obligations under them. Personnel with access are bound by confidentiality obligations.

1.3 Your responsibilities. You are responsible for the lawfulness of the Personal Data you provide and your instructions, including any notices and consents owed to your clients and employees.

2. SECURITY AND SUBPROCESSORS

2.1 Security. We maintain safeguards appropriate to the risk and consistent with Section 4.4 of the MSA, including access controls limiting access to personnel who need it, encryption of Personal Data in transit and at rest, access logging, and security training for personnel.

2.2 Subprocessors. You authorize us to use subprocessors, including hosting and AI providers, to deliver the Services. We bind each to written data protection terms no less protective than this DPA and remain responsible for their performance. Our current list is available on request.

2.3 Security incidents. We will notify you without undue delay, and within 3 business days, after confirming unauthorized access to Personal Data in our possession or control, and will share the information reasonably available to help you meet your own legal notice obligations. You are responsible for notifying regulators, carriers, and individuals where required, and we will cooperate reasonably.

3. ASSISTANCE, AUDITS AND DELETION

3.1 Assistance. Taking into account the nature of the Services, we will reasonably help you respond to individual rights requests, regulator inquiries, and data protection assessments relating to Personal Data. We may charge reasonable fees for assistance that goes beyond ordinary support.

3.2 Audits. On request, we will give you the information reasonably needed to show our compliance with this DPA, such as security documentation, questionnaire responses, and available third-party assessments. If that is not enough, you may audit our compliance once per year on at least 30 days’ notice, during business hours, subject to confidentiality, and without access to other customers’ data or to our systems beyond what is reasonably necessary.

3.3 Return, deletion, and location. Export, deletion, and backup handling follow Section 4.8 of the MSA. We process Personal Data in the United States.

4. LIABILITY AND PRECEDENCE

4.1 Liability. Section 11 of the MSA, including its limits and exceptions, applies to this DPA.

4.2 Precedence. For the processing of Personal Data, this DPA controls over the MSA and any Order Form, as stated in Section 12.6 of the MSA.