Data Collection and Privacy Policy

Effective Date: July 9, 2025

1. Introduction

At Reverb, we are committed to protecting the privacy and security of the personal data we collect, use, and store. This Data and Privacy Policy outlines our practices regarding the collection, use, disclosure, and protection of information, ensuring compliance with applicable data protection laws and regulations. Cybersecurity and data protection are of utmost importance to Reverb. Everyone, from our clients and partners to our employees and contractors, should feel that their data is safe.

Scope

This policy applies to all personal data processed by Reverb in the course of our business operations, including data collected from customers, employees, partners, website visitors, and anyone who has permanent or temporary access to our systems and data.

2. Definitions

When used in this policy, the following terms have the following meanings:

- **CCPA:** The California Consumer Privacy Act of 2018, as may be amended from time to time.
- **Data Controller:** 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:** 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:** 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:** An identified or identifiable natural person to which Personal Data relates.
- **GDPR:** The General Data Protection Regulation (EU) 2016/679.
- **Instructions:** 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:** 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:** 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**: 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.
- **Sub-processor:** 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.

3. Principles of Data Processing

We adhere to the following principles when processing personal data:

- **Lawfulness, Fairness, and Transparency:** Personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation:** Personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible

with those purposes.

- **Data Minimization:** Personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data is accurate and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage Limitation:** Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and Confidentiality (Security):** Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- **Accountability:** We are responsible for, and able to demonstrate compliance with, these principles.

4. Types of Data Collected

We may collect various types of personal data, including but not limited to:

- **Identity Data:** Name, date of birth, gender identity, marital status.
- **Contact Data:** Billing address, home address, email address, telephone numbers.
- **Website Data:** Browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our website or services. (see website section below for more detail)
- **Usage Data:** Information about how you use our website, products, and services.
- **Marketing and Communications Data:** Your preferences in receiving marketing from us and your communication preferences.
- **Employment Data (for employees/applicants):** CVs, qualifications, references, payroll information, emergency contact details.

5. How Data is Collected

We use different methods to collect data from and about you, including:

- **Direct Interactions:** You may give us your Identity, Contact, and Usage Data by filling in forms or by corresponding with us by phone, email, or otherwise.
- **Automated Technologies or Interactions:** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions, and patterns. We collect this personal data by using cookies, server logs, and other similar technologies.
- **Third Parties or Publicly Available Sources:** We may receive personal data about you from various third parties and public sources, such as:
    - Technical Data from analytics providers (e.g., Google Analytics).
    - Contact, Financial, and Transaction Data from providers of technical, payment, and delivery services (e.g. Quickbooks, Hubspot, Thinkific).
    - Identity and Contact Data from publicly available sources (e.g.,Crunchbase, Linkedin, Geekwire, etc.).

Website Data

- We collect **cookies or similar tracking technologies on our website**. This means information that our website server transfers to your computer. This information can be used to track your session on our website. Cookies may also be used to customize our website content for you as an individual. If you are using one of the common Internet web browsers, you can set up your browser to either let you know when you receive a cookie or to deny cookie access to your computer.
    - We use cookies to recognize your device and provide you with a personalized experience.
    - We also use cookies to attribute visits to our websites to third-party sources.
    - We may also use automated tracking methods on our website in communications with you and in our products and services to measure performance and engagement.
- **Embedded Content:** If the website embeds content from other sites (e.g., YouTube videos, social media feeds), mention that these third-party sites may also set their own cookies.

Web Analysis Tools

- We may use web analysis tools like Google Analytics that are built into Reverb's website to measure and collect anonymous session information.

6. Purpose of Data Collection and Use

We use your personal data for the following purposes:

- **To provide and manage our services:** To fulfill contracts, process transactions, and deliver products/services you have requested.
- **To manage our relationship with you:** Including notifying you about changes to our terms or privacy policy, and asking you to provide feedback or take a survey.
- **To improve our website, products, and services:** Through data analysis, research, and development.
- **To administer and protect our business and website:** Including troubleshooting, data analysis, support, and reporting.
- **To deliver relevant website content to you:** And measure or understand the effectiveness.
- **To make suggestions and recommendations to you:** About products or services that may be of interest to you.
- **For marketing and promotional purposes:** To send you updates, newsletters, and promotional materials that may be of interest to you, where you have consented to receive such communications.
- **For recruitment and employment purposes:** To process job applications, manage employee records, and fulfill employment contracts.
- **To comply with legal and regulatory obligations:** Including responding to lawful requests from public authorities.

Processed Data by service as a Reverb client

Reverb does not directly store confidential or sensitive data to perform work with clients. Reverb collects personal information including name and email which are collected to schedule meetings and communicate on a lawful basis defined by GDPR. Reverb stores communications and contact information within their Hubspot CRM software and Reverb Google applications. Contacts stored have expressed legitimate interest as a prospect/lead, legitimate interest as an existing customer, when the communication is necessary to the performance of a contract or when they have freely given consent.

- Leadership Coaching service - name and email stored within Hubspot. Coaching goals and sometimes personal development plans or behavioral assessments

are stored in Google Drive with restricted sharing permissions and need to know access to this information.
- Facilitation - name and email stored within Hubspot. Survey feedback, and sometimes personal development plans or behavioral assessments are stored in Google Drive with restricted sharing permissions and need to know access to this information.
- HR Consulting - name and email for main contacts stored within Hubspot. All other data is managed on client owned systems and processed per client's data protection methods.
- Recruiting - name, email, work history, references all stored within BambooHR ATS system.

7. Data Sharing and Disclosure

Data Recipients: Google Workspace and Hubspot CRM are the primary recipients of data; this is where Reverb's data is stored. Other critical systems with data include PandaDoc, BambooHR, Bill.com, BigTime, and Notion. A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

We may share your personal data with the following categories of recipients:

- **External Third Parties:**
    - Software service providers acting as processors who provide IT and system administration services, payment processing, marketing, and other business support services (Google Workspace, Hubspot, Quickbooks, BigTime).
    - Professional advisors acting as processors or joint controllers including lawyers, bankers, auditors, CPA's, and insurers who provide consultancy, banking, legal, insurance, and accounting services.

We require all third parties to adhere to the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them access to process your personal data for specified purposes and in accordance with our instructions.

Third-Party Risk Management

Since Reverb does not have developed systems, software, applications, or SaaS products and only utilizes vetted third-party tools, managing third-party risks is critical. Our process for managing these risks includes:

- **Tool Evaluation and Reputation:** Employees must evaluate the security of any tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. Employees should use only reputable tools and avoid using tools developed by individuals or companies without established reputations. It is Reverb policy to use only internal Reverb tools when working with client data, otherwise, all client data is required to be removed prior to use of a third party tool. When a tool is selected for company use, its data protection and security are reviewed.

- **Due Diligence Questions for Third-Party Tools:** Before engaging with a third-party tool, we verify:
  - If they are certified by a reputable security organization (ISO, SOC).
  - If they are transparent about their security policies and procedures.
  - Review documented privacy and data collection policies of the vendor.
  - How effective their incident response is, including how they identify, prioritize, and remediate vulnerabilities in their systems.
  - What data of our organization a third party can access.
  - If multi-factor authentication is in place.
  - The compliance status or assessment/audit status at least once every 12 months (e.g., PCI compliance, any other accreditation or licensing required for that industry).

8. Data Retention: Minimization, Validation, and Deletion

We will only retain your personal data for as long as necessary to fulfill the legitimate business purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements.

- **Record Retention:** We retain non-sensitive data connected to the data subject as long as this is necessary for our legitimate business purposes. We consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. We comply with documented retention requirements specified by clients in the client service agreement and schedule of services contract by tracking this in our CRM on the project or customer record.
- **Data Validation:** Data is validated when it is collected, created, and updated to maintain integrity and accuracy. If a Data Subject and Reverb disagree about whether Client

Personal Data is complete and accurate, Reverb will escalate the issue to the Client and cooperate with the Client as necessary to resolve the issue. Reverb documents instances of disagreement and escalates issues to clients.

- **Deletion:** You have the right to request that we delete your data. We will do so, provided that we do not have a compelling reason for keeping it. To request deletion, please email privacy@reverbpeople.com.

9. Your rights as a data subject

Depending on your jurisdiction, you may have the following rights regarding your personal data:

- **Right to be informed:** The right to be informed about how your personal data is processed.
- **Right of access:** The right to request access to your personal data.
- **Right to rectification:** The right to request correction of inaccurate or incomplete personal data.
- **Right to erasure ("right to be forgotten"):** The right to request deletion of your personal data under certain circumstances.
- **Right to restrict processing:** The right to request the restriction of processing of your personal data under certain circumstances.
- **Right to data portability:** The right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit those data to another controller.
- **Right to object:** The right to object to the processing of your personal data under certain circumstances, including for direct marketing.
- **Rights in relation to automated decision-making and profiling:** The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.
- **Right to withdraw consent:** Where we are relying on consent to process your personal data, you have the right to withdraw that consent at any time.

To exercise any of these rights, please contact us using the contact details provided on the last page.

10. Reporting Data or Security Concerns

Responsible Disclosure Program

Reverb is committed to protecting the privacy and security of our data and our clients' data. While we primarily rely on third-party vendors for our technical infrastructure, we value the security community's efforts in identifying potential vulnerabilities.

If you believe you have discovered a security vulnerability related to Reverb's use of our third-party tools or our operational processes, we encourage you to report it to us responsibly. Please contact us immediately at support@reverbpeople.com.

We request that you:

- Provide detailed information about the vulnerability, including steps to reproduce it, potential impact, and any proof-of-concept.
- Do not disclose the vulnerability publicly until we have had an opportunity to address it.
- Do not exploit the vulnerability beyond what is necessary to demonstrate it.
- Avoid privacy violations, destruction of data, or interruption of our services.

We will acknowledge your report promptly, investigate the issue thoroughly, and keep you informed of our progress. We are committed to ensure the safety and privacy of our data.

Reporting security concerns: There are a variety of security concerns that you may experience, and each should be reported accordingly. Our Support Team needs to know about successful breaches, sensitive documents and resources that you may have unintentionally discovered or that do not have proper security settings applied, and malware so they can better protect our data. For this reason, we ask you to report these instances as soon as possible to privacy@reverbpeople.com. If you receive phishing or other suspicious emails, please report these to Google immediately via the "Report Spam" or "Report Phishing" feature in the drop-down list at the top right corner of the message in Gmail. Reporting these instances allows Google to investigate and prevent future similar attempts.

11. Client Partnership

We agree to assist Client, through appropriate technical and organizational measures, insofar as possible, to fulfill its obligations to respond to requests for Data Subjects seeking to exercise their Data Subject Rights. Unless otherwise directed by Client, Reverb will refer all Data Subjects who contact Reverb directly to Client to exercise their Data Subject Rights. Supplier will communicate to the Data Subject the steps that person must take to gain access to or otherwise exercise their rights vis-à-vis their Client Personal Data. We will refer all Data Subjects who contact Reverb, directly to Client to exercise their Data Subject Rights. Complaints for indications of any unauthorized or Unlawful Processing of Client Personal Data will be directed to privacy@reverbpeople.com.

If the data subject request is denied, at Client's direction, provide the Data Subject with a written explanation that is consistent with any relevant instructions previously provided by Client.

Reverb will maintain the integrity of all Client Personal Data, ensuring it remains accurate, complete and relevant for the stated purposes for which it was Processed. Data is validated when it is collected, created and updated.

To exercise your rights, or if you have any questions about our processing of your personal data, please contact us via email at privacy@reverbpeople.com.

If you would like to review Reverb's full Information Security and Governance Policies. Please reach out to privacy@reverbpeople.com and we can provide upon request.

Data Controller Contact Information

The data controller responsible for your personal information is:
Mikaela Kiner Coaching and Consulting, LLC dba Reverb
ATTN: COO, 6523 California Ave. SW #220 Seattle, WA. 98136
Email: privacy@reverbpeople.com
If you have any questions about this Privacy Notice or our data collection practices, please contact us at the email address above.