DATA PROCESSING AGREEMENT

A. Roles and Responsibilities

For the purposes of data protection laws, Tribu World SL ("Provider") acts as the Data Controller for any personal data collected directly from Customers using our Services. When the Provider processes personal data on behalf of the Customer, particularly if the Customer uses the Services to store or process data related to individuals within their community or organization, the Provider may act as a Data Processor.

B. Data Processing Scope and Purpose

The Provider processes personal data only as necessary to deliver the Services and for the following purposes:

- Account Management: To register and manage Customer accounts.
- Subscription and Payment Processing: To handle billing and financial transactions.
- Service Improvement: To analyze usage data and optimize features.
- Compliance: To adhere to legal obligations, such as anti-fraud measures.

The specific categories of data processed may include, but are not limited to, names, email addresses, phone numbers, billing information, and any other data provided by the Customer.

C. Customer Obligations

As a Data Controller, the Customer agrees to:

- Ensure that all personal data provided to the Provider has been collected in compliance with applicable data protection laws.
- Inform data subjects, as required by law, of the Provider's role in processing personal data.
- Obtain all necessary consents and permissions from data subjects before sharing personal data with the Provider.

D. Data Processor Obligations (Article 28 of GDPR)

When the Provider acts as a Data Processor on behalf of the Customer, the following terms apply:

- Processing Instructions: The Provider will process personal data only in accordance with documented instructions from the Customer, unless required by law to act otherwise.
- Confidentiality: The Provider ensures that any personnel authorized to process personal data are bound by confidentiality obligations.

- Security Measures: The Provider implements appropriate technical and organizational measures to protect personal data, as outlined in Article 32 of the GDPR, to ensure a level of security appropriate to the risk.
- Sub-processors: The Provider may engage third-party sub-processors to facilitate the provision of Services. A list of such sub-processors will be made available to the Customer upon request. The Provider ensures that any sub-processors are bound by equivalent data protection obligations.
- Data Breach Notification: In the event of a personal data breach, the Provider will notify the Customer without undue delay and provide sufficient information to assist the Customer in meeting any legal obligations to report or inform data subjects of the breach.
- Assistance with Data Subject Rights: The Provider will assist the Customer, insofar as possible, to respond to requests from data subjects exercising their rights under data protection laws, such as access, rectification, erasure, and data portability.

E. Data Transfer and International Processing

The Provider may transfer personal data to countries outside the European Economic Area (EEA) as necessary to provide the Services. In such cases, the Provider ensures that appropriate safeguards, such as Standard Contractual Clauses (SCCs), are in place to protect the personal data in accordance with Chapter V of the GDPR.

1. Data Retention

The Provider will retain personal data only for as long as necessary to fulfill the purposes for which it was collected or to comply with applicable legal, regulatory, or contractual retention obligations. Upon termination of the Services or at the Customer's request, the Provider will delete or return all personal data, unless retention is required by law.

2. Data Protection Impact Assessment (DPIA)

If required by applicable data protection laws, the Provider will assist the Customer in carrying out a Data Protection Impact Assessment (DPIA) related to the processing activities covered under these Terms. This includes providing necessary documentation and information to evaluate the impact of the data processing operations.

3. Audit Rights

The Customer has the right to audit the Provider's compliance with data protection obligations under this agreement. Such audits must be:

- Pre-scheduled: Conducted during normal business hours with reasonable notice.
- Non-disruptive: Carried out in a manner that does not disrupt the Provider's operations.
- Limited in Scope: Focused solely on data protection practices relevant to the processing of personal data on behalf of the Customer.

The Provider may provide access to documentation or conduct virtual audits to satisfy this requirement.

4. Data Subject Rights and Requests

The Provider will inform the Customer of any data subject requests related to the processing of personal data, such as requests for access, correction, or deletion. It is the Customer's responsibility to handle these requests unless the Provider is legally required to respond. If assistance is needed, the Provider will provide reasonable support to the Customer.

5. Termination and Data Deletion

Upon termination of the Services, the Provider will, at the Customer's direction, either delete or return all personal data processed on behalf of the Customer. If deletion is not possible, the Provider will continue to protect the personal data and restrict any further processing until deletion is possible.

Contact for Data Protection Inquiries
For data protection-related questions or concerns, please contact us at:
Email: info@tribuworld.net