1. Introduction

At RAWTech ("we," "us," "our") respect the privacy rights of our users ("users," "you," and "you're") and recognize the importance of protecting the information we collect about you. Our commitment to protecting the privacy and security of data extends beyond mere compliance; we are committed to protecting the privacy and security of our employees, customers, and partners. This Data Protection and Privacy Policy outlines our practices concerning the collection, use, and safeguarding of personal data.

2. Data Collection Practices

2.1. We collect personal information in the following ways:

- **Directly**: Such as when you register for an account, subscribe to our newsletters, or contact us with inquiries.
- **Indirectly**: Via usage data, cookies, and similar technologies when you use our services or visit our websites.

2.2. **What Data is Collected:** RAWTech collects data necessary for effective service delivery, including but not limited to:

2.2.1. **Customer Data:**

- **Personal Identification Information:** Full name, billing and shipping addresses, email addresses, and telephone numbers for order processing, customer service, and to provide updates and marketing communications.
- **Financial Information:** Payment card details or financial account information, processed securely for transaction purposes, without RAWTech retaining full details.
- **Usage Data:** Collected via cookies and analytics tools, this information helps us understand how our digital services are used and how we can improve user experience.

2.2.2. **Employee Data:**

- **Employment and Background Information:** Including job titles, work history, educational background, and potentially, background checks. Utilized for employment purposes, performance assessments, and regulatory compliance.
- **Sensitive Information:** Such as national identification numbers or health information for benefits administration and emergency contact details for safety purposes, under strict confidentiality.

2.3. How Data is Used

We may use your collected information to:

- **To Fulfill Our Services:** Processing orders, delivering services, and facilitating payments.
- **Communication**: Communicate important notices and promotional materials
- **For Improvement and Innovation:** Analyzing how our services are used to enhance user experience and develop new features.
- **Regulatory Compliance:** Meeting legal obligations and regulatory requirements.
- **Security Purposes:** To protect against fraud, abuse, and unauthorized access.

2.4. How We Protect Your Data

Our commitment extends to implementing robust technical and organizational measures, including but not limited to encryption, access control, secure software development practices, and regular security training for our staff.

3. Consumer Rights

Every individual whose data we hold has the right to:

- **Right to Access their data:** Individuals can request copies of their personal information.
- **Right to Rectification:** Individuals can request correction of personal data.
- **Right to Erasure:** Individuals can request deletion of personal data in certain conditions.
- **Right to Restrict Processing:** Limiting how we use personal data.
- **Right to Data Portability:** Individuals can request personal data in a common format.
- **Right to Object:** Individuals can object to certain types of data processing, including for marketing purposes.

We will not sell, lease, or share your personal information with third parties outside of RAWTech without your consent, unless required by law.

Requests related to these rights can be directed to our Data Protection Officer via dpo@rawtechs.com.

4. Data Security Measures

RAWTech employs robust security methods to prevent unauthorized data access, including:

- **Encryption:** Both at rest and in transit, using modern algorithms to ensure that data intercepted by unauthorized entities is unreadable.
- **Layered Security:** Implementation of firewalls, intrusion detection systems, and regular security audits.
- **Access Control:** Ensuring only authorized personnel have access to sensitive data, based on the principle of the least privilege.
- **Employee Training:** Comprehensive training programs on data protection for all employees.
- **Physical Security:** Access controls to data centers and secure disposal of data-bearing devices.
- **Regular Security Assessments:** Conducting vulnerability scans and penetration testing to identify and rectify potential security loopholes.

5. External Websites

Our website may contain links to other websites. We are not responsible for the privacy practices of third-party websites.

6. Data Breach Response Plan

Should a data breach occur, our predetermined plan includes:

- **Immediate Detection and Assessment:** Identifying the cause and extent of the breach.
- **Containment and Eradication:** Limiting the breach's impact and removing vulnerabilities.
- **Notification:** Informing affected parties and regulatory authorities, if applicable, within the timeframe mandated by law.
- **Post-Incident Analysis:** A thorough investigation to prevent future incidents, including but not limited to a review of existing security protocols and the implementation of additional safeguards.

7. Consent Procedures for Data Collection

Consent is obtained through:

- **Explicit Consent:** Providing clear, understandable consent forms detailing the intended use of collected data.
- **Documentation:** Keeping detailed records of consent instances, including digital acknowledgements.
- **Revocation of Consent:** Offering straightforward mechanisms for individuals to withdraw consent.

8. Encryption Standards and Procedures

Data is encrypted using:

- **End-to-End Encryption (E2EE):** Ensuring that data is encrypted on the sender's system and only decrypted on the recipient's system.
- **Public Key Infrastructure (PKI):** Utilizing a combination of public and private cryptographic keys to secure data in transit.
- **Data Encryption Standard Compliance:** Adhering to AES, RSA, and other established encryption standards for data at rest and in transit.
- **AES-256 for Data at Rest:** Ensuring stored data is secured against unauthorized access.
- **TLS 1.3 for Data in Transit:** Providing secure communication channels over the internet.

Regular updates and patches are applied to maintain the highest level of security against emerging threats.

9. Personal Privacy Undertaking

We respect personal privacy by:

- **Minimizing data collection** - Only collecting data that is directly relevant and necessary.
- **Transparency** - Being clear about how we collect, use, and share personal data.
- **Secure Data Handling** - Implementing stringent data handling and processing protocols to safeguard data privacy.

10. Modifications and Updates

This policy is reviewed periodically to ensure it remains compliant with the latest regulatory and technological standards. RAWTech commits to proactively informing stakeholders of significant policy amendments through our official communication channels. Your continued use of our services signifies your acceptance of any changes.

11. Contact Information

For privacy inquiries or concerns, please contact our Data Protection Officer at dpo@rawtech.com, or write to us at:

RAWTech Privacy Office
[United States]

Last Updated: [02/18/2024]

This policy constitutes a commitment to uphold the highest standards of data protection and privacy for all stakeholders involved with RAWTech.