Privacy and Data Handling Policy

Effective Date: 22/08/2022

Last Updated: 22/08/2022

At The Acorn Solution, we are committed to protecting the privacy and security of the data that we collect, process, store, and share on behalf of our users. This Privacy and Data Handling Policy explains how we collect, process, use, store, share, and dispose of information, including Personally Identifiable Information (PII), in compliance with Amazon's Acceptable Use Policy (AUP), Data Protection Policy (DPP), and applicable data privacy laws.

1. Data Collection

We collect data through the Amazon Services API to provide functionality to Authorized Users as defined by Amazon. The types of data we collect include:

- **Personally Identifiable Information (PII):** Customer names, addresses, email addresses, contact information, and shipping details required to facilitate order fulfilment for merchant-fulfilled orders.
- **Non-PII Data:** Order details, inventory levels, and shipment tracking information necessary for business operations.

We ensure that we only collect data that is necessary to perform these business-critical functions and never request unnecessary or unrelated information.

2. Data Processing

Data collected through the Amazon Services API is used solely to perform essential functions on behalf of Authorized Users. These include:

- Processing and fulfilling customer orders, including generating shipping labels and providing shipment tracking.
- Ensuring compliance with tax, regulatory, and legal requirements.
- Supporting any additional features requested by Authorized Users, such as order management and inventory tracking.

Any analytical or automated processes (e.g., AI models) used to process this data are thoroughly tested and are disclosed to Authorized Users with clear documentation of their accuracy and purpose.

3. Data Storage

All data is securely stored using Amazon Web Services (AWS) infrastructure, employing industry-standard security protocols, including:

- **Encryption:** All PII and sensitive data are encrypted both at rest and in transit using AES-256 encryption.
- **Access Control:** We enforce strict access control policies, ensuring that only authorized personnel with a business need can access the data.
- **Data Retention:** We retain PII and other data for a period of 90 days after collection unless otherwise required by law. After this period, data is securely deleted from our systems unless retention is mandated for legal or compliance purposes.

4. Data Usage

The data we collect is used exclusively for the following purposes:

- Processing orders for merchant-fulfilled shipping.
- Generating shipping labels and providing shipment tracking.
- Compliance with legal, tax, and regulatory obligations.
- Providing Authorized Users with business-critical insights, in full compliance with Amazon's Acceptable Use Policy.

We do not use data for marketing, advertising, or any other unauthorized purposes.

5. Data Sharing

We only share data when it is necessary to complete essential business functions, and we take rigorous steps to ensure data is handled securely by any third-party service providers:

- **Third-Party Sharing:** Data may be shared with third-party logistics providers to facilitate order fulfilment. All third-party providers are subject to stringent data security standards that meet or exceed our own policies.
- **Affiliated Entities:** We may share data with affiliated entities that play a role in providing the Authorized User services, provided these entities adhere to data protection standards.
- **Compliance:** Data may also be shared when required by applicable law or to comply with regulatory requirements.

Under no circumstances do we sell or share data for marketing purposes, nor do we aggregate or share data across Authorized Users.

6. Data Disposal

When data is no longer needed, it is securely deleted from our systems according to the following process:

- **Data Deletion:** After a 90-day retention period, all PII and non-essential data is permanently deleted from our servers unless required by law for a longer retention period.
- **Authorized User Requests:** Authorized Users may request data deletion at any time, and we will comply promptly by securely disposing of the data within our systems.

7. Security Measures

We implement comprehensive security measures to protect the data we handle, including:

- **Encryption:** All PII is encrypted both at rest and during transmission.
- **Access Control:** Strict access control policies limit access to data on a need-to-know basis within our organization. Only authorized employees and contractors have access to data required to perform their tasks.
- **Multi-Factor Authentication (MFA):** We utilize MFA to secure access to our systems and data.
- **Regular Audits:** We conduct regular security audits and vulnerability assessments to ensure our data protection protocols remain effective and up-to-date.

8. Compliance with Data Protection Laws

We comply with all relevant data protection regulations, including the **General Data Protection Regulation (GDPR)**, **California Consumer Privacy Act (CCPA)**, and other applicable privacy laws. In the event of any data breaches or incidents, we will follow the appropriate notification procedures outlined by these laws.

9. User Rights and Transparency

We are fully transparent with Authorized Users regarding the data we collect, process, and share. Authorized Users have the following rights:

- **Right to Access:** Authorized Users can request access to the data we hold on their behalf.
- **Right to Deletion:** Authorized Users can request the deletion of their data at any time.
- **Right to Correction:** Authorized Users can request corrections to any inaccurate data we hold.

10. Changes to the Policy

We may update this Privacy and Data Handling Policy periodically to reflect changes in our services or legal requirements. Authorized Users will be notified of any significant changes to our policies via email or through our application.