

## **PRIVACY POLICY**

### **31Labels by Anush**

(A brand of Ahaya Supermart Private Limited)

**Effective Date:** February 26, 2026

**Last Updated:** February 26, 2026

Ahaya Supermart Private Limited operating its brand 31Labels, an ecommerce market place ("**31Labels**", "**we**", "**us**", or "**our**") adheres strictly to all the applicable legislation and regulations relating to the protection of data and processing, storage, usage, collection and/or application of such data including without limitation the Digital Personal Data Protection Act, 2023 and rules 2025 made therein ("**DPDP Act**") as a Data Fiduciary under Section 2(g) of the Act, the Information Technology Act, 2000 ("**IT Act, 2000**"), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and any other applicable rules framed thereunder; and all other guidelines (whether statutory or non-statutory) ("**Data Protection Legislation**") when processing your digital personal data for shipping purposes on <https://31labels.store/>. This enhanced Shipping Policy integrates Data Protection Legislation compliances, ensuring transparent notice, informed consent, purpose limitation, and robust data safeguards for shipping-related activities.

**Ahaya Supermart Private Limited** is a company incorporated under the Companies Act, 2013, with its registered office at, Mumbai, Maharashtra, India. We operate a curated online fashion marketplace connecting customers with independent designers and brands through our website <https://31labels.store/> and mobile application (collectively, the "Platform").

By accessing or using the Platform, you ("you", "your", "Customer", "Data Principal") expressly consent to the collection, processing, storage, sharing, and transfer of your Personal Data as described in this Privacy Policy. If you do not agree with the terms of this Privacy Policy, please discontinue use of the Platform immediately.

**We are committed to protecting your privacy and handling your Personal Data responsibly and transparently.**

For the purposes of this Privacy Policy:

- a. "**Personal Data**" means any data about an individual who is identifiable by or in relation to such data, including demographic, contact, financial, and online identifiers.
- b. "**Data Principal**" means the individual to whom the Personal Data relates (i.e., you, the customer/user).
- c. "**Data Fiduciary**" means any person who alone or in conjunction with others determines the purpose and means of processing Personal Data (i.e., Ahaya Supermart Private Limited for the purposes of the DPDP Act).

- d. **"Data Processor"** means any person who processes Personal Data on behalf of a Data Fiduciary.
- e. **"Processing"** means any operation or set of operations performed on Personal Data, including collection, recording, storage, retrieval, use, sharing, erasure, or destruction.
- f. **"Sensitive Personal Data"** includes financial information (such as bank account details, credit/debit card information), passwords, biometric information, physical or mental health records, sexual orientation, and any other category designated as sensitive under applicable law. Payment instrument details such as credit/debit card information are processed through certified third-party payment gateway providers and are not stored on our servers, except in tokenized or masked form as permitted by applicable law.
- g. **"Child"** means an individual below the age of 18 years.

## **4. PERSONAL DATA WE COLLECT**

We collect and process the following categories of Personal Data:

### **4.1 Information You Provide Directly**

#### **4.1.1 Account and Profile Information:**

- a. Full name, email address, mobile number, date of birth, gender, profile picture
- b. Shipping and billing addresses
- c. Account credentials (username, password—stored in encrypted form)

#### **4.1.2 Transaction and Payment Information:**

- a. Order details (products purchased, order value, order history)
- b. Payment method details (card type, last four digits of card number, bank name, UPI ID)
- c. Transaction identifiers and payment status
- d. Billing and shipping addresses for each order

#### **4.1.3 Communication and Support Data:**

- a. Correspondence via email, chat, phone calls, or support tickets
- b. Customer service queries, complaints, feedback, reviews, ratings
- c. Survey responses and promotional participation data

#### **4.1.4 User-Generated Content:**

- a. Product reviews, ratings, comments, photos uploaded by you
- b. Wish lists, shopping cart information, product preferences

## **4.2 Information We Collect Automatically**

### **4.2.1 Technical and Device Information:**

- a. IP address, device type, operating system, browser type and version
- b. Device identifiers (IMEI, MEID, advertising ID)
- c. Mobile network carrier, screen resolution, time zone settings

### **4.2.2 Usage and Behavioral Data:**

- a. Pages viewed, time spent on pages, clickstream data, search queries
- b. Products browsed, items added to cart or wish list
- c. Referral source, exit pages, session duration

### **4.2.3 Location Data:**

- a. Approximate location derived from IP address
- b. Precise geolocation (with your explicit consent for location-based services such as store locator or delivery tracking)

### **4.2.4 Cookies and Tracking Technologies:**

- a. Session cookies, persistent cookies, pixel tags, web beacons, log files
- b. Analytics tools (Google Analytics, Firebase Analytics)
- c. Social media plugins (Facebook, Instagram, WhatsApp)

## **4.3 Information from Third-Party Sources**

- a. Updated delivery address and contact information from logistics partners
- b. Payment verification and fraud detection data from payment gateways and banks
- c. Social media profile information (name, profile picture, email) when you sign in via Facebook, Google, or Apple ID (with your consent)
- d. Credit bureau information for fraud prevention and risk assessment (where legally permitted)

## **5. PURPOSES OF PROCESSING PERSONAL DATA**

We collect and process personal data solely for lawful purposes connected with providing, operating, improving, and securing the Platform, including:

- (a) creation and management of user accounts;
- (b) processing and fulfilment of orders;
- (c) facilitating payments and refunds;
- (d) customer support and grievance redressal;
- (e) fraud prevention and platform security;
- (f) compliance with applicable legal and regulatory obligations; and
- (g) sending transactional communications.

We shall not process personal data for purposes incompatible with the above without obtaining additional consent where required under applicable law.

## 6. CONSENT MECHANISM

### 6.1 Free, Specific, Informed, and Unambiguous Consent

Your consent for processing Personal Data is obtained through clear affirmative action, such as:

- a. Ticking a checkbox during account registration or checkout
- b. Clicking "I Agree" or "Accept" buttons
- c. Opting in to receive marketing communications
- d. Granting permissions for location access, camera, gallery, notifications (for mobile app users)

### 6.2 Notice at the Point of Collection

Before or at the time of collecting your Personal Data, we provide you with a clear and concise notice specifying:

- a. What Personal Data we collect
- b. The purposes for which it will be processed
- c. Categories of third parties with whom it may be shared
- d. Your rights under the DPDP Act
- e. How to withdraw consent

### 6.3 Granular Consent for Specific Purposes

We seek separate consent for distinct purposes, such as:

- a. Marketing communications (SMS, email, WhatsApp, push notifications)
- b. Location-based services
- c. Sharing data with third-party partners for analytics or advertising
- d. Processing Sensitive Personal Data (payment information, health data if applicable)

### 6.4 Withdrawal of Consent

You have the **right to withdraw your consent** at any time. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

#### **How to Withdraw Consent:**

- a. **For Marketing Communications:** Click the "Unsubscribe" link in any promotional email, or adjust notification preferences in your account settings (Profile > Communication Preferences).
- b. **For Location Access:** Disable location permissions in your device settings (Settings > Apps > 31Labels > Permissions).

- c. **For Account Data Processing:** Contact our Grievance Officer or Data Protection Officer (details in Section 14 below) with a written request to withdraw consent.

**Timeframe for Processing Withdrawal:** We will process your consent withdrawal request within **7 business days** of receipt. Upon withdrawal, we will cease processing your Personal Data for the relevant purpose and notify any third-party processors to do the same, except where processing is required by law or for existing contractual obligations.

**Consequences of Withdrawal:**

- a. Withdrawal of consent for account data processing may result in closure of your account and deletion of your data (subject to legal retention obligations).
- b. Withdrawal of consent for location services will disable location-based features (store locator, delivery tracking).
- c. Withdrawal of marketing consent will stop promotional communications but not transactional messages (order confirmations, shipping updates).

**7. CONSEQUENCES OF REFUSAL TO PROVIDE PERSONAL DATA**

Certain Personal Data is **mandatory** for us to provide you with our services. Refusal to provide such mandatory data may result in the following consequences:

<b>Data Requested</b>	<b>Purpose</b>	<b>Consequence of Refusal</b>
Name, Email, Mobile Number	Account creation and identity verification	You will not be able to create an account or place orders on the Platform.
Shipping Address	Order delivery	We cannot process or deliver your order without a valid shipping address.
Payment Information	Transaction processing	Payment cannot be completed; order will not be confirmed.
Billing Address	Invoice generation and tax compliance	Order may be cancelled or delayed pending receipt of billing information.
Age Verification (for restricted products)	Legal compliance (e.g., alcohol, tobacco-related accessories)	You will not be able to purchase age-restricted products.
OTP Verification	Account security and fraud prevention	Account creation or login may be blocked to prevent unauthorized access.

**Optional Data:** Providing optional data (such as date of birth, gender, profile picture, preferences) helps us personalize your experience and offer targeted recommendations, but refusal will not prevent you from using core Platform services.

## **8. COOKIES AND TRACKING TECHNOLOGIES**

Due to the communications standards on the Internet, when you visit, access or browse the Platforms, we automatically receive the uniform resource locator of the site from which you visit, access or browse the Platforms, details of the website you visit on leaving the Platforms, the internet protocol (“IP”) address of each User’s computer operating system, type of web browser the User is using, email patterns, and the name of the User’s internet service provider. This information is used solely to analyse overall User trends and to help us improve our services. Please note that the link between the User’s IP address and the User’s personally identifiable information is not shared with third parties without such User’s permission or except when required by law or to provide or facilitate the User with the services. Notwithstanding the above, the User acknowledges that we reserve the right to share some of the aggregate findings, including the personal information provided by the Users in an unidentifiable, aggregate form, and not the specific data with advertisers, sponsors, investors, strategic partners, and others in order to help grow the business. The amount of information sent to us depends on the settings of the web browser used by the User to access the Platforms. The User may refer to the browser used, if the User wishes to learn what information is provided to us.

The Platforms use temporary cookies to store certain data. We do not store Personal Information in the cookies. Information collected by us, by any means whatsoever, that does not personally identify the User as an individual (such as patterns of utilization described above) is exclusively owned by us and may be used by us and third-party service providers for technical administration of the Platforms, user administration, research, development, and other purposes.

You understand that you may set or amend your web browsers to delete or disable cookies. If you choose to disable cookies on your computer or mobile telecommunication device, it may impair, degrade or restrict access to certain areas of the Platforms.

We may allow other companies or entities to serve advertisements that may be of interest to you. These companies or entities include third party advertisement servers, advertisement agencies, advertisement technology vendors and research firms. In the course of serving advertisements or optimizing the services to Users, we may allow authorised third parties to place or recognize a unique cookie on the User’s browser.

You agree and understand that we do not exercise control over third party websites displayed as search results or links on the Platforms. These other sites may place their own cookies or other files on the Users’ computer, collect data or solicit personal information from the Users, on which we have no control and shall not be held responsible or liable. We do not make any representations concerning the privacy practices or policies of such third parties or terms of use of such websites, nor do we guarantee the accuracy, integrity, or quality of the information, data, text, software, sound, photographs, graphics, videos, messages or other materials available on such websites. The inclusion or exclusion does not imply any endorsement by us of such websites, the websites’ provider, or the information on the website.

We may keep records of telephone calls received from and made to Users for the purpose of administration of services, research and development, training, business intelligence, business

development, or for User administration. We may share such telephone records with third parties when required by law or when required to provide or facilitate the User with the services.

You consent to our reproduction/publishing of all testimonials and reviews given by you on the Platforms in relation to the services or the Products. You agree that we may edit the testimonials and reviews provided by you and reproduce/publish such edited or paraphrased versions of the testimonials and reviews on the Platforms. If the User has any concerns with the reproduction/publication of any testimonial or review provided by you, the User may contact us at [help@31labels.com](mailto:help@31labels.com).

## **8.1 Types of Cookies We Use**

### **8.1.1 Strictly Necessary Cookies (Essential)**

- a. Enable core Platform functionality (login, shopping cart, checkout)
- b. Maintain session security and prevent fraud
- c. Remember your language and region preferences
- d. **Cannot be disabled** as they are essential for Platform operation.

### **8.1.2 Performance Cookies (Analytics)**

- a. Collect anonymous data on how visitors use the Platform (pages visited, time spent, bounce rate)
- b. Help us identify technical errors and improve website performance

Examples: Google Analytics, Firebase Analytics

### **8.1.3 Functional Cookies (Preference)**

- a. Remember your settings and preferences (display name, currency, shipping address)
- b. Enable social media sharing and embedded content (YouTube videos, Instagram feeds)
- c. Improve user experience by remembering your choices

### **8.1.4 Targeting/Advertising Cookies (Marketing)**

- a. Track your browsing behavior across websites to display personalized ads
- b. Measure effectiveness of advertising campaigns

Examples: Facebook Pixel, Google Ads, Criteo

## **8.2 Third-Party Cookies**

We may allow third-party service providers (analytics tools, advertising networks, payment gateways) to place cookies on your device. These third parties have their own privacy policies governing the use of cookies.

### **8.3 Managing Cookies**

You can control and manage cookies through your browser settings:

- a. **Chrome:** Settings > Privacy and Security > Cookies
- b. **Safari:** Preferences > Privacy > Cookies and Website Data
- c. **Firefox:** Options > Privacy & Security > Cookies and Site Data

For more information about cookies, visit [www.allaboutcookies.org](http://www.allaboutcookies.org).

## **9. SHARING AND DISCLOSURE OF PERSONAL DATA**

We may share personal data only on a need-to-know basis with:

- (a) Sellers for the purpose of fulfilling orders placed through the Platform;
- (b) logistics and delivery partners;
- (c) payment gateway providers;
- (d) analytics and cloud service providers;
- (e) professional advisors; and
- (f) governmental or regulatory authorities where legally required.

All third parties are contractually bound to maintain confidentiality and implement reasonable security safeguards.

### **9.4 Legal and Regulatory Authorities**

We may disclose your Personal Data to government authorities, law enforcement agencies, courts, regulatory bodies, or other third parties where required by law or where we have a legitimate interest to do so, including:

- a. In response to court orders, subpoenas, search warrants, or legal processes
- b. To comply with tax, accounting, and audit requirements
- c. To investigate or prevent fraud, security breaches, or illegal activities
- d. To protect the rights, property, or safety of 31Labels, our customers, or the public
- e. In connection with legal proceedings, regulatory inquiries, or enforcement of our Terms of Use

### **9.5 Business Transfers**

In the event of a merger, acquisition, reorganization, sale of assets, or bankruptcy, your Personal Data may be transferred to the acquiring entity or successor, subject to the same data protection standards as outlined in this Privacy Policy. We will notify you of any such change in ownership or control of your Personal Data.

## 9.6 With Your Consent

We may share your Personal Data with other third parties where you have provided explicit consent for such sharing (e.g., participation in co-branded promotions, referral programs, or integration with third-party apps).

## 10. DATA SECURITY

### 10.1 Security Measures

We are committed to protecting your Personal Data from unauthorized access, alteration, disclosure, or destruction. We implement **reasonable technical, organizational, and physical security safeguards**, including:

#### Technical Measures:

- a. Encryption of Sensitive Personal Data (payment information, passwords) using industry-standard protocols (SSL/TLS, AES-256)
- b. Secure payment gateways compliant with PCI-DSS standards
- c. Multi-factor authentication (OTP verification) for account access
- d. Regular security audits, vulnerability assessments, and penetration testing
- e. Firewalls, intrusion detection systems, and anti-malware software

#### Organizational Measures:

- a. Access controls and role-based permissions (employees and contractors access data only on a need-to-know basis)
- b. Confidentiality agreements and data protection training for employees
- c. Incident response plan and data breach notification procedures
- d. Regular review and update of security policies

#### Physical Measures:

- a. Secure data centers with restricted access, surveillance, and environmental controls
- b. Backup and disaster recovery mechanisms to prevent data loss

### 10.2 Data Breach Notification

In the event of a **personal data breach** that is likely to cause significant harm to you (such as financial fraud, identity theft, or unauthorized disclosure of Sensitive Personal Data), we will:

- a. Notify the **Data Protection Board of India** (or other relevant authority) within the timeframe prescribed under the DPDP Act and DPDP Rules, 2025.

- b. Inform you directly via email, SMS, or in-app notification, providing details of the breach, potential impact, and steps you should take to protect yourself.
- c. Take immediate remedial measures to contain the breach and prevent further unauthorized access.

### 10.3 Third-Party Security

We require all third-party service providers, data processors, and business partners to implement appropriate security measures and comply with data protection obligations through binding contracts and data processing agreements.

### 10.4 Your Responsibility

You are responsible for:

- a. Maintaining the confidentiality of your account credentials (username, password, OTP)
- b. Using strong, unique passwords and enabling two-factor authentication where available
- c. Logging out of your account after each session, especially on shared or public devices
- d. Reporting any suspected unauthorized access or security breach to our Grievance Officer immediately

**We will never ask you for your password, OTP, CVV, PIN, or full card number via phone, email, or SMS. Beware of phishing attempts and fraudulent communications impersonating 31Labels.**

## 11. DATA RETENTION AND ERASURE

### 11.1 Retention Period

Retention periods vary depending on the category of data and legal/regulatory requirements:

Data Category	Retention Period	Basis for Retention
Account Information	Duration of account + 3 years' post-closure	Customer relationship management, legal compliance
Order and Transaction Data	7 years from date of transaction	Accounting, tax, and audit requirements (Income Tax Act, GST Act)
Payment Information	1 year days (tokenized thereafter)	PCI-DSS compliance, fraud prevention
Communication Records (emails, chat logs)	3 years from last interaction	Customer support, dispute resolution
Marketing Consent Logs	Duration of consent + 2 years post-withdrawal	Compliance audit, consent management

Grievance/Complaint Records	5 years from resolution	Legal compliance (Consumer Protection Act)
Website/App Logs, Cookies	13 months	Analytics, security monitoring (DPDP Rules)

## 11.2 Deletion and Anonymization

Once the retention period expires and we no longer have a lawful basis to retain your Personal Data, we will:

- a. **Delete** the data securely and irreversibly from our active systems and backups, or
- b. **Anonymize** the data such that it can no longer be linked to you as an identifiable individual, and may retain it for statistical analysis or research purposes.

## 11.3 Legal Holds

In certain circumstances, we may be required to retain Personal Data beyond the standard retention period due to:

- a. Ongoing litigation, investigation, or regulatory inquiry
- b. Unresolved disputes or grievances
- c. Legal hold notices or court orders

## 12. CROSS-BORDER DATA TRANSFER

### 12.1 Transfer Outside India

Your Personal Data may be **transferred to, stored in, or processed in countries outside India** for the purposes described in this Privacy Policy, including:

- a. Cloud storage and hosting services (e.g., servers located in Singapore, United States, European Union)
- b. Payment processing through international payment gateways
- c. Customer support services provided by offshore service providers

Analytics and marketing tools operated by global technology companies

### 12.2 Safeguards for Cross-Border Transfer

We ensure that cross-border transfers of your Personal Data are subject to **appropriate safeguards** to protect your privacy rights, including:

- Entering into **Standard Contractual Clauses (SCCs)** or **Data Processing Agreements (DPAs)** with third-party recipients that impose binding data protection obligations.
- Transferring data only to countries that have been **approved by the Central Government of India** under the DPDP Act as providing adequate data protection standards.

- Ensuring that recipients implement **reasonable security safeguards** equivalent to those required under Indian law.

### 12.3 Restricted Countries

We will **not transfer** your Personal Data to any country or jurisdiction that has been **notified as a restricted country** by the Central Government of India under Section 16 of the DPDP Act, unless explicitly required by law or with your explicit consent.

### 12.4 Data Localization

Certain categories of Sensitive Personal Data (such as payment information, biometric data) may be stored exclusively within India in compliance with applicable data localization requirements.

## 13. CHILDREN'S DATA AND PARENTAL CONSENT

### 13.1 Age Restriction

Our Platform and services are **not directed to children** below the age of **18 years** ("Child" or "Minor"). We do not knowingly collect, process, or solicit Personal Data from children.

#### **If you are under 18 years of age:**

- a. You must **not** create an account, place orders, or provide any Personal Data on the Platform without the consent of your parent or legal guardian.
- b. If you wish to use the Platform, you must have your parent or legal guardian create an account on your behalf and supervise your use.

### 13.2 Verifiable Parental Consent Mechanism

In the event that we offer services that may be used by children (such as gift registries, educational content, or family accounts), we will implement a **verifiable parental consent mechanism** as required under the DPDP Act and DPDP Rules, 2025, which includes:

#### **Step 1: Age Verification**

- a. Requiring users to provide their date of birth during registration.
- b. Using age-gating mechanisms to identify users below 18 years.

#### **Step 2: Parental Identity and Relationship Verification**

- a. Verifying the identity and age of the parent or legal guardian through government-backed systems such as **DigiLocker**, Aadhaar-based e-KYC, or other secure methods.
- b. Confirming the legitimacy of the parent-child relationship through documentary evidence (birth certificate, Aadhaar card showing relationship, school records).

### **Step 3: Obtaining Verifiable Consent**

- a. Seeking explicit, affirmative consent from the verified parent or guardian through a dedicated consent form or digital signature.
- b. Providing clear notice to the parent/guardian about:
  - i. What Personal Data of the child will be collected
  - ii. How it will be used and shared
  - iii. The child's rights and the parent's right to withdraw consent
  - iv. Contact details for grievance redressal

### **Step 4: Maintaining Records**

- a. Keeping detailed records of the age verification process, parental identity verification, and consent documentation for audit purposes.

### **13.3 Prohibition on Tracking and Behavioral Monitoring**

We will **not engage in tracking, behavioral monitoring, or targeted advertising** directed at children, in compliance with Section 9 of the DPDP Act.

### **13.4 If We Discover We Have Collected Children's Data**

If we become aware that we have inadvertently collected Personal Data from a child without verifiable parental consent, we will:

- a. Delete such data immediately and permanently from our systems.
- b. Notify the parent or guardian (if contact information is available).
- c. Take steps to prevent future collection of children's data without proper consent.

### **13.5 Parental Rights**

Parents or legal guardians of children may exercise the following rights on behalf of the child:

- a. Request access to the child's Personal Data
- b. Request correction or deletion of the child's Personal Data
- c. Withdraw consent for processing the child's Personal Data
- d. Lodge a grievance regarding the processing of the child's Personal Data

Parents may contact our Data Protection Officer or Grievance Officer (details in Section 14 below) to exercise these rights.

## **14. GRIEVANCE REDRESSAL AND DATA PROTECTION**

## 14.1 Grievance Redressal

In accordance with the Information Technology Act, 2000 and the Consumer Protection Act, 2019, address Your complaints and concerns relating to the Platform, including issues regarding, account access, orders, refunds, and content.

### Grievance Details:

1	Name:	Khushi Singh
2	Designation:	Grievance Officer
3	Postal Address:	SanRaj Corporate Park - 4th Dimension, 4th floor, Mindspace, Malad (West), Mumbai 400064
4	Contact Number:	8879043131
5	Email:	<a href="mailto:help@31labels.com">help@31labels.com</a>

## 14.2 Timeline for Grievance Redressal

- a. **Resolution:** We will endeavor to resolve your grievance within **15 business days** from the date of acknowledgment, or such other period as may be prescribed under applicable law (up to a maximum of 30 days for complex matters).

## 14.3 Data Fiduciary Role under the DPDP Act

For the purposes of the Digital Personal Data Protection Act, 2023, **Ahaya Supermart Private Limited** acts as a **Data Fiduciary** in respect of the Personal Data collected from you through the Platform. We process your Personal Data only for **lawful purposes**, as described in Section 5 of this Privacy Policy, and in compliance with the obligations under Sections 8 and 9 of the DPDP Act.

## 14.4 Data Protection Officer (if applicable)

As of the date of this Privacy Policy, we are **not notified** as a "Significant Data Fiduciary" (SDF) by the Central Government under Section 10 of the DPDP Act. If in the future we are classified as a Significant Data Fiduciary, we will:

- a. Appoint a **Data Protection Officer (DPO)** resident in India, whose contact details will be published on this page.
- b. Conduct periodic **Data Protection Impact Assessments (DPIAs)** to identify and mitigate risks to Data Principals.
- c. Undertake **annual data audits** by independent auditors to verify compliance with the DPDP Act.
- d. Implement additional security safeguards and transparency measures as prescribed under the DPDP Rules for Significant Data Fiduciaries.

You will be notified of any change in our status and the updated contact details for the Data Protection Officer.

## 14.5 Notice and Consent Obligations

Before or at the time of collecting your Personal Data, we provide you with a **clear and concise notice** (through privacy notices, pop-ups, consent forms, or account settings) specifying:

- a. The categories of Personal Data to be collected
- b. The purposes of processing
- c. The categories of third parties with whom data may be shared (e.g., logistics partners, payment gateways, sellers, marketing platforms)
- d. Your rights under the DPDP Act (access, correction, erasure, grievance redressal, nomination)
- e. The mechanism for withdrawing consent

Your consent is obtained through **affirmative action** (such as ticking a checkbox, clicking "I Agree", or enabling permissions), and you may withdraw your consent at any time (see Section 6.4).

## 14.6 Data Security and Breach Notification

We implement **reasonable security safeguards** as contemplated under Section 8 of the DPDP Act to protect your Personal Data (see Section 10 for details). In the event of a **personal data breach** that is likely to cause significant harm to you, we will:

- a. Notify the **Data Protection Board of India** (or other relevant authority) within the prescribed timeframe.
- b. Inform you of the breach and any steps you may need to take to mitigate potential harm (see Section 10.2).

## 14.7 Data Retention and Erasure Obligations

We retain your Personal Data only for as long as necessary to fulfil the purposes for which it was collected, or as required under applicable law (see Section 11 for retention periods). Once the relevant purpose has been fulfilled and retention is no longer necessary, we will delete, anonymize, or irreversibly de-identify your Personal Data, subject to any statutory retention obligations.

## 15. DATA PRINCIPAL RIGHTS UNDER THE DPDP ACT

As a Data Principal, you have the following rights under the Digital Personal Data Protection Act, 2023, which you may exercise subject to applicable law:

### 15.1 Right to Access (Section 11)

You have the right to obtain from us:

- a. A summary of the Personal Data we hold about you and how it is being processed.
- b. Information about the identities of Data Processors and other Data Fiduciaries with whom your Personal Data has been shared.

**How to Exercise:**

Log in to your account and navigate to **Profile > My Data**. Alternatively, send a written request to our Grievance Officer at [help@31labels.com](mailto:help@31labels.com) with the subject line "Data Access Request". We will provide the requested information within **7 business days**, in a clear and accessible format.

### 15.2 Right to Correction (Section 12)

You have the right to request correction, completion, or updating of your Personal Data if it is inaccurate, incomplete, or out-of-date.

**How to Exercise:**

You may update your account information (name, email, mobile number, addresses) directly by logging into **Profile > Edit Profile**. For corrections to order history, transaction records, or other data not accessible through your account, contact our Grievance Officer at [help@31labels.com](mailto:help@31labels.com) with the subject line "Data Correction Request". We will process your request within **5 business days**.

### 15.3 Right to Erasure (Section 13)

You have the right to request deletion of your Personal Data where:

- a. The purpose for which it was collected has been fulfilled.
- b. You have withdrawn consent (where processing was based on consent).
- c. Retention is no longer necessary for legal or business purposes.

**How to Exercise:**

To delete your account and Personal Data, log in to **Profile > Account Settings > Delete My Account**, or send a written request to [help@31labels.com](mailto:help@31labels.com) with the subject line "Data Erasure Request". Upon verification of your identity, we will permanently delete your Personal Data within **30 days**, except where retention is required by law (e.g., for tax, accounting, fraud prevention, or ongoing legal proceedings).

**Exceptions:**

We may refuse or delay erasure if:

- a. Retention is required under applicable law (e.g., Income Tax Act, GST Act, Consumer Protection Act).
- b. There is an ongoing dispute, investigation, or legal proceeding involving your account.

- c. Erasure would prejudice our ability to defend legal claims or enforce our Terms of Use.

#### 15.4 Right to Grievance Redressal (Section 11(3))

You have the right to lodge a grievance regarding the processing of your Personal Data and to receive a response within the prescribed timeline.

##### **How to Exercise:**

Contact our Grievance Officer (details in Section 14.1) via email, phone, or postal mail. We will acknowledge your grievance within **24 hours** and resolve it within **15 business days** (or up to 30 days for complex matters). If you are not satisfied with the resolution, you may approach the **Data Protection Board of India** (once constituted) or other relevant authorities.

#### 15.5 Right to Nominate (Section 14)

You have the right to **nominate another individual** (such as a family member, legal heir, or trusted person) who shall, in the event of your **death or incapacity**, exercise your rights under the DPDP Act on your behalf, including the rights to access, correct, erase, and grievance redressal.

**"Incapacity"** means the inability to exercise your rights due to mental or physical limitations, as certified by a competent medical authority.

##### **How to Exercise:**

Log in to your account and navigate to **Profile > Nomination Settings**. Provide the nominee's full name, relationship to you, contact details (email and mobile number), and upload supporting documentation (if required). Alternatively, send a written nomination request to [help@31labels.com](mailto:help@31labels.com) with the subject line "Data Nomination Request", including:

- a. Your full name and account details
- b. Nominee's full name, relationship, and contact information
- c. A signed declaration authorizing the nomination

##### **Nominee's Rights:**

Upon your death or incapacity, the nominee may exercise your rights by providing us with:

- a. **Proof of your death** (death certificate issued by competent authority), or
- b. **Proof of your incapacity** (medical certificate from a registered medical practitioner or court order declaring incapacity).
- c. **Proof of nominee's identity** (government-issued ID, Aadhaar, PAN, etc.).

We will verify the nominee's entitlement and process their request within **15 business days**.

## **Updating or Revoking Nomination:**

You may update or revoke your nomination at any time by logging into your account or by sending a written request to the Grievance Officer.

## **16. WITHDRAWAL OF CONSENT MECHANISM**

You have the **right to withdraw your consent** for the processing of your Personal Data at any time, in accordance with Section 6(4) of the DPDP Act. Withdrawal of consent must be as easy as giving consent.

### **16.1 How to Withdraw Consent**

#### **For Marketing Communications (Email, SMS, WhatsApp, Push Notifications):**

- a. Click the "**Unsubscribe**" link at the bottom of any promotional email.
- b. Reply "**STOP**" to any promotional SMS.
- c. Adjust notification preferences in **Profile > Communication Preferences** and uncheck relevant options (promotional emails, SMS, WhatsApp updates, push notifications).

#### **For Location Access:**

- a. Disable location permissions in your device settings: **Settings > Apps > 31Labels > Permissions > Location > Deny**.

#### **For Cookies and Tracking:**

- a. Manage cookie preferences through our **Cookie Consent Banner** (displayed on first visit) or by visiting **Preferences > Cookie Settings** in your browser.

#### **For Account Data Processing (Entire Account):**

- a. Send a written request to [help@31labels.com](mailto:help@31labels.com) with the subject line "**Withdrawal of Consent – Full Account**", stating clearly that you wish to withdraw all consent for processing your Personal Data.

### **16.2 Timeline for Processing Withdrawal**

Upon receipt of your withdrawal request, we will:

- a. **Acknowledge** your request within **24 hours**.
- b. **Cease processing** your Personal Data for the relevant purpose within **7 business days**.

- c. **Notify any third-party Data Processors** to cease processing and erase relevant data, except where processing is required by law or for existing contractual obligations.

### 16.3 Effect of Withdrawal

- a. **Lawfulness of Prior Processing:** Withdrawal of consent will **not affect** the lawfulness of processing that occurred before the withdrawal.
- b. **Contractual Obligations:** If processing is necessary for the performance of a contract (e.g., to fulfill an order you have already placed), we may continue processing until the contract is completed, after which your data will be deleted (subject to legal retention requirements).
- c. **Legal Obligations:** If processing is required by law (e.g., tax records, regulatory reporting), we may continue to retain and process your data to comply with such obligations, but only for the minimum period required.

### 16.4 Consequences of Consent Withdrawal

Consent Withdrawn	Consequence
Marketing Communications	You will stop receiving promotional emails, SMS, WhatsApp messages, and push notifications. Transactional messages (order confirmations, shipping updates, security alerts) will continue.
Location Access	Location-based features (store locator, delivery tracking, region-specific content) will be disabled.
Account Data Processing	Your account will be closed, and your Personal Data will be deleted (subject to legal retention obligations). You will no longer be able to place orders, access order history, or use the Platform.
Cookies and Tracking	Personalization and targeted advertising will be disabled. Strictly necessary cookies (required for website functionality) will continue to function.

### 16.5 Withdrawal Does Not Require Justification

You are **not required to provide any reason or justification** for withdrawing your consent. We will process your request without undue delay.

## 17. LINKS TO THIRD-PARTY WEBSITES AND SERVICES

Our Platform may contain links to third-party websites, social media platforms, payment gateways, or other online services operated by independent parties (such as brand websites, influencer blogs, partner stores, or external payment providers). These third-party sites have their own **separate privacy policies** and are not governed by this Privacy Policy.

#### We are not responsible for:

- a. The privacy practices, data protection measures, or content of third-party websites.
- b. Any loss, damage, or breach of privacy resulting from your interaction with third-party sites.

#### We strongly encourage you to:

- a. Review the privacy policies of any third-party website before providing your Personal Data.
- b. Exercise caution when clicking on external links or sharing information with third parties.

#### **Examples of Third-Party Links:**

- a. Social media sharing buttons (Facebook, Instagram, Pinterest, Twitter)
- b. Payment gateway pages (Razorpay, Paytm, PhonePe)
- c. Brand or designer websites linked from product pages
- d. Customer review platforms or blogs

## **18. UPDATES AND MODIFICATIONS TO THIS PRIVACY POLICY**

We reserve the right to **update, modify, or revise** this Privacy Policy from time to time to reflect changes in:

- a. Our business practices, products, or services.
- b. Applicable laws, regulations, or industry standards (such as amendments to the DPDP Act or issuance of new DPDP Rules).
- c. Feedback from customers, regulators, or auditors.

### **18.1 Notification of Changes**

- a. **Effective Date:** Any changes to this Privacy Policy will be effective from the date specified in the "Last Updated" field at the top of this page.
- b. **Notice to You:** We will notify you of material changes by:
  - i. Displaying a prominent notice on the Platform (banner, pop-up, or in-app notification).
  - ii. Sending an email or SMS to your registered contact details (where legally required or where changes significantly affect your rights).
  - iii. Posting the updated Privacy Policy on this page with a revised "Last Updated" date.

### **18.2 Your Acceptance of Changes**

- a. **Continued Use = Acceptance:** By continuing to access or use the Platform after the updated Privacy Policy becomes effective, you acknowledge that you have read, understood, and agreed to the updated terms.
- b. **Objection to Changes:** If you do not agree with the updated Privacy Policy, you must discontinue use of the Platform and may request deletion of your account and Personal Data by contacting our Grievance Officer.

### **18.3 Version History**

We maintain a version history of this Privacy Policy for transparency and audit purposes. Previous versions may be requested by contacting [help@31labels.com](mailto:help@31labels.com).

## **20. GOVERNING LAW AND JURISDICTION**

This Privacy Policy and any disputes arising out of or in connection with the processing of your Personal Data shall be governed by and construed in accordance with the **laws of India**, including:

- a. The Digital Personal Data Protection Act, 2023
- b. The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- c. The Consumer Protection Act, 2019
- d. Other applicable Indian laws and regulations

Any disputes shall be subject to the exclusive jurisdiction of the **courts in Mumbai, Maharashtra**, India, unless otherwise prescribed by the Data Protection Board of India or other competent authority under the DPDP Act.

## **END OF PRIVACY POLICY**

**Ahaya Supermart Private Limited**

Operating as: **31Labels by Anush**

Website: <https://31labels.store/>

Email: [help@31labels.com](mailto:help@31labels.com)

Last Updated: 11<sup>th</sup> March, 2026