

Annapurna Tech Universe Private Limited

Privacy Policy

A-Pay Application

Updated: 29th January 2026

INTRODUCTION

The term "Company", "we", "our" or "us" refer to Annapurna Tech Universe Private Limited registered at Registrar of Companies (ROC) on the records of the Ministry of Corporate Affairs (MCA), under the Companies Act, 2013 having its registered office at Plot No. 3753, KHATA No.1594, Ghatikia, Khandagiri, Bhubaneswar, Khorda- 751030, Orissa.

We have developed a mobile application called "**A-Pay**" (referred to as "Application" or "Platform"). This Application enables Customer(s), also referred to as "you" or "End-Users", to conveniently make loan repayments, bill payments and recharges, online shopping and other value added services.

When you use our application, you are entrusting us with your personal information ("Personal Information"). We highly value your privacy and are committed to protecting it by adhering to this privacy statement. This Privacy Policy ("Policy") governs the collection, storage, use, and processing of Personal Information by the Application, a service provided by us, including but not limited to loan repayments, bill payments and recharges, online shopping and

other value added services. By accessing or using the A-Pay application, you agree to the terms outlined in this policy.

This Policy outlines how A-Pay Application gathers, retains, employs, and manages your Personal Information across various mediums, including our websites, applications, mobile sites, chatbots, notifications, or any other means employed by A-Pay to deliver its services (referred to as the "Platform"). By visiting, downloading, or using the A-Pay Platform, and/or sharing your information or utilizing our products/ services, you explicitly consent to abide by this Policy and the relevant terms and conditions. We highly value the trust you bestow upon us and prioritize the safeguarding of your privacy, ensuring the highest standards for secure transactions and protection of your personal data.

This Policy complies with Indian laws, rules and regulations, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 , as per the Information Technology Act, 2000. These Indian laws, rules and regulations necessitate the publication of a privacy policy governing inter alia the practices relating to collection, usage, storage, transfer, and disclosure of Personal Information. Personal Information encompasses data associated with a specific individual and includes sensitive personal information, which necessitates heightened protection measures due to its sensitive and personal nature. This Policy is aligned with Indian laws, and the processing of your Personal Information will adhere to these laws as our products/ services are exclusively offered to Indian customers in India. If you do not agree with this Policy, kindly refrain from using or accessing our Platform.

1. Collection of Personal Information

1.1 Information Gathered

We collect the below mentioned personal information when you use our services or interact with us. This information may include, but is not limited to:

- **Identification Data:** Name, DOB, gender, phone number, collected at the time of registration on the App, which is required to enable you to login to the App and for us to: verify your identity, determine your eligibility for using its proprietary technology; and safeguard against illegal activities such as fraud, cheating, misappropriation, etc.
- **Verification Information:** OTPs received from A-Pay Application for verifying your phone number for Login.
- **Device Information:** Information about your device, including the device identifier are required to identify the user and prevent the user to login the app from multiple devices.
- **Cookies & Tracking:** Cookies, which will help in identifying your browser or A-Pay Application. Additionally, data about the time spent, IP address are required to identify the device so as to safeguard against illegal activities such as fraud, cheating, misappropriation, etc.
- **Media Permissions:** Camera Permission, Read External Storage, and Read Media Image: Our app allows users to upload their photos to make the app more intuitive. To enable this feature, we request camera permission, read external storage permission, and read media image permission for new devices. By granting access, users can seamlessly take pictures within the app or choose existing photos from their gallery.
- **Communication Permissions:** SMS, Calls & Contact Permission- To ensure secure onboarding and account setup, we access specific SMS (OTP) solely to verify your mobile number and bind the SIM for UPI registration. This is a mandatory step as per NPCI guidelines to authenticate UPI users. Our app uses Call permission to verify that a valid SIM card is inserted in the device during registration or login. This step is essential to prevent fraudulent activities and unauthorized access to UPI services. To enhance user convenience, we request access to your contacts solely to allow easy selection of numbers for mobile prepaid recharges.

- **Location Permission:** We access location permission to determine available products and delivery feasibility of the ecommerce services and other value added services.
- **Internet Permissions:** Internet Permissions and Access to Wi-Fi State: These permissions are essential for the app to connect to the internet.
- **Biometric Permission:** Our app prioritizes user safety and privacy by offering a seamless biometric login experience. Instead of remembering complex passwords, users can simply use their fingerprint to securely access their accounts.

2. Purpose and Use of Information

A-Pay may process the information collected as mentioned above for purposes, including but not limited to:

- **Account Management:** Creation of user accounts, ensuring identity authentication, and granting access and privileges.
- **Payment Processing:** Execution of payment processes, communication for query resolutions, transactional facilitation, and compliance with pertinent regulatory stipulations.
- **Transaction Security:** Authentication of transactional requests, validation of standing instructions, and confirmation of payments.
- **User Experience:** Enhancement of user experiences through comprehensive analysis of aggregated user behavior data.
- **Service Management:** Monitoring, review, and customization of services to ensure user safety, convenience, and regulatory compliance, inclusive of audit processes.
- **Terms Enforcement:** Enforcement of applicable terms and conditions, dissemination of information regarding online/offline offers, products, services, and updates.

- **Dispute Resolution:** Resolution of disputes, provision of technical support, rectification of system anomalies, and ensuring service safety and integrity.
- **Security & Fraud Prevention:** Detection of security breaches, prevention of illegal activities, and undertaking of forensic audits as part of internal or external audits or investigations.
- **Legal Compliance:** Compliance with legal obligations while endeavouring to minimize intrusive processing to safeguard user privacy.

3. Cookies and Similar Technologies

We utilize "**cookies**" and similar technologies on our platform to enhance user experience, analyze web page flow, and measure promotional effectiveness. These technologies help in providing targeted information and features. You have the option to manage cookies via your browser settings, although this might affect certain platform features.

4. Sharing and Disclosure of Information

Your Personal Information is shared in accordance with applicable laws, following due diligence and aligned with the outlined purposes in this Policy.

We may share your Personal Information with various entities, including **business partners, service providers, regulatory bodies, governmental authorities, financial institutions, and internal teams** such as security and investigation teams.

This sharing of Personal Information, as applicable, is based on a need-to-know basis and serves various purposes, including but not limited to:

- Facilitating the provision of products/services availed by you and enabling services between you and the relevant service providers.
- Completing payment transactions initiated by you on merchant sites, where merchants request your Personal Information based on your instructions obtained from us.
- The customer's phone number is shared with the TSP of the BBPS (Bharat Bill Payment System) service provider for facilitating BBPS transactions. This is done in strict compliance with regulatory requirements and for the legitimate purpose of processing bill payments.
- Meeting requirements from financial institutions for **fraud prevention, risk management, fund recovery**, as per applicable laws/regulations.
- Rendering services related to **communication, data storage, transmission, security, analytics, fraud detection, risk assessment, and research**.
- Enforcing our Terms or Policy and responding to claims of violations or protecting the rights, property, or safety of users or the public.
- Complying with legal requirements, court orders, or other legal processes in good faith, as reasonably necessary.
- Responding to government authorities' requests for initiatives and benefits and resolving grievances or disputes.
- Collaborating with internal investigation departments within us or agencies appointed by us for investigative purposes within or outside Indian jurisdiction.
- In the event of mergers, acquisitions, or restructuring our business, sharing information with relevant entities.

While information is shared with third parties as per this Policy, the processing of your Personal Information is regulated by their policies. We ensure **stricter or no less stringent privacy protection obligations** are imposed on these third parties, wherever applicable and feasible to inter alia ensure that the third party receiving sensitive information does not disclose it further. However, we may share Personal Information with legally recognized authorities, regulatory

bodies, governmental authorities, and financial institutions as per the purposes outlined in this Policy or in compliance with applicable laws. We do not assume responsibility or liability for the use of your Personal Information by these third parties or their policies.

The Company or any person on its behalf shall not publish sensitive personal data or information.

5. Storage and Retention

Where applicable, we store Personal Information within India, abiding by applicable laws, and retain it for a duration necessary for the purpose it was collected. However, we may retain Personal Information related to you if deemed necessary to prevent fraud or abuse, or if required by law due to legal/regulatory proceedings or directives. Upon reaching the retention period, Personal Information is deleted in compliance with applicable laws.

We may share personal information with various entities or recipients for specific purposes as permitted by law or outlined in this Policy. Recipients include:

- Business partners, service providers, merchants, regulatory bodies, financial institutions, etc.
- Third parties for transaction fulfillment, communication, and service-related activities.
- Internal departments for purposes outlined in this Policy.
- Governmental authorities or agencies as required by law.

6. Reasonable Security Practices

We prioritize the security of your personal and sensitive information. We have implemented **administrative, technical, and physical security measures** to

safeguard your data. While we strive for an effective security system, we acknowledge that no system is entirely impenetrable.

As part of our reasonable security practices, we conduct [rigorous internal and external reviews](#) to ensure robust information security. This includes [encryption and controls for both data in motion and data at rest](#) within our network and servers. Our databases are stored on servers protected by [firewalls, with access restricted through password protection and strict limitations](#).

You play a crucial role in maintaining the confidentiality and security of your A-Pay account. Please refrain from sharing your [login ID, password, and OTP details](#) with anyone. It is your responsibility to promptly inform us of any actual or suspected compromise on your personal information.

To enhance security, we offer [multiple levels of protection](#) within the A-Pay Application. This includes features such as a [login/logout option](#) and the ["Enable Screen Lock"](#) feature, allowing you to add an extra layer of security to your application. We have implemented preventive controls to ensure that your A-Pay account remains secure on your device, and login credentials cannot be used on a different device without additional authentication/OTP.

7. Third-Party Products, Services, or Websites

When using A-Pay, you may find links to other websites or applications. These operate under their own privacy policies, beyond our control. Once you leave our platform, your data is governed by the privacy policy of the visited site or app. Review their policies before proceeding, as they may differ from ours. We hold no responsibility for how third parties handle your information. For concerns, contact the domain owner directly.

8. Your Consent

We process your Personal Information with your consent. By utilizing the A-Pay platform or services and/or by providing your Personal Information, you **explicitly consent to the processing of your Personal Information by us**, adhering to the terms outlined in this Policy.

If you share Personal Information related to other individuals, you affirm that you possess the authority to do so and grant us permission to utilize the information in accordance with this Policy.

9. Privacy Controls

You have choices about the information we collect and how we use it:

- **Device-level settings:** Controls on your device may determine what information we collect.
- **Delete Account:** Delete your App account entirely.
- **Content Removal:** You may also request that content be removed from our servers in accordance with applicable law.

10. Modifications to Policy

Due to the dynamic nature of our business operations, our policies will undergo alterations. We retain the exclusive discretion to amend, adjust, supplement, or remove segments of this Policy **without prior written notice to you**. We will post the changes on the website to keep you updated on the changes. Although we will make reasonable efforts to notify you of these modifications, **it remains your responsibility to periodically review this Policy** for updates or alterations on our website. Your continual usage of our services/Platform subsequent to the publication of such modifications implies your acceptance and consent to the revised terms. It is assured that alterations to policies will never compromise the protection of Personal Information already disclosed by you.

11. Contact Information

Have Questions or Concerns?

If the user has any complaints or concerns including those pertaining to breach of Terms of Use, Privacy Policy and other policies or questions can drop an email to:

 support@atu.co.in

We are committed to responding to your queries within a reasonable timeframe. Any delays in resolution will be communicated to you proactively.

Geographic Scope

This app works in **INDIA**. Deactivate/Delete account links also work in **INDIA**.