

AS-FinMobile Privacy Policy

Armsoft is committed to protecting your privacy. This Policy describes how the AS-FinMobile mobile application (“Application”) may collect, use and disclose information from or about you and explains how the information may be disclosed or used.

Agreement to Policy

By using the AS-MobileBank mobile application, you signify that you have read, understood, and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Policy.

Collecting, Using and Sharing: Information that we collect

The Application obtains the information you provide when you download and login the Application. Login is optional. However, please keep in mind that you may not be able to use some of the features offered by the Application unless you login.

For a better experience, while using our Application, we may require you to provide us with certain personally identifiable information. When you use the Application, you generally provide (a) your username, password and other information necessary to login, such as one-time passwords; (b) transaction-related information, such as transactions and account numbers when you make payments and transfers; (c) information you provide us when you contact us for help; (d) information you enter into our system when using the Application, such as utility contract information; (e) information resulting from your mobile activity.

The app does use third-party services that may collect information used to identify you. Links to the privacy policies of third-party service providers used by the Application:

- [Firebase Analytics](#)

Automatically Collected Information

The Application may collect certain information automatically, including, but not limited to, the type of mobile device you use, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the Application.

Log Data

Whenever you use our Application, in a case of an error we collect data and information (through third-party products) on your phone called Log Data. This Log Data may include information such as your device Internet Protocol (“IP”) address, device name, operating system version, the configuration of the app when utilizing our Service, the time and date of your use of the Service, and other statistics.

Device Permissions

Depending on the user's specific device and operating system, this Application may request certain permissions that allow it to access the user's data as described below. Some permissions require explicit consent from the user, while others may be granted automatically or do not require user approval due to being categorized as “normal” permissions. Users can manage or revoke any granted permissions at any time through their device settings. However, revoking certain permissions may impact the proper functioning of the Application.

Permissions that Require Explicit User Consent

These permissions must be actively granted by the user:

- Biometric Authentication (Face ID / Fingerprint) – Used to verify your identity when logging into pages that contain sensitive or secret information.
- Calendar Access – Allows the app to access calendar information, typically to display or manage date-specific data.
- Access to Device Storage (Read) – Enables the app to read files from your device’s storage.
- Access to Device Storage (Write) – Enables the app to save files or data to your device.

Permissions Granted Automatically or Considered “Normal”

These permissions are generally granted at installation or do not require a prompt:

- Internet Access – Required for the app to connect to the internet and exchange data with servers.
- Network State Access – Used to detect whether the device is connected to a network and the type of connection.
- Vibration Control – Allows the app to trigger vibrations, for example, as a notification method.
- Screenshot Detection – Used to detect when a screenshot is taken for security or monitoring purposes. This does not involve accessing personal data and typically does not require user permission.

Security Measures

We are concerned about safeguarding the confidentiality of your information. We protect information you provide us in several ways. We use encryption standards and SSL (Secure Socket Layer) technology to help ensure that information is passed without being intercepted by third parties. User Names, Passwords and one-time passwords are used to safeguard access to your information through AS-FinMobile. But remember that no method of transmission over the internet, or method of electronic storage is 100% secure and reliable, and we cannot guarantee its absolute security. We strongly encourage you to assist us in that effort by not sharing your AS-FinMobile Usernames and Passwords with anyone. In respect to any credit card or other

payment processing details you have provided us, we commit that this confidential information will be stored in the most secure manner possible.

[Changes](#)

This Policy is subject to change and any changes to this Policy will become effective once posted at this link. Thus, you are advised to review this page periodically for any changes. Your use of the Application following these changes means you accept the revised Policy.

[Contact Information](#)

If you have any questions or suggestions regarding this Privacy Policy, please contact us at support@armsoft.am. We will make every effort to resolve your concerns.