

Privacy Policy for WITNC

Last Updated: 13-Oct-2025

This Privacy Policy describes how WITNC collects, uses, and protects your information. Your privacy and security are the foundation of our Service.

Our Core Privacy Promise: Zero-Knowledge

We operate on a "zero-knowledge" principle. All of your sensitive asset and personal information ("Your Data") is encrypted on your device using your password before it is stored on our servers. We cannot decrypt, read, or access the contents of Your Data.

1. Information We Collect

- **Account Information:** We collect your email address to create and manage your account through Firebase Authentication.
- **Your Data (Encrypted):** We collect the information you enter into the app, which includes personal details, contact information for your lawyer, CA, and relatives, and details about your various assets. This information is always stored and handled in its encrypted form.
- **Recipient Information:** We collect the names, email addresses, and preferred languages of your designated Recipients to facilitate the data transmission process.
- **Configuration Data:** We store your well-being check preferences (frequency, threshold) and notification preferences (push, email).
- **Technical Information:** We may collect anonymous technical data for security and operational purposes, such as your device's FCM token for push notifications.

2. How We Use Your Information

- **To Provide the Service:** To securely store Your Data (encrypted), and to automatically transmit it to your Recipients according to the rules you set.
- **To Communicate With You:** To send you periodic well-being check notifications via push notification and/or email, as you have configured.
- **To Secure and Maintain the Service:** To authenticate you, process your settings, and ensure the operational integrity of the app.

3. Data Security

- **End-to-End Encryption:** Your Data is encrypted on your device and remains encrypted on our servers and during transmission.
- **Your Password as the Key:** Your password is the key to this encryption. It is never transmitted to us, and we cannot recover it. This ensures that only you can access your unencrypted data within the app.
- **Secure Infrastructure:** We use Google Cloud and Firebase, industry-standard secure cloud service providers, to host our backend and database.

4. Information Sharing and Disclosure

We do not share your information, except in the following limited circumstances:

- **With Your Designated Recipients:** The entire purpose of the Service is to share Your Data (in its encrypted form) with your Recipients when your well-being check threshold is met. We also use third-party services (like SendGrid) to deliver these notification emails.
- **With Service Providers:** We use third-party services like Google Cloud (for hosting and functions) and SendGrid (for email delivery) that process data on our behalf. These providers are bound by their own privacy policies.
- **For Legal Reasons:** We may disclose information if required to do so by law or in response to valid requests by public authorities.

5. Data Retention and Deletion

- Your Data is retained as long as your account is active.
- Upon the successful transmission of Your Data to your Recipients, your account and all associated data will be scheduled for permanent deletion from our systems after a period of one year.
- If you manually delete your account from within the app, your data will also be scheduled for permanent deletion.

6. Contact Us

If you have any questions about this Privacy Policy, please contact us at **optionsdelta24@gmail.com**