Privacy Policy for My Protection AI

Effective Date: 07/23/2025
Last Updated: 07/23/2025

My Protection AI respects your privacy and is committed to protecting it. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our online scam detection service (the "Service"). Please read this policy carefully to understand our practices regarding your information and how we will treat it.

At this time the Service is only available in the United States. We are not intending to collect or process data of individuals in any other territory.

1. Information We Collect

When you use the Service, we may collect the following information:

Personal Information:

- **Email and Text/ SMS Access**: To identify and alert you of potential scams, we may request access to your email and/ or your SMS/Text accounts. This includes the ability to read headers and content for scam detection purposes. Your emails, messages, and private information will not be recorded or taken from your device. We will store your email address for authentication. We will also collect your phone number to provide services for texting and for future two-factor authentication.
- **Contacts Information**: With your explicit permission, we may access your phone's contacts to cross-reference with known scam sources and provide enhanced scam prevention services.

Device Information:

- Information about the device you use to access the Service, including device model, operating system, browser, email provider, and unique device identifiers. This will ensure proper use of the Service on your device.

Cookies:

- We use cookies and similar tracking technologies on our website to enhance your experience, analyze site usage, and assist in our marketing

efforts. This includes cookies set by HubSpot, a third-party service we use for analytics and customer communication.

- HubSpot may place cookies in your browser to track how you interact with our site, including page views, referral sources, and engagement with content. These cookies do not store personal information unless you choose to provide it.

- You can control or disable cookies through your browser settings. For more information about the cookies HubSpot uses, please visit: https://knowledge.hubspot.com/privacy-and-consent/what-cookies-does-hubspot-set-in-a-visitor-s-browser

Usage Data:

- Details about how you use the Service, such as feature usage, errors, and diagnostics.

2. How We Use Your Information

We use the information we collect for the following purposes:

- **Scam Detection**: Analyze emails, texts, and contacts to identify and alert you to potential scams or malicious activity.

- **Service Improvement**: Improve the functionality, performance, and security of the Service.

- **User Support**: Respond to your inquiries and provide assistance related to the Service.

- **Legal Compliance**: Comply with applicable laws, regulations, and legal processes.

We retain your personal information for as long as we have an ongoing legitimate business need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax, or accounting requirements).

The criteria used to determine appropriate retention period for personal information include:

- The amount, nature, and sensitivity of the personal information.

- The purpose(s) for which the personal information was collected and used.

- Whether we have a legal obligation to retain personal information or

whether retaining personal information is necessary to resolve disputes, including the establishment, exercise, or defense of legal claims.

To improve scam detection capabilities, the Service may use automated systems to identify patterns and trends in the data it scans. These systems may generate aggregated insights to enhance detection algorithms and service performance. No personal or identifiable data is retained or used in these synthesized insights.

We do not store, log, or retain the contents of emails, messages, or files scanned by the Service beyond the scope of what is necessary to perform immediate detection functions.

3. How We Share Your Information

We do not sell your information to third parties. However, we may share your information in the following circumstances:

- **Service Providers**: With trusted third-party providers who perform functions necessary to operate the Service (e.g., cloud storage, analytics).
- **Marketing Service Providers:** With third parties, such as analytics providers (e.g., Google Tag Manager and Google Analytics) and social media platforms, for marketing and promotional purposes exclusive to promoting MyProtection.AI and relevant content therein. This may also include the use of text messaging (SMS) for limited marketing communications, subject to your consent and applicable laws. Message and data rates may apply.
- **Analytics and Advertising Partners:** With third party marketing tools, like email campaign providers or social media platform providers.
- **Legal Obligations**: When required to comply with a legal obligation or protect our rights, users, or the public.
- **Corporate Transactions:** In connection with the negotiation or execution of a merger or sale of our business.
- **Consent**: With your explicit consent, we may share information for other purposes not listed here.

4. How We Protect Your Information

We use industry-standard security measures to protect your information, including encryption, secure servers, and strict access controls. However, no method of transmission or storage is 100% secure, and we cannot

guarantee absolute security.

5. Your Choices and Controls

To the extent you are provided additional privacy rights in the state you reside, you have the following rights with respect to the information that we collect (in each case, subject to applicable law):

- Right to Know: To know the categories and specific personal information we have collected, the categories and sources from which we collected the personal information, the categories of third parties with whom we share personal information, and the business or commercial purpose for collecting or selling (if applicable) personal information, and the right to request information about and opt out of automated decision making (if applicable).
- Right to Access: To request a copy of the personal information that we have collected about you during the past 12 months.
- Right to Opt-Out of Sales or Sharing: To opt out of sales of personal information (if applicable) or sharing personal information for cross-contextual behavioral advertising.
- Right to Delete: To request that we delete the personal information that we have collected from you.
- Right to Correct: To correct inaccurate information that we maintain about you.
- Right to Limit Disclosure of Sensitive Information: To limit the disclosure of sensitive personal information, if we use or disclose sensitive personal information.
- Freedom from Discrimination: To exercise the rights described above free from discrimination or retaliation as prohibited under applicable law.
- Right to Opt-Out of the Sale or Sharing of Personal Information to Third Parties and California Shine the Light: Residents of the State of California have the right to request information from us regarding other companies to whom the company has disclosed certain categories of information during the preceding year for those companies' direct marketing purposes. If you are a California resident and would like to make such a request, please contact us.

6. Permissions Required for the Service

To provide scam detection services, the following permissions are required:

- **Email Account Access**: To scan for potential scams, we require access to your email account via secure APIs (e.g., Google Gmail API, Microsoft Graph API, Apple IMAP).
- **Contacts and Text Access**: To identify and notify you of potential scams from your unknown contacts or text messages, we require permission to access your phone's contacts and Text/SMS data accounts on both iOS and Android devices.

7. Third-Party Services

Our Service may use third-party services to process your information (e.g., email providers, telecommunications providers, cloud platforms, CRM, Stripe payment processing). These third parties are bound by their own privacy policies, which we encourage you to review.

8. Children's Privacy

a. Children Under 13

Our Services are **not directed to children under the age of 13**, and we do not knowingly collect personal information from children under 13. If we learn that we have collected personal information from a child under 13 without verified parental consent, we will promptly delete that information. If you believe that we may have collected information from a child under 13, please contact us at support@myprotection.ai.

b. Teens Ages 13 to 17

We recognize the importance of protecting the privacy of teens. If you are between the ages of 13 and 17, you may use our Services, but certain protections and rights apply:

- **Limited Data Collection:**
  We only collect the personal information necessary to provide our Services and to improve your user experience.
- **No Sale or Sharing Without Opt-In (Ages 13-15):**
  For California residents ages 13 to 15, we do not sell or share your personal information without your affirmative authorization ("opt-in") as required under the California Consumer Privacy Act (CCPA/CPRA). You may withdraw this authorization at any time by [describe how, e.g., updating your account settings or contacting us].
- **Right to Opt-Out (Ages 16-17):**
  If you are 16 or 17 years old, you have the right to direct us **not to sell or share your personal information** at any time. You can

exercise this right by visiting our "Do Not Sell or Share My Personal Information" page [or equivalent mechanism].

- **Age-Appropriate Notices:**
  We strive to provide privacy notices that are easy to understand and suitable for teen users.
- **Parental Inquiries:**
  Although we do not generally collect personal information from children under 13, parents or legal guardians who believe we have collected personal information from their child may contact us to review, correct, or delete that information.

c. Your Privacy Rights

If you are between the ages of 13 and 17 (or the parent or guardian of such a user), you have the right to:

- Request access to the personal information we have collected about you
- Request that we delete your personal information
- Request that we correct inaccurate personal information
- Opt-out of the sale or sharing of your personal information (as applicable to your age group)

9. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The most current version will be available on our website, and we will notify you of significant changes through the Service or other means.

10. Contact Us

If you have any questions about these Terms or the Service, please contact us at: support@myprotection.ai