AEGIS Privacy Policy

Effective Date: June 24, 2025

Aegis App Inc. (“AEGIS”) (“we,” “our,” or “us”) respects your privacy and is committed to protecting it through our compliance with this Privacy Policy. This Policy describes the types of information we may collect or that you may provide when you use our website, mobile application and services (the “Services”), and our practices for collecting, using, maintaining, protecting, and disclosing that information.

AEGIS does not sell your personal information, use it for targeted advertising, or engage in automated profiling that affects your rights.

We take your privacy seriously. This section explains how we collect, use, and share your information.

Defined Terms:

1. **AEGIS** – Aegis App Inc., including its affiliates and subsidiaries.

2. **App** – The AEGIS mobile application.

3. **Emergency Response Partner** – A trusted third-party service that coordinates emergency response on behalf of AEGIS.

4. **Emergency Service Providers** – Any third party (including Emergency Response Partners, first responders, medical centers, hospitals) that provides emergency response or healthcare services in connection with the Services.

5. **HIPAA** - Health Insurance Portability and Accountability Act of 1996.

6. **Services** – The website, App, and any services provided by AEGIS.

7. **Third-Party Service Providers** – Any external vendor, contractor, or partner (other than an Emergency Response Partner) engaged by AEGIS to support the Services, including hosting, analytics, communications, and infrastructure providers.

8. **User Data** – All personal, location, medical, and technical information collected from or about a user of the Services.

1. Information We Collect

We may collect the following types of data when you use our Services:

- **Account Information**. We may collect personal information in connection with the creation or administration of your Aegis account, such as your name, email address, phone number, addresses, and any other information that you provide to us or that we otherwise collect.

- **Emergency Contact Information.** Names and phone numbers of designated emergency contacts provided by you.

- **Optional Profile Information.** To help personalize your experience and support more effective emergency response, our Services allow you to add optional account details. This may include labeling frequent locations (e.g., home, work, school), entering personal identifiers such as your height, weight, gender, or providing health-related details like medical conditions, medications, allergies, or accessibility needs.

  All of this information is entirely optional and is used solely to enhance your safety by assisting Emergency Service Providers and improving the accuracy of our emergency support features. By providing this information, you consent to its use for these limited, safety-related purposes.

  Please note: AEGIS is not a healthcare provider and is not subject to the federal privacy rules that apply to doctors and hospitals under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). While we are committed to safeguarding your data, HIPAA protections do not apply to AEGIS directly. Some Emergency Service Providers we work with may be covered under HIPAA, and those providers will handle your information in accordance with their own privacy obligations.

- **Purchases**. If you choose to upgrade your account or make purchases within the Services, such as in-app purchases (such as subscribing to premium features), we may collect personal information related to the transaction, including billing details and purchase history. All payments are securely processed through third-party platforms, including Stripe (via our website) and the Apple App Store or Google Play. AEGIS does not collect or store your full payment card information. However, we may receive limited information from those platforms—such as confirmation of your purchase, the type of subscription selected, and associated billing details—to help manage your account and deliver the services you've selected. AEGIS does not control how these third parties collect or use your information. We recommend reviewing the Apple Privacy Policy and the Google Privacy Policy for more information. Stripe’s processing of your payment information is governed by its Privacy Policy. All transactions through Stripe are encrypted and processed through PCI-DSS compliant methods. We use this data solely to provide you with the Services you’ve purchased, manage billing, and detect or prevent fraudulent activity.

- **Your Communications with Us**. We may collect the information you communicate to us, such as through email, contact forms on our website, or our web chat tool. This personal information may include, but is not limited to, your email address, phone number, or mailing address.

- **Interactive Features.** We and others who use our Services may collect personal information that you submit or make available through our interactive features (e.g., commenting functionalities, forums, blogs, and social media pages). Any information you provide using the public sharing features of the Services will be considered "public," unless otherwise required by applicable law, and is not subject to the privacy protections referenced herein.

- **Location Data.** With your permission, AEGIS collects and processes precise and general location data from your mobile device to enable key safety features such as real-time tracking, emergency alerts, and check-ins with selected emergency contacts. We may collect:

  - **Real-time location** while the App is active or running in the background (with your permission)

  - **Location history** stored for up to two (2) days for all members and three (3) days for premium subscribers, to support emergency events and improve response accuracy

  - **Check-in data** including time-stamped locations shared with your designated emergency contacts

  - **General location data** (e.g., city or ZIP code) derived from your IP address, Wi-Fi networks, or Bluetooth signals

  We may also use location analytics provided by your phone's operating system and services to enhance performance, troubleshoot issues, and improve user experience, subject to their respective privacy policies.

- **Device & Usage Information:** When you use our Services, we may automatically collect certain technical data, such as your IP address, device ID, mobile carrier, browser type, operating system, app version, crash logs, and diagnostic data. We may also collect anonymized data about how you use the App—like features accessed, content interactions, pages visited, search activity, session duration—to help us troubleshoot, improve performance, and enhance your user experience. As we expand AEGIS, additional technical and usage metrics may be collected to support new features and services.
- **Account Activity and Interactions:** We may collect certain information related to App usage including but not limited to log files, support inquiries, and emergency event history.

---

2. How We Use Your Data

We use the personal information you provide and the technical information we collect automatically for a range of purposes essential to delivering and improving our Services.

To Provide and Improve the AEGIS Experience

We use your data to deliver core App and Services functionality and ensure a seamless, safe, and responsive experience. This includes:

- Managing your user profile, account settings, and emergency contacts
- Enabling access to key features like SOS alerts, check-In, and saved location services
- Responding to your customer support or technical inquiries
- Transmitting critical personal, location, and medical information to our Emergency Response Partner when you trigger an alert
- Sharing your real-time location, check-in status, and other selected data with your designated emergency contacts to keep them informed and engaged in your safety
- Helping first responders arrive better informed and prepared to assist you
- Monitoring performance and usage to fix bugs, prevent crashes, and improve App stability
- Performing quality assurance and internal analytics to maintain system integrity
- Personalizing your experience based on your preferences and interactions with the App

We process only the minimum necessary information to perform these functions, and always with a focus on protecting your safety and privacy.

Marketing Features and Services

We may use your information to communicate with you about new features, safety enhancements, or special updates to the Services that may improve your experience. This may include:

- Sending occasional emails, in-App messages, or notifications, where permitted by law and with your consent where required
- Informing you of safety resources or feature rollouts that may benefit you
- Sharing relevant offerings from trusted partners if they relate to your safety or emergency preparedness

You can opt out of marketing communications at any time through your App settings or by following the unsubscribe instructions in any message.

We also analyze user engagement data to evaluate the effectiveness of our communication and outreach efforts (e.g., what messages are opened, which features drive interest).

Research and Development

We use de-identified or aggregated data whenever possible to inform how we evolve our Services. This data cannot reasonably identify you. Examples of how your data helps drive innovation include:

- Understanding which features users rely on most
- Identifying trends in App use that help us improve system design and safety workflows
- Developing new Services features and tools based on real-world usage patterns
- Enhancing reliability and responsiveness during emergency events

- Conducting market research to better understand the needs of the communities we serve

Our goal is to continuously improve our Services while minimizing the personal data we retain or analyze.

Administrative and Legal Purposes

We also use personal information to support essential business operations and comply with legal requirements. This includes:

- Detecting and preventing fraud, abuse, and unauthorized access
- Ensuring system and data security
- Verifying your identity and processing user rights requests
- Debugging and fixing technical issues
- Conducting audits, usage analytics, and compliance reviews
- Improving and upgrading our systems and infrastructure
- Supporting research, product development, and internal quality control
- Enforcing our Terms of Use and other legal agreements
- Fulfilling obligations under applicable laws and regulations
- Sharing information with Third-Party Service Providers as needed to deliver our Services safely and reliably

---

Social Media and Third-Party Interactions

If you engage with AEGIS on social media (e.g., following us on Instagram, tagging us in a post, or responding to our updates), we may use publicly available or shared information to:

- Respond to your questions, testimonials, feedback, or comments
- Share content or safety resources you've interacted with
- Enhance how we communicate about AEGIS's mission and features
- Supplement any information you've provided directly to AEGIS (if applicable)

Note that social media platforms are separate from AEGIS and governed by their own privacy policies. We do not control how those platforms collect, use, or share your information.

---

3. Sharing Your Data

We may disclose your information to third parties for a variety of reasons, as outlined below. We limit this sharing to what is necessary to provide our Services, support our operations, protect our users, or comply with the law. We DO NOT sell your personal data to third parties. Further, AEGIS does not use your data for automated profiling or decision-making that could impact your legal rights or access to emergency services.

With Service Providers and Advisors

We may share personal information with Third-Party Service Providers who help us operate AEGIS and deliver our Services. These include providers of hosting, analytics, email communications, emergency response integrations (such as our Emergency Response Partner), marketing support, fraud prevention, and technical infrastructure.

With Emergency Service Providers

If you activate an emergency event within AEGIS, we may share critical data (such as your profile information, location, audio/video submissions, emergency contact info, and/or user-provided medical information) with our Emergency Response Partner and, where applicable, Emergency Service Providers.

AEGIS IS NOT A LICENSED EMERGENCY DISPATCH PROVIDER. WHEN YOU ACTIVATE AN ALERT IN THE AEGIS APP, YOUR DATA IS SECURELY TRANSMITTED TO OUR EMERGENCY RESPONSE PARTNER, WHICH IS RESPONSIBLE FOR COORDINATING WITH EMERGENCY SERVICE PROVIDERS. AS SUCH, AEGIS DOES NOT DIRECTLY DISPATCH EMERGENCY PERSONNEL. WE CANNOT GUARANTEE EMERGENCY RESPONSE TIMES, ACTIONS TAKEN, OR THE EFFECTIVENESS OF THE RESPONDERS AND OTHER EMERGENCY SERVICE PROVIDERS ONCE YOUR DATA IS HANDED OFF. AEGIS DISCLAIMS ANY LIABILITY FOR DELAYS, MISCOMMUNICATIONS, OR ADVERSE OUTCOMES RESULTING FROM EMERGENCY SERVICE PROVIDERS OR ANY THIRD-PARTY RESPONSE.

AEGIS is not a HIPAA-covered entity and does not assume responsibility for the privacy practices of Emergency Service Providers. Any medical or health information shared is done so to facilitate emergency care and is subject to applicable laws and the privacy policies of those entities.

These limitations are further described in our Terms of Use, which govern your use of the Services.

Public Posts

Any content you voluntarily share on our blog, community forums, social media pages (such as comments, reviews, or testimonials) may be publicly accessible. We may also repost or link to such content on our website, App, or third-party sites. We are not responsible for any information you choose to post in public areas. If you would like us to remove content you submitted, please email us.

With Business Partners Offering Integrated Services

If you choose to use certain App features that rely on integrations with third-party partners, we may share relevant data (such as your contact details, device information, or geolocation data) with those partners to provide the requested service.

For Business Transactions

In the event of a merger, acquisition, asset sale, corporate restructuring, bankruptcy, or similar transaction, your personal information may be transferred or disclosed as part of that process. If so, we will take reasonable steps to ensure that your personal data collected through the Services continues to be treated in accordance with this Privacy Policy.

For Business and Research Purposes

We may share information that has been aggregated or de-identified in a way that it can no longer reasonably be linked to any specific individual. This type of data may be shared with trusted partners, researchers, or public safety organizations to support broader safety-related insights and innovation. These uses do not involve the disclosure of any personal or identifiable information.

Compliance and Protection

We may share your information with law enforcement, government agencies, or other parties when we believe it is necessary to:

- Comply with legal obligations or valid legal processes (e.g., subpoena, court order, or government investigation)
- Investigate or prevent fraud, security issues, or other harm
- Enforce our Terms of Use or protect our rights, safety, or property
- Respond to claims or protect the rights of AEGIS users or others

We reserve the right, but do not undertake an obligation, to challenge or notify users of any law enforcement or government request, unless prohibited by law or if doing so would put others at risk.

---

4. Health-Related Information Authorization

By using the Services, you consent to AEGIS and its Third-Party Service Providers collecting, using, retaining, and disclosing any health-related or emergency data you provide (including optional medical history) solely to support emergency assistance. This consent allows us to share information with Emergency Service Providers through our Emergency Response Partner where needed for timely aid. This is not a HIPAA authorization and does not create obligations under HIPAA for AEGIS.

You acknowledge and agree that:

- AEGIS is not a healthcare provider and is not subject to HIPAA.
- Some Emergency Service Providers involved in your emergency event may be subject to HIPAA and will handle your information in accordance with their own privacy obligations.
- Your data is shared solely for the purpose of supporting emergency response and related quality assurance, compliance, or legal obligations.

This consent is required to use the Services, as health-related data is essential for providing effective emergency assistance. You may withdraw this consent at any time by discontinuing use of the Services and deleting your account.

5. Data Retention

AEGIS retains your personal information only for as long as reasonably necessary to fulfill the purposes outlined in this Privacy Policy or as otherwise permitted or required by law. This includes, but is not limited to:

- Delivering and improving our Services
- Supporting emergency response functionality
- Complying with applicable legal, regulatory, and contractual obligations
- Resolving disputes and enforcing our Terms of Use
- Conducting audits, research, or internal business analysis

The duration of data retention may vary depending on the nature of the information, the context in which it was collected, and applicable legal or operational requirements. In all cases, AEGIS exercises discretion in determining appropriate retention periods and reserves the right to retain or delete data at its sole discretion, unless otherwise required by law.

Emergency Data Retention

We retain emergency-related data securely for a limited period to support users who may require documentation for legal, safety, or evidentiary purposes—such as filing police reports, pursuing claims, or verifying the occurrence of an incident. However, AEGIS makes no representation or guarantee regarding the availability or completeness of such records, and users are advised to preserve any critical evidence on their own systems or through official channels whenever possible.

6. Data Security

At AEGIS, we are committed to protecting your personal information through a combination of administrative, technical, and physical safeguards designed to meet industry standards. These include end-to-end AES 256-bit encryption for sensitive data, continuous 24/7 system monitoring, and role-based access controls. We also implement device, network, and server security measures to help prevent unauthorized access.

We are actively working to roll out two-factor authentication (2FA) for administrative accounts to further strengthen access controls. Once live, 2FA will add an additional layer of protection to sensitive systems and user data.

While we take commercially reasonable steps to safeguard your information, no method of transmission over the internet or method of electronic storage is completely secure. As such, we cannot guarantee absolute security, and you use the Services at your own risk. We encourage all users to take appropriate measures to protect their accounts and devices, including using strong passwords and maintaining up-to-date security software.

7. Your Privacy Rights

Your privacy rights may vary depending on your location and applicable law. Below are your rights and options for managing how we collect, use, and communicate with you:

Communications Preferences

- **Email:** To stop receiving promotional emails, use the "unsubscribe" link found at the bottom of our emails. Note that you will still receive service-related communications (e.g., transaction confirmations, legal notices).
- **Text Messages:** To opt out of SMS/text messages, follow the opt-out instructions included in each message.
- **Push Notifications & Location:** You may disable push notifications and/or location tracking at any time via your mobile device settings.

Device Permissions

Location Access: You can manage the App's access to location and other permissions through your mobile device settings.

Account Deletion

You may delete your AEGIS account in one of the following ways:

- **In-App Deletion**:
  Navigate to your profile by tapping the icon in the top-right corner of the App. Select **"Delete Account"**, then confirm your choice by tapping **"I'm Sure"** after the 5-second delay. This helps prevent accidental deletions.

- **Request via Support**:
  You may also request account deletion by contacting us directly at the email found below. For security purposes, we may require identity verification before processing your request.

Please note: Deleting your account will permanently remove your profile and stored data, except where retention is required by law or for legitimate business purposes.

Do Not Track

We do not respond to "Do Not Track" signals from browsers.

Cookies & Advertising

You may configure your browser settings to manage or disable cookies. Note that disabling cookies may impact the functionality of our Services.

Children's Policy

AEGIS is not intended for children under the age of 13, and we do not knowingly collect personal information from anyone under 13. If we learn that we have inadvertently collected personal data from a child under 13, we will take steps to delete such information promptly. If you are a parent or guardian and believe your child has provided us with personal information, please contact us.

California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA):

- The right to know what personal information we collect and how we use it;
- The right to request access to the personal information we collect;
- The right to request deletion of your personal information;
- The right to correct inaccurate personal information;
- The right to opt out of the “sale” or “sharing” of personal information;
  The right to limit the use of sensitive personal information (if applicable).

Although we do not sell your personal information, California residents may still submit such a request by contacting us.

Nevada Privacy Rights

Nevada residents have the right to request that we do not sell certain personal information to third parties. Although we do not sell your personal information, Nevada residents may still submit such a request by contacting us.

International Users

AEGIS is intended for use only within the United States. If you are located outside of the U.S., please do not use the Services. We do not knowingly process personal data of individuals in the European Union or other jurisdictions subject to the General Data Protection Regulation (GDPR).

Exercising Your Rights

To exercise any of these rights, please contact us at legal@aegisapp.io We will respond in accordance with applicable laws and timeframes.

---

8. Changes to This Privacy Policy

We may update this Privacy Policy periodically. We will notify you of any material changes through the App, by email or other means. Please review it regularly to stay informed.

If you object to any of the changes to this Privacy Policy, you must cease using our Services, and may request us to erase your personal information. Any information that is collected through your use of our Services is covered by the Privacy Policy in effect at the time such information is collected.

---

9. Contact Us

If you have any questions about our privacy practices, this Privacy Policy or our Services, please contact us via email at legal@aegisapp.io

Version: 2025-06-24