PRIVACY NOTICE

At goHappy Labs, LLC (“Company”, "we," "our," or "us"), we are committed to maintaining the privacy and security of the personal information of our customers, partners, and users. This Privacy Policy outlines how we collect, use, disclose, and safeguard your information when you use our software-as-a-service platform and related services (collectively referred to as the "Services"). By accessing or using our Services, you agree to the terms of this Privacy Policy.

1. Information We Collect

We may collect various types of information, including but not limited to:

- Contact Information: Names, email addresses, phone numbers, and other contact details.
- Company Information: Company names, industry, and other business-related details.
- User Data: Usernames, passwords, and other authentication credentials.
- Usage Data: Information about how you use our Services, including log data, feature usage, and interactions with the platform.
- Communication Data: Correspondence, feedback, and inquiries you send to us.
- Billing Information: Payment information and billing details.

2. How We Use Your Information

We use your information for the following purposes:

- Providing and Improving Services: To operate, maintain, and enhance our Services.
- Communication: To respond to your inquiries, send important updates, and provide customer support.
- Personalization: To customize your experience and provide tailored content.
- Analytics: To analyze usage patterns and improve our Services.
- Legal Compliance: To comply with applicable laws, regulations, or legal processes.

3. How We Share Your Information

We may share your information with third parties under the following circumstances:

- Service Providers: We may engage third-party service providers to assist us in delivering our Services.
- Business Partners: In cases where you have integrated our Services with third-party platforms.
- Legal Compliance: If required by law or in response to valid legal requests.
- Merger or Acquisition: In the event of a merger, acquisition, or sale of all or a portion of our assets.
- Consent: With your consent or at your direction.

4. Data Security

We implement industry-standard security measures to protect your information from unauthorized access, disclosure, alteration, or destruction. However, no method of transmission over the internet or electronic storage is entirely secure.

5. Your Choices

You have the right to:

- Access and Correct Your Information: You can access and update your personal information through your account settings.
- Opt-Out: You can opt-out of promotional communications.
- Data Portability: You can request a copy of your data in a structured format.

6. Data Anonymization and Benchmarking

We may use certain data that you provide for benchmarking purposes. In cases where we use certain data you provide for benchmarking purposes, we will use reasonable efforts to anonymize the data before using it for benchmarking purposes and we will anonymize any such data to protect the confidentiality and privacy of any individuals included in the data. Our benchmarking of data may include comparing the anonymized data with similar data from other sources to assess industry trends, best practices, and performance metrics. We will use Confidential Information only as necessary to perform our obligations under this Agreement, and shall hold Confidential Information with the same level of care that we hold our own Confidential Information (but in any event with no less than a reasonable level of care). We will disclose Confidential Information to only those third parties who provide services for the purpose of delivering the Services and have previously agreed in writing to protect third party Confidential Information to the same extent as required in this Agreement Data provided by you for benchmarking purposes shall remain your sole property, and we will assert no rights or interest in the data, except as required for benchmarking purposes. We will retain the data only for as long as necessary to fulfill the benchmarking purposes. We will comply with all applicable privacy laws regarding the data, and we will also ensure that our employees and subcontractors who have access to the data are bound by appropriate confidentiality obligations.

7. Data Sub-Processor Disclosure

In accordance with our Privacy Policy and commitment to user data privacy, we disclose that we engage the following third-party entities to provide certain services on our behalf. These sub-processors may process certain personal data in the course of providing these services.

- Auth0: Auth0 is a flexible, drop-in solution to add authentication and authorization services to your applications. Your personal data may be transferred to Auth0 and processed for the purpose of providing secure authentication and user management services.
- AWS: Amazon Web Services (“AWS”) is a hosting platform that we use for our application deployment. Your personal data may be processed and stored on

servers managed by AWS, which are located globally, for the purpose of running our services and ensuring their availability to you.

- Telnyx: Telnyx is a communication software that we utilize for telecommunication services, such as voice, messaging, and 911 connectivity. When using these services, your personal data may be processed and transferred to Telnyx.
- Cloudflare: We use Cloudflare for content delivery network (CDN) services, DDoS protection, and internet security services. Your data, including personal data, may be transferred to Cloudflare and processed for the purpose of securing our services and improving their performance.

Please note that we enter into General Data Protection Regulation (GDPR) compliant data processing agreements with all our sub-processors, ensuring that they meet high standards for data privacy and security. They are not authorized to use your personal data for their own purposes and are obligated to implement appropriate technical and organizational measures to protect your data.

We will endeavor to update this list as our service providers change, and we encourage you to periodically review this list for any changes. If you have any questions or concerns about our use of these sub-processors, please contact us as described in our Privacy Policy.

8. Shared Security Responsibility Model (SSRM)

Customers

- User Access Management: Customers are responsible for managing and securing user access to the Services. This includes establishing strong access controls, managing user roles, and implementing two-factor authentication or other strong authentication methods.
- Data Security: Customers have a responsibility for the security of the data they input into the SaaS application. This includes ensuring data is entered and stored securely, and that only the proper information is inputted into the application.
- Compliance: Customers may have certain responsibilities related to compliance with various regulations, depending on the industry and region. This could include GDPR for customer data.

goHappy

- Application Security: As the provider of the software application, we are responsible for using commercially reasonable efforts to ensure the application is secure. This includes conducting regular security testing, patching vulnerabilities, and implementing secure coding practices.
- Data Security: While customers have responsibilities for the data they input, we also have responsibilities for the security of that data while it's stored in our systems. This includes implementing data encryption, managing data access, and ensuring data is backed up and can be restored if necessary.
- User Access Management: We are responsible for providing features that allow Customers to secure their user access, such as two-factor authentication, password strength requirements, and account lockout policies.

3rd Party Service Providers

- Physical Security: Cloud service providers are responsible for the physical security of their data centers. This includes controls like security guards, CCTV cameras, and access restrictions.
- Infrastructure Security: The cloud provider is also responsible for the security of the cloud infrastructure. This includes securing the underlying hardware, the network, and the server environment.
- Platform Security: Depending on the specific services offered, the cloud provider may also have responsibilities for the security of the platform on which the goHappy application runs. This could include things like operating system security, firewall configuration, and network segmentation.

9. California Consumer Privacy Act ("CCPA")

As a California resident, you have the right to:

- Request access to your personal information.
- Request deletion of your personal information.
- Opt-out of the sale of your personal information.
- Non-discrimination in terms of service or pricing if you exercise your privacy rights.

How to Exercise Your Rights:

- You can exercise your rights under CCPA by submitting your requests to ccpa@gohappyhub.com. We will verify your request in accordance with CCPA requirements.

10. Children's Privacy

Our Services are not intended for individuals under the age of 18. We do not knowingly collect or store information from children.

11. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. Any updates will be posted on our website, and the "Effective Date" at the top will indicate when the changes take effect.

12. Contact Us

If you have any questions, concerns, or requests related to this Privacy Policy, please contact us at privacy@gohappyhub.com or 833-464-2779.

goHappy Labs, LLC
4820 Lake Brook Drive
Suite 140
Glen Allen, VA 23060

By using our Services, you agree to the terms of this Privacy Policy.