ReachU LLC

Privacy Notice

(Effective: August 7, 2024**)**

Thank you for choosing to be a part of our community at ReachU LLC ("the Company," "we," "us," or "our"). We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about this Privacy Notice ("Notice") or our practices with regard to your personal information, please contact us at info@reachuapp.com.

When you use our mobile application ("App"), website at ReachU.com ("Site"), or other of our services ("Services"), you trust us with your personal information. We take your privacy very seriously. In this Notice, we seek to explain to you in the clearest way possible what information we collect, ways we collect your personal data, how we use it, ways we share your personal data, ways we retain and safeguard your personal data, and what rights you have in relation to it. We hope you take the time to read it carefully, as it is essential.

This Notice applies to all information collected through our App, Site, and/or any related services, sales, marketing, or events ("Services"). BY USING OUR APP, SITE, or other SERVICES, YOU CONSENT TO THE TERMS OF THIS PRIVACY NOTICE. IF THERE ARE ANY TERMS IN THIS NOTICE THAT YOU DISAGREE WITH, PLEASE DISCONTINUE THE USE OF OUR APP, SITE OR OTHER SERVICES.

Please read this Notice carefully, as it will help you make informed decisions about sharing your personal information with us. In addition to reviewing this Notice, please also review our Terms & Conditions ("Terms") and any other terms and conditions that may be posted elsewhere in the App, Site, or otherwise communicated to our users, because the Terms and all such terms and conditions are also part of the agreement between you and us.

Our App is designed to work with third-party support programs ("Third-Party Programs"). Those Third-Party Programs have their own terms and conditions and privacy conditions. We do not manage or control those terms and privacy conditions. You should know such terms and privacy conditions before using our App. Compliance with those terms and privacy conditions is a requirement of the use of our App.

What information do we collect?

"Personally Identifiable Information" alone or in combination with other information or in certain contexts can be used to identify, distinguish, or trace you or the device(s) (collectively, "Device") used to access the Site is referred to in this document as "PII." PII, together with all other information about you and/or your Device(s) that we acquire is referred to collectively as your "personal data." "Content" as used herein refers generally to any type of information, including text, images, video, whether sourced from you, us or third parties.

We acquire PII that may include, in certain contexts, but is not limited to, your name, postal address, zip code, email address, telephone number, ethnicity, grade classification, school, college and major, *as well as information you generate like content engagement, event attendance, or personal usage metrics*. We also acquire your IP address, User ID, and/or Device ID, which certain jurisdictions consider to be PII because it could be used to identify an individual or Device if it were combined with other identifying information.

We collect personal information that you voluntarily provide to us when registering to the App, contacting us, or when you generate data by using the App and its features.

The information that you generate while using the App includes browsing history within the app,

event attendance through check-in features, content engagement metrics or wellness scores. All information generated in the App is protected by Amazon Web Services as well as internal safeguards, including:

- Employee Training on Data Privacy
- Periodic Security Risk Assessments
- Access Logging for Sensitive Information

We collect information regarding your mobile device and push notifications when you use our App or Site. We may request access or permission to certain features from your mobile device, like your camera. You may change this access through your device settings.

Sensitive PII

In certain circumstances, such as purchasing a product through our App, Site, or other Services, you may provide a credit, debit, or payment account number, or other payment information that we recognize as more sensitive than other PII. We generally do not request on or through the Site other data that is often considered "highly sensitive," such as other financial account information (e.g., credit report information, bank account numbers), personal health information, or government-issued identification numbers (e.g., social security number, drivers' license number, or passport number). However, we will collect such Sensitive PII when necessary to offer you certain Services.

Anonymous Data

Some of the personal data that we acquire cannot identify, distinguish, or trace you or your Device, even if combined with other identifying information, and some Personal Data that could be considered PII when combined with other identifying information is not used in a way that identifies, distinguishes or traces you or your Device but is instead used in an anonymous way, often aggregated with other anonymous Personal Data about other users.

Medical Disclaimer & Data

The information contained in our App, including but not limited to, content, graphics, images and any other materials, is for informational purposes only. It is not intended to be a substitute for professional medical advice, diagnosis, or treatment. Our App and Site do not knowingly store, house or maintain your medical or other healthcare information. Always seek the advice of your doctor or other qualified healthcare provider with any questions you may have regarding a medical condition or treatment and never disregard professional medical advice or delay in seeking it because of something you have read on our App or Site or through the use of our Services.

WAYS WE COLLECT YOUR PERSONAL DATA

In General

We collect only personal data that you provide to us voluntarily, and where applicable, with your consent. We take measures to ensure that we collect personal data for specified, explicit and legitimate reasons only — namely, to provide products and Services to you and meet our legal obligations. We also take steps to limit the personal data we collect to only the minimum necessary to carry out our business objectives.

We may collect your personal data when you:

- *Contact us by phone or online;*
- *Create a user account;*
- *Interact with our social media pages (such as Instagram, Facebook, Twitter or LinkedIn);*

- *Sign up for our newsletters or alerts;*
- *View our content or products;*
- *Purchase a product or Services;*
- *Attend an event that we may host;*
- *When you apply for a job with us; and/or*
- *Communicate with us via email or other channels, such as our Contact Us form.*

In these instances, we may collect personal data such as your name, email address, postal address (or other geolocation information), phone number, demographic information, and usage data. If you purchase any Services from us as applicable, we will collect the information necessary to complete that transaction, such as your name, email address, residential address, and payment information.

Log Files

We may use log files to record data about your visit to our Site. When you use our Site, we may collect the IP (Internet Protocol) address connected to your computer (or the proxy server you use to access the World Wide Web), your computer operating system, the type of browser you are using, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics, mobile device operating system (if you are accessing the Site using a mobile device), as well as the name of your ISP (Internet Service Provider) or your mobile carrier. We may use this information to analyze overall trends to help improve the Site. We do not share log data with third parties unless required by law to do so.

Telephone Consumer Protection Act

If you share your telephone number with us through any of our Services, you expressly agree to receive communications from us, our agents, representatives, affiliates, or business partners, via e-mail, SMS or text messages, phone calls, video calls, and push notifications. You further expressly agree that these communications may be generated using automated technology, such as an automatic telephone dialing system, or artificial or prerecorded voice, even if your telephone number(s) is/are listed on any corporate, state, or federal Do-Not-Call lists.

You represent that for the telephone number(s) that you provide to us, you are the current subscriber or customary user and that you have the authority to provide the consent described above to be contacted at such number(s). You agree to promptly alert us whenever you stop using a particular telephone number. Standard charges may apply to the receipt of these calls or text messages.

Data Acquired Elsewhere

We may also acquire your personal data offline or otherwise outside of our App or Services. For example, we may purchase or otherwise acquire such personal data from third-party data suppliers. We reserve the right to merge or commingle this other personal data with your personal data collected on or through the Site.

Social Network Integration

If you choose to access, visit, and/or use any third-party social networking service(s) that may be integrated with the Services, we may receive your personal data that has been made available to those services, including information about your contacts on those services. For example, some social networking services allow you to push Content from our Services to your contacts or to pull information about your contacts so you can connect with them on or through our Services. Some social networking services will also facilitate your registration for our Services or enhance or personalize your experience on our Site. Your decision to use a social networking service in connection with our Services is voluntary. However, you should make sure you are comfortable with your personal data that the third-party social networking services may make available to us by

visiting those services' privacy notices and/or modifying your privacy settings directly with those services. We reserve the right to use, transfer, assign, sell, share, and provide access to all of your personal data that we receive through third-party social networking services in the same ways as all of your personal data we receive through our Site (as described below).

Cookies and Similar Tracking Technologies Use of Cookies on the Site

When you use and access the Site, we may place a number of cookie files in your web browser. We use cookies for the following purposes:

- To enable certain functions of the Services;
- To provide analytics;
- To store your preferences;
- To enable advertisement delivery, including behavioral advertising

We use both persistent and session cookies on the Services and we may use different types of cookies to run the Services. The other types of cookies include:

Essential cookies. We may use essential cookies to authenticate users and prevent fraudulent use of user accounts.

Necessary cookies. We may use necessary cookies to enable core functionality such as security, network management, and accessibility.

Preference cookies. We may use preference cookies to remember information that changes the way the Services behaves or looks, such as the "remember me" functionality of a registered user or a user's language preference.

Analytics cookies. We may use analytics cookies to track information on how the Services are used so that we can make improvements. We may also use analytics cookies to test new advertisements, pages, features or new functionality of the Application or Services to see how our users react to them.

Advertising cookies. These types of cookies are used to deliver advertisements on and through the Services and track the performance of these advertisements. These cookies may also be used to enable third-party advertising networks to deliver ads that may be relevant to you based on your activities or interests.

Notice and Consent for Use of Cookies

In accordance with the EU General Data Protection Regulation (see below), we may provide you with a clear and conspicuous notice that summarizes our use of cookies, seeks your consent for the use of such cookies, and outlines the ways you can control such cookies when visiting the Site. If no such notice presents itself to users who visit our Site, this means that we do not implement cookies.

What Are Your Choices regarding Cookies

If you want to delete, limit or refuse cookies, please visit the cookies preference page or the help page of your web browser. Note that if you delete, limit or refuse to accept cookies, you may not be able to use all of the offered features or store your preferences. Further, some of our pages may not display properly.

Use of Third-Party Cookies and Other Tracking Technologies on the Site

In addition to our own cookies, we may also use various third-party cookies to report usage statistics of the App or Services and deliver advertisements on and through the App or Services.

ANALYTICS AND BEHAVIORAL REMARKETING

We may use third-party service providers to monitor and analyze the use of our Site, as well as use remarketing services to advertise on third-party websites to you after you visit our Site. We and our third-party service providers use cookies to inform, optimize and serve ads based on your past visits to our Services.

Google Analytics and Google AdWords

We may use Google Maps™ mapping service, Google Analytics, or any other analytics service provider to optimize our Services and overall experience, and Google AdWords, Google Maps, Google Analytics, or any other analytics service provider may use cookies, tags, or other technologies to collect data about a user's behavior and their mobile devices. We do not use Google Maps mapping service to collect or process data that uniquely identifies an individual except as needed to offer products and services to you, including the hosting of your content. Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our service and may use the collected data to personalize and contextualize the ads of its own advertising network. This data is shared with other Google services. Google AdWords is a remarketing service provided by Google Inc.

You can opt out of having your activity while using our Services made available to Google Analytics by installing the Google Analytics opt-out browser add-on. The add-on prevents the Google Analytics JavaScript from sharing information with Google Analytics about visit activities. You can opt out of Google Analytics for Display Advertising and customize the Google Display Network ads by visiting the Google Ads Settings page: http://www.google.com/settings/ads. Please see the Google Privacy Policy for more information on Google Maps and Google Analytics services. Also reference the terms and conditions and privacy policy of any other analytics service provider for more information.

Facebook

Facebook remarketing service is provided by Facebook Inc.

You can learn more about interest-based advertising from Facebook by visiting this page: https://www.facebook.com/help/164968693837950

To opt-out of Facebook's interest-based ads follow these instructions from Facebook: https://www.facebook.com/help/568137493302217

Facebook adheres to the Self-Regulatory Principles for Online Behavioral Advertising established by the Digital Advertising Alliance. You can also opt-out from Facebook and other participating companies through the Digital Advertising Alliance in the USA http://www.aboutads.info/choices/, the Digital Advertising Alliance of Canada in Canada http://youradchoices.ca/ or the European Interactive Digital Advertising Alliance in Europe http://www.youronlinechoices.eu/, or opt-out using your mobile device settings.

For more information on the privacy practices of Facebook, please visit Facebook's Data Policy: https://www.facebook.com/privacy/explanation

Use of Pixel Tags, Clear GIFs, Beacons and/or Other Similar Technologies for Email Marketing

We may use beacons (which are like cookies), pixel tags, clear GIFs and other similar technologies in email marketing communications with our clients and other stakeholders to collect data about recipients' actions (e.g., the number of recipients who open the message or click on a link in the message) such as email marketing communications, measure the success of our marketing

campaigns and compile results about the usage of our App and/or Services.

We may request to send you push notifications regarding your account or the mobile application. If you wish to opt-out from receiving these types of communications, you may turn them off in your device's settings.

How do we use your information?

We process your information for purposes based on legitimate business interests, the fulfillment of our contract with you or our business partners, compliance with our legal obligations, and/or your consent.

We use personal information collected via the App for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interests, in order to enter into or perform a contract with you or our business partners, with your consent, and/or for compliance with our legal obligations. We indicate the specific processing grounds we rely on next to each purpose listed below.

We use the information we collect or receive:

- **To facilitate account creation and logon process.** The information you volunteer during the signup process is used for communication purposes and to have demographic representation of our users.
- **Request Feedback.** We may use your information to request feedback and to contact you about your use of our App.
- **To enforce our terms, conditions, and policies for Business Purposes, Legal Reasons, and Contractual.**
- **To respond to legal requests and prevent harm.** If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond.
- **To manage user accounts.** We may use your information to manage our account, keeping it in working order, and answer any questions you submit to us.
- **To deliver services to the users.** We may use your information to provide you with the requested service.
- **For other business purposes.** We may use your information for other business purposes, such as data analysis, identifying usage trends, determining the effectiveness of our features, to evaluating and improving our App and your experience, and sending you updates.
- If you apply for a job or contractor position with us, we may also use your personal data to process your application, conduct background screening, or check references. Once hired, we may use your personal data to facilitate payment (and benefits, as applicable).

Will your information be shared with anyone?

We only share information with your consent, to comply with laws, to provide you with services, to protect your rights, or to fulfill business obligations.

We may process or share data based on the following legal basis:

- **Consent:** We may process your data if you have given us specific consent to use your personal information for a specific purpose.
- **Legitimate Interests:** We may process your data when it is reasonably necessary to achieve our legitimate business interests, including but not limited to, marketing research, user authentication, software support, user relationship management, and social media channels.
- **Performance of a Contract:** Where we have entered into a contract with you, we may process your personal information to fulfill the terms of our contract.
- **Legal Obligations:** We may disclose your information where we are legally required to do so

to comply with applicable law, government requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).

- **Vital Interests:** We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

More specifically, we may need to process your data or share your personal information in the following situations:

- **Vendors, Consultants and Other Third-Party Service Providers.** We may share your data with third-party vendors, service providers, contractors, or agents who perform services for us or on our behalf and require access to such information to do that work. Examples include payment processing, data analysis, email delivery, hosting services or customer service. Unless described in this Notice, we do not share, sell, rent or trade any of your information with third parties for their promotional purposes.
- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this Privacy Notice. Affiliates include our parent company, subsidiaries, joint venture partners or other companies that we control or that are under common control with us. This also includes the university that has subscribed to our app.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services, or promotions. This will include businesses or other partners providing Third-Party Programs. Our App is typically used to provide access to or management of Third-Party Programs of which Users are members or clients.

Other Sharing Circumstances

We may also share your personal data in other circumstances, such as the following:

- *As required by law, or in response to a subpoena or other government information request*
- *If we believe that the disclosure is in the interest of your security or our security (including exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction)*
- *If another company acquires or merges with us*
- *If we go out of business, enter bankruptcy, or experience some other change of control.*

How long do we keep your information?

We keep your information for as long as necessary to fulfill the purposes outlined in this Notice unless otherwise required by law.

We will only keep your personal information for as long as it is necessary for the purposes set out in this Notice unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this Notice will require us to keep your personal information past the termination of the user's account. When we have no ongoing legitimate business need to process your personal information, we will further anonymize it; if that is not possible, we will store your personal information and isolate it from further processing until deletion is possible.

How do we keep your information safe?

We aim to protect your personal information through organizational and technical security measures.

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. Our service provider has completed numerous security evaluation processes. However, please also remember that we cannot guarantee that the internet itself is 100% secure. Although we do our best to protect your personal information, transmission of personal information to and from our App is at your own risk. You should only access the services within a secure environment.

We employ several organizational security measures including regular security risk assessments, access logging for sensitive information, and termination policies for employees who misappropriate your data.

What are your privacy rights?

You may review, change, or terminate your account at any time.

When you delete your account, we delete all your personal information and any/all information that you have generated while using the App. You may also request a log of the information you have generated or request to amend your information.

Account Information

If you would like to review or change the information in your account or terminate your account, you can contact us at info@reachuapp.com

Upon your request to terminate your account, we will deactivate your account and all associated information from our active databases. However, some information may be retained in our files to troubleshoot problems, assist with any investigations, enforce our Terms of Use and/or comply with legal requirements.

Opt-Out of Email Marketing.

You can unsubscribe from our marketing email list at any time by contacting us using the details provided below. You will then be removed from the marketing email list – however, we will still send you service-related emails that are necessary for the administration and use of your account. To opt out, you may access your account settings and update your preferences or contact us using the contact information provided. You can also set these preferences when you register for your account.

Virtual Meetings

Please note that the App may facilitate meetings through virtual web calling for user convenience. Any interactions, discussions, or engagements conducted during virtual meetings are voluntary and not required, governed, or guaranteed by the Company. The Company disclaims any liability arising from or related to interactions that occur during virtual meetings facilitated by the App.

Controls for Do-Not-Track Features

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track (DNT) feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will

inform you about that practice in a revised version of this Notice.

USERS OUTSIDE THE UNITED STATES

Your Privacy Rights Under GDPR

If you are in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, you have certain data privacy rights, as defined by the General Data Protection Regulation (GDPR). We further provide additional information for individuals from the European Union, the UK, and Switzerland, as defined by the EU-US Data Privacy Framework. We describe all of these rights in our *Supplemental Privacy Notice for Individuals in the European Union, UK, and Switzerland*.

Your Privacy Rights Under California, Colorado, Connecticut, Utah, or Virginia Laws

If you are a resident of California, Colorado, Connecticut, Utah, or Virginia, you have certain data privacy rights. We describe these rights in our *Supplemental Privacy Notice for Residents of California, Colorado, Connecticut, Utah, and Virginia*. On July 1, 2024, the Florida Digital Bill of Rights law (FDBR/SB 262), the Oregon Consumer Privacy Act (SB619), and the Texas Data Privacy & Security Act (TDPSA/HB 4), and on October 1, 2024, Montana's Consumer Data Privacy Act (SB 384) will take effect. These laws shall be incorporated into this Supplemental Privacy Notice on their respective effective dates.

Your Privacy Rights Under the Australia Privacy Act

If you are a citizen of Australia, you have certain data privacy rights, as defined by the Australia Privacy Act. We describe these rights in our *Supplemental Privacy Notice for Citizens of Australia*.

Your Privacy Rights Under Brazil's Data Protection Law

If you are a citizen of Brazil, you have certain data privacy rights, as defined by the Brazil Data Protection Law. We describe these rights in our Supplemental Privacy Notice for Citizens of Brazil.

Your Privacy Rights Under Other Regulated Countries or Jurisdictions

If you are a citizen or resident of regulated countries or jurisdictions not specifically mentioned in this Privacy Notice, you may have certain data privacy rights as defined by the laws and regulations of such regulated countries or jurisdictions. We commit to honor the privacy rights of individuals from such regulated countries or jurisdictions. If you have a question about these rights, please use the information in the *How to Contact Us* section below.

DATA TRANSFERS

Data Transfers from the EU/EEA to the US or Elsewhere

If you are in the European Union/European Economic Area (EU/EEA), please be aware that we operate in the United States (US). As such, we may transfer your personal data from the EU/EEA to the US to provide you with products and Services or otherwise communicate with you. We take measures to adequately safeguard your personal data when transferred to the United States or elsewhere and aim to comply with applicable data privacy laws and regulations.

When we transfer personal data from the EU/EEA to countries or international organizations based outside the EU/EEA, the transfer takes place on the basis of legally permitted grounds, such as with your informed consent prior to the transfer, or via standard contractual clauses (i.e., pre-defined data protection clauses added to contracts) with those clients for whom we transfer such personal data.

Data Transfers from Australia to the US or Elsewhere

If you are a citizen of Australia, please be aware that we operate in the United States. As such, we may transfer your personal data from Australia to the US to provide you with products and Services, or otherwise communicate with you. We take measures to adequately safeguard your personal data when transferred from Australia to the US or elsewhere.

Data Transfers from China to the US or Elsewhere

If you are in China, please be aware that we operate in the United States. The Personal Information Protection Law (PIPL) is an extra-territorial law applicable to entities doing business both within and outside of China that process personal information on natural persons within the territory of China. PIPL requires a lawful basis for the data processing and specific, informed consent. We are aware that China does not distinguish between based on an individual's permanent place of residence or citizenship.

Please be informed that we may transfer your personal data from China to the US for the purposes of: (a) providing products or services to individuals in China; (b) assessing or analyzing the behavior of individuals in China; or (c) for other purposes to be specified.

Data Transfers from Other Regulated Countries or Jurisdictions to the US or Elsewhere

If you are a citizen of a country or jurisdiction not specifically mentioned in this Privacy Notice, please be aware that we operate in the United States. As such, we may either transfer your personal data from your home country or jurisdiction to the US or other countries to provide you with products and Services or otherwise communicate with you. We take measures to adequately safeguard your personal data when transferred from a country or jurisdiction not specifically mentioned in this Privacy Notice to the US or elsewhere. Your usage of our Services, along with your submission of your information, is considered consent and represents your agreement to that transfer.

DATA SECURITY

We constantly strive to align our data security practices with industry-accepted standards for securely handling, transmitting, and storing personal data. To prevent unauthorized access, maintain data accuracy, and the correct use of information, we implement administrative, physical, and technical measures to safeguard and secure the information we collect on the App. We utilize industry-accepted encryption technologies and strengths to reduce the risk of others viewing information passing between you and our App.

Since the Internet is not a completely secure environment, we cannot ensure or warrant the security of any information you transmit to us. We offer no guarantees that information cannot or will not be accessed, disclosed, altered, or destroyed by a breach of any of our administrative, physical, or technical measures.

MALWARE/SPYWARE/VIRUSES

We don't knowingly use or permit the use of malware, spyware, viruses, and/or other similar types of software.

NOTIFICATION IN EVENT OF DATA BREACH

International, federal, and state laws and regulations may require us to notify our clients and/or individual victims in the event of a breach of personal data. In such an unfortunate event, we will promptly notify our clients and/or data breach victims in accordance with notification procedures defined in our internal policies and as required by applicable law.

LINKS

The App or Site may contain links to and from other third-party sites not operated by us. Please be aware that we are not responsible for the privacy practices of these third-party sites. We encourage you to be aware when you leave our App or Site and to read the privacy notices of each third-party website that collects your personal data.

UPDATES TO NOTICE

We may update this Notice from time to time. The updated version will be indicated by an updated "Revised" date, and the updated version will be effective as soon as it is accessible. If we make material changes to this Privacy Notice, we may notify you by email or a notice within the App. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

CONTACT US

If you have questions or comments about this Privacy Notice, you may contact our Data Protection Team by email at info@reachuapp.com.

This document was last updated on August 9, 2024.