

Privacy Policy

In order to use the Services, we will ask you to enter certain information about you, such as your name, your age, occupation, learning goals, etc. We will also automatically collect information from your device, such as language settings, IP address, time zone, device type and model, device settings, operating system, Internet service provider, mobile carrier, hardware ID, and other unique identifiers (such as IDFA and AAID). We need this data to provide our Services, analyze how our users interact with our Services, and serve ads.

For improving the service and serving ads, we use third-party solutions. As a result, we may process data using solutions developed by **Apple, Google, Clarity, Sentry, Namecheap, Facebook, AppsFlyer, Firebase, Amplitude, Tableau, Facebook, CookieYes, Solidgate, PayPal, Customer.io, Zendesk, Shake**. Therefore, some of the data is stored and processed on servers operated by such third parties. This enables us to: (1) analyze different interactions (how often users make purchases, what is the average time spent by users on the Website and App); (2) serve and measure ads (and are able to show them only to a particular group of users, for example, to users that have already visited the Website). Consequently, we, in particular, better understand which of our features and content you see the most value and are able to focus on them to enhance your experience and increase the quality of our Services.

Please read our Privacy Policy below to know more about what we do with data (Section 2), what data privacy rights are available to you (Section 5), who will be the data controller (Section 16), and how to influence personalized advertising (Subsection 2.8). If any questions remain unanswered, please contact us at support@powero.app.

Unless otherwise defined herein, all capitalized terms used in this Privacy Policy share the definitions provided in the Terms and Conditions of Use.

General Terms

This Privacy Policy explains what personal data is collected when you access and use our website www.powero.app (the “**Website**”), Powero mobile app (the “**App**”) and related services, including all information, text, graphics, software, and our emails (the “**Content**”) and how such personal data will be processed. The Website, Powero mobile app, the Content, and our services are collectively called the “**Services**”.

BY USING THE SERVICES, YOU PROMISE US THAT (I) YOU HAVE READ, UNDERSTAND AND AGREE TO THIS PRIVACY POLICY, AND (II) YOU ARE OVER 16 YEARS OF AGE (OR HAVE HAD YOUR PARENT OR GUARDIAN READ AND AGREE TO THIS PRIVACY POLICY FOR YOU). If you do not agree or are unable to make this promise, you must not use the Services. In such a case, you must (a) cancel any active Subscriptions or trials; (b) delete the App from your device or leave the Website and not access or use it; and (c) contact us and request deletion of your data.

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“**EEA**” includes all current member states of the European Union and the European Free Trade Association. For the purpose of this Policy, EEA shall include the United Kingdom of Great Britain and Northern Ireland.

“**Process**”, in respect of personal data, includes collecting, storing, using, and disclosing to others.

1. Personal Data Controller

Pikelo Limited, a company registered and acting under the laws of the Republic of Cyprus with registration, having its registered address at 21 Panteli Katelari Street, Libra House, 6th Floor, 1097 Nicosia, Cyprus, will be the controller of your personal data.

2. Categories of Personal Data We Collect

We collect data you voluntarily provide (for example, when you enter your name and email). We also collect data automatically (for example, your IP address and activity logs) and use third-party service providers to facilitate this collection.

2.1. Data you provide

You provide us with information about yourself when you contact us regarding the use of the Services, or when you register for and/or use the Services. This includes your name and your contact details, including your email address.

2.2. Data provided by third parties

When you log in with **Google**, we receive personal data from your Google account. This includes your email, name, profile image, and Google ID. You can revoke access provided to us on the [Apps Permissions](#) page. To know more about how Google processes your data, visit its [Privacy Policy](#).

When you use Sign In with **Apple** to register an account in the Services, we get personal data from your Apple ID account. This data may include, in particular, your name and verified email address. You may choose to share your real email address or an anonymous one that uses the private email relay service. Apple will show you its detailed privacy information on the Sign In with Apple screen. Apple lets you revoke access provided to the App in your Apple ID settings by following the [next steps](#). Find more about Sign In with Apple [here](#).

2.3. Data we collect automatically

a. [Data about how you found us](#)

We collect data about your referring app or URL (i.e., the app or website where you were when you tapped or clicked our ad).

b. [Device and Location data](#)

We collect data from your device. Examples of such data include: language settings, IP address, time zone, type and model of a device, device settings, operating system, Internet service provider, mobile carrier, and hardware ID.

c. Usage data

We record how you interact with our Services. For example, we log your taps/clicks on certain areas of the interface, the features, and content you interact with, how often you use the Services, and the amount of time you spend within them. We also track the age of your account and the duration of your Subscription, your Subscription orders, whether you currently have premium access, whether you accessed trial content, your total spending and refund activity across our platforms. We may also record the ads in our App or Website with which you interact (and the Internet links to which those ads lead). In case the App encounters any errors or crashes, we also receive crash reports that include information about the circumstances leading up to the issue.

d. Advertising IDs

We collect your Apple Identifier for Advertising (“IDFA”), Identifier for Vendor (“IDFV”) or Google Advertising ID (“AAID”) (depending on the operating system of your device) when you access our App or Website from a mobile device. You can typically reset these numbers through the settings of your device’s operating system (but we do not control this).

e. Transaction data

To purchase Subscription(s) or make other Purchases, you need to provide your financial account data, such as your credit card details. This data may contain personal data. Please note that transactions are managed by our trusted third-party providers, and we do not collect or store full credit card number data, though we may receive credit card-related data, data about the transaction, including: date, time and amount of the transaction, the type of payment method used, and the status of the transaction.

f. Cookies

A cookie is a small text file that is stored on a user’s device for record-keeping purposes. Cookies can be either session or persistent. A session cookie expires when you close your browser and is used to facilitate more straightforward navigation of our Services. A persistent cookie remains on your hard drive for an extended period of time. We also use tracking pixels that set cookies to assist with delivering online advertising.

Cookies are used, in particular, to automatically recognize you the next time you visit our Website. As a result, the information that you have earlier entered in certain fields on the Website may automatically appear the next time you use our Services. Cookie data will be stored on your device, and most of the time, only for a limited time period.

3. For What Purposes We Process Your Personal Data

3.1. To provide our Services

We process personal data to enable you to use the Services in a seamless manner and to prevent or address errors or technical issues.

To host personal data and enable our Services to operate and be distributed, we use **Google Cloud** ([Privacy Policy](#)) and **Namecheap** ([Privacy Policy](#)), platform for on-demand deployment, related hosting and backend services.

We use Firebase Performance Monitoring, Firebase Crash Reporting and Crashlytics, which are monitoring services provided by Google. To learn more, please visit [Google's Privacy Policy](#), [Privacy and Security in Firebase](#) and [Crashlytics' Data Collection Policy](#).

Clarity is a user behavior and website debugging analytics tool. We use it to understand how users are interacting with our Services through session replays and heatmaps. Clarity was developed by Microsoft, so you may find more info about Clarity's approach to privacy in [Microsoft Privacy Statement](#).

Sentry is a code analysis tool which allows us to log front-end mistakes, monitor the performance of client parts of a code, and analyse code vulnerabilities. While performing its functions, Sentry may access a limited number of your data, such as IP address, browser information, OS version, device type. More info about Sentry data processing is in [Privacy Policy](#).

CookieYes helps us to customize the cookie banner, record your consent, and manage other cookie compliance needs on our Website. You may find more information about your data processing by CookieYes in the [Data Processing Agreement](#).

Shake is a bug reporting and in-app feedback tool that helps us identify issues within our App and improve the user experience. Shake allows users to submit detailed reports about errors or unexpected behavior, which may include diagnostic information such as device details, app version, logs, screenshots, and other technical data relevant to the reported issue. This information enables us to investigate problems more efficiently and maintain the stability and performance of our Services. You may find more information about Shake's data processing practices in its [Privacy Policy](#).

3.2. To customize your experience

We process your personal data, such as preferences and goals set in the App, to tailor the content of the Services and make offers tailored to your personal preferences.

3.3. To manage your account and provide you with customer support

We process your personal data to secure access to your personal account and to send you technical notifications or emails regarding the performance of our Services, security, payment transactions, notices regarding the Terms and Conditions of Use, or this Privacy Policy.

3.4. To communicate with you regarding your use of our Services

We communicate with you, for example, by push notifications or by email. These may include reminders and motivational messages that encourage you to continue using the App, as well as other information about the Services. To opt out of receiving push notifications, you need to change the settings on your device. To opt out of receiving emails, you should click the unsubscribe link in the footer of our emails.

For this purpose, we may use **Customer.io**, a multi-channel marketing automation platform for delivery of emails, push notifications, and other service-related communications to our users. Customer.io processes certain user data to enable targeted messaging and improve the relevance of our communications. You may find more information about Customer.io's data processing practices in its [Privacy Policy](#).

3.5. To provide you with customer support

We process your personal data to respond to your requests for technical support.

We use **Zendesk** ticketing system to handle customer inquiries. When you send us inquiries via contact form or via email, we will store the details provided by you via Zendesk ticketing system, which enables us to track, prioritize and quickly solve your requests. To learn more, please visit this [Privacy Policy](#).

3.6. To research and analyze your use of the Services

This helps us to better understand our business, analyze our operations, maintain, improve, innovate, plan, design, and develop the Services and our new products. We also use such data for statistical analysis purposes, to test and improve our offers. This enables us to better understand what features our users like more, and which categories of users use our Services. As a result, we often decide how to improve the Services based on the results of this processing.

To perform research and analysis about how users interact with our Services we use **Appsflyer**. Appsflyer enables us to understand, in particular, how users find us (for example, who was the advertiser that delivered an ad to users, which led you to our Services). Appsflyer also provides us with different analytics tools that enable us to research and analyze use of the Services – [Privacy Policy](#), [Opt Out](#).

We use **Facebook Analytics**, which is a service provided by Facebook that allows us to use different analytical tools. On Facebook Analytics we get, in particular, aggregated demographics and insights on how many people access the Services, how often users make purchases, and other users' interactions within the Services – [Privacy Policy](#).

We also use **Amplitude**, an analytics service provided by Amplitude Inc. We use this tool to understand how users use our Services. Amplitude collects various technical information, in particular, time zone, type of device (phone or tablet), unique identifiers (such as IDFA). Amplitude also allows us to track various interactions that occur on the App or the Website. As a result, Amplitude helps us to decide which features we should focus on. Amplitude provides more information on how it processes data in its [Privacy Policy](#).

To track and analyze behavior of our Services' users (in particular, how they react to changes of App's or Website's structure, text or any other component), we use **Firebase Remote Config**. Firebase Remote Config is an A/B testing and configuration service provided by Google – [Privacy Policy](#) and [Privacy and Security in Firebase](#).

We also use **Firebase Analytics**, which is an analytics service provided by Google. In order to understand Google's use of data, consult Google's [Partner Policy](#) (see also, Firebase [Privacy information](#) and [Google's Privacy Policy](#)).

To perform our Website analysis, we also use **Tableau**, a company providing interactive data visualization products focused on business intelligence – [Tableau Privacy Policy](#).

3.7. To send you marketing communications

We process your personal data for our marketing campaigns. We may add your email address to our marketing list. As a result, you will receive information about our products, such as special offers. If you do not want to receive marketing emails from us, you can unsubscribe by following the instructions in the footer of the marketing emails.

We may send you push notifications for marketing purposes. To opt out of receiving push notifications, you need to change the settings on your device.

Customer.io is a multi-channel marketing automation platform that we use to deliver marketing emails, push notifications, and other service-related communications to our users. Customer.io processes certain user data to enable targeted messaging and improve the relevance of our communications. You may find more information about Customer.io's data processing practices in its [Privacy Policy](#).

3.8 To personalize our ads

We and our partners, including **Facebook** and **Google**, use your personal data to tailor ads and possibly even show them to you at the relevant time. For example, if you have installed our App, you might see ads of our products, for example, in your Facebook's feed.

How to opt out or influence personalized advertising

iOS: On your iPhone or iPad, go to Settings > Privacy & Security > Apple Advertising and deselect Personalized Ads.

Android: To opt-out of ads on an Android device, go to Settings > Privacy > Ads and enable Opt out of Ads personalization. In addition, you can reset your advertising identifier in the same section (this also may help you to see less of personalized ads).

macOS: On your MacBook, you can disable personalized ads: go to System Preferences > Security & Privacy > Privacy, select Apple Advertising, and deselect Personalized Ads.

Windows: On your laptop running Windows 10, you shall select Start > Settings > Privacy and then turn off the setting for Let apps use advertising ID to make ads more interesting to you based on your app activity. If you have other Windows version, please follow the steps [here](#).

Browsers: It is also may be possible to stop your browser from accepting cookies altogether by changing your browser's cookie settings. You can usually find these settings in the "options" or "preferences" menu of your browser. The following links may be helpful, or you can use the "Help" option in your browser.

Cookie settings in [Internet Explorer](#)

Cookie settings in [Firefox](#)

Cookie settings in [Chrome](#)

Cookie settings in Safari ([web](#) and [iOS](#))

To learn even more about how to affect advertising choices on various devices, please look at the information available [here](#).

In addition, you may get useful information and opt out of some interest-based advertising, by visiting the following links:

Network Advertising Initiative – <http://optout.networkadvertising.org/>

Digital Advertising Alliance – <http://optout.aboutads.info/>

Digital Advertising Alliance (Canada) – <http://youradchoices.ca/choices>

Digital Advertising Alliance (EU) – <http://www.youronlinechoices.com/>

DAA AppChoices page – <http://www.aboutads.info/appchoices>

Google allows its users to [opt out of Google's personalized ads](#).

We value your right to influence the ads that you see, thus we are letting you know what service providers we use for this purpose and how some of them allow you to control your ad preferences.

We use **Facebook pixel** on the Services. Facebook pixel is a code placed on the Services collecting data that helps us track conversions from Facebook Ads, build targeted audience and remarket to people who have taken some actions on the Services (for example, made a purchase).

We use **Facebook Ads Manager** together with **Facebook Custom Audience**, which allows us to choose audiences that will see our ads on Facebook or other Facebook's products (for example, Instagram). Through Facebook Custom Audience we may create a list of users with certain sets of data, such as an IDFA, choose users that have completed certain actions in App (for example, installed it). As a result, we may ask Facebook to show some ads to a particular list of users. As a result, more of our ads may show up while you are using Facebook or other Facebook's products (for example, Instagram). You may learn how to opt out of advertising provided to you through Facebook Custom Audience [here](#).

Facebook also allows its users to influence the types of ads they see on Facebook. To find how to control the ads you see on Facebook, please go [here](#) or adjust your [ads settings on Facebook](#).

Google Ads is an ad delivery service provided by Google that can deliver ads to users. In particular, Google allows to us to tailor the ads in way that they will appear, for example, only to users that have conducted certain actions with our App (for example, show our ads to users who have purchased a subscription). Some other examples of events that may be used for tailoring ads include, in particular, installing our App. Google allows its users to opt out of [Google's personalized ads](#).

3.9. To process your payments and refunds

We provide paid features and/or services within the Services. For this purpose, we use third-party payment processing services (for example, payment processors). As a result of this processing, you will be able to make a payment for a Subscription, and we will be notified that the payment has been made. We will also process your personal data to handle your refund requests as provided in our Terms and Conditions of Use.

We will not store or collect your payment card details ourselves. This information will be provided directly to our third-party payment processors.

We use **Solidgate**, which is a payment gateway service provider. Also, we may use **PayPal** ([Privacy Statement](#)) to process your payments.

3.10. To enforce our Terms and Conditions of Use and to prevent and combat fraud

We use personal data to enforce our agreements and contractual commitments, to detect, prevent, and combat fraud. As a result of such processing, we may share your information with others, including law enforcement agencies (in particular if a dispute arises under our Terms and Conditions of Use).

3.11. To comply with legal obligations

We may process, use, or share your data when the law requires it, in particular if a law enforcement agency requests it by lawful means.

3.12. To ensure the security of the Services

We process your personal data to ensure the security of our Services.

We use **Google Cloud Armor** and **Firebase App Check**, security services provided by Google, to help protect our Website, Application, and backend systems from fraudulent activity, misuse, and automated abuse. These technologies help us determine whether certain actions originate from legitimate users or unauthorized automated sources and ensure that requests to our systems come from genuine versions of our Application. By using these services, we are able to prevent fraudulent use of our Services, safeguard user data, and maintain the overall security and integrity of our platform. You can learn more by visiting Google's [Privacy Policy](#).

4. Under What Legal Bases We Process Your Personal Data

In this section, we are letting you know what legal basis we use for each particular purpose of processing. For more information on a particular purpose, please refer to Section 3. This section applies only to EEA-based users.

4.1. Your consent

Under this legal basis, we will send you marketing emails. You have the right to withdraw your consent at any time by clicking on the unsubscribe link in the footer of our marketing emails.

4.2. Performing our contract with you

Under this legal basis ,we:

- Provide our Services (in accordance with our Terms and Conditions of Use);
- Customize your experience;
- Manage your account and provide you with customer support;
- Communicate with you regarding your use of our Services; and
- Process your payments.

4.3. Legitimate interests, unless those interests are overridden by your interests or fundamental rights and freedoms that require the protection of personal data

We rely on legitimate interests:

- to communicate with you regarding your use of our Services. This includes, for example, sending you push notifications proposing that you try the specific feature of the App. The legitimate interest we rely on for this purpose is our interest in encouraging you to use our Services more often.
- to research and analyze your use of the Services. Our legitimate interest for this purpose is our interest in improving our Services so that we understand users' preferences and are able to provide you with a better experience (for example, to make the use of the App or the Website easier and more enjoyable, or to introduce and test new features).
- to send you marketing communications. The legitimate interest we rely on for this processing is our interest in promoting our Services in a measured and appropriate way.
- to personalize our ads. The legitimate interest we rely on for this processing is our interest in promoting our Services in a reasonably targeted way.
- to enforce our Terms and Conditions of Use and to prevent and combat fraud. Our legitimate interests for this purpose are enforcing our legal rights, preventing and addressing fraud and unauthorized use of the Services, and non-compliance with our Terms and Conditions of Use.

4.4. Compliance with legal obligations.

5. With Whom We Share Your Personal Data

We share information with third parties that help us operate, provide, improve, integrate, customize, support, and market our Services. We may share some sets of personal data, in particular, for purposes indicated in Section 3 of this Privacy Policy. The types of third parties we share information with include, in particular:

5.1. Service providers

We share personal data with third parties that we hire to provide services or perform business functions on our behalf, based on our instructions. We share your personal information with the following types of service providers:

- mobile app marketplaces (Apple App Store, Clarity, Sentry);
- cloud storage providers (Google, Namecheap);
- authentication providers (Apple, Google);
- data analytics providers (Facebook, Appsflyer, Firebase, Amplitude, Tableau);
- marketing partners (in particular, social media networks, marketing agencies, Facebook, Google);
- measurement partners (CookieYes);
- online security solutions provider (Google);
- payment processing providers (Solidgate, PayPal).
- communication services providers (Customer.io, Zendesk).

5.2. Law enforcement agencies and other public authorities

We may use and disclose personal data to enforce our Terms and Conditions of Use, to protect our rights, privacy, safety, or property, and/or that of our affiliates, you or others, and to respond to requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, or in other cases provided for by law.

5.3. Third parties as part of a merger or acquisition

As we develop our business, we may buy or sell assets or business offerings. Customers' and users' information is generally one of the transferred business assets in these types of transactions. We may also share such information with any affiliated entity (e.g., parent company or subsidiary) and may transfer such information in the course of a corporate transaction, such as the sale of our business, a divestiture, merger, consolidation, or asset sale, or in the unlikely event of bankruptcy.

6. How You Can Exercise Your Privacy Rights

To be in control of your personal data, you have the following rights:

Accessing / reviewing / updating / correcting your personal data. You may review, edit, or change the personal data that you had previously provided on the Services.

Deleting your personal data. You can request erasure of your personal data as permitted by law. When you request deletion of your personal data, we will use reasonable efforts to honor your request. In some cases, we may be legally required to keep some of the data for a certain time; in such event, we will fulfill your request after we have complied with our obligations.

Objecting to or restricting the use of your personal data. You can ask us to stop using all or some of your personal data or limit our use thereof.

Additional information for EEA-based users:

If you are based in the EEA, you have the following rights in addition to the above:

The right to lodge a complaint with the supervisory authority. We would love you to contact us directly, so we can address your concerns. Nevertheless, you have the right to lodge a complaint with a competent data protection supervisory authority, in particular in the EU Member State where you reside, work, or where the alleged infringement has taken place.

The right to data portability. If you wish to receive your personal data in a machine-readable format, you can send a respective request to us as described below.

To exercise any of your privacy rights, please send a request to support@powero.app.

7. Age Limitation

We do not knowingly process personal data from persons under 16 years of age. If you learn that anyone younger than 16 has provided us with personal data, please contact us at support@powero.app.

8. International Data Transfers

We do business globally. We may transfer personal data to countries other than the country in which the data was originally collected in order to provide the Services set forth in the Terms and Conditions of Use and for purposes indicated in this Privacy Policy. If these countries do not have data protection laws equivalent to those of the country in which you initially provided the information, we deploy additional safeguards.

In particular, if we transfer personal data originating from the EEA to countries with not adequate level of data protection, we use one of the following legal bases: (i) Standard Contractual Clauses approved by the European Commission (details available [here](#)), or (ii) the European Commission adequacy decisions about certain countries (details available [here](#)).

9. Changes to This Privacy Policy

We may modify this Privacy Policy from time to time. If we decide to make material changes to this Privacy Policy, you will be notified through our Services or by other available means and will have an opportunity to review the revised Privacy Policy. By continuing to access or use the Services after those changes become effective, you agree to be bound by the revised Privacy Policy.

10. Supplemental Notice for California Residents

This Supplemental California Privacy Notice only applies to our processing of personal information that is subject to the California Consumer Privacy Act of 2018 (the “CCPA”). The CCPA provides California residents with the right to know what categories of personal information we have collected about them and whether we disclosed that personal information for a business purpose (e.g., to a service provider) in the preceding twelve months. California residents can find this information below.

Category of Personal Information Collected	Categories of Third Parties to Whom Personal Information is Disclosed for a Business Purpose
Identifiers	Service providers Users or third parties you share with
Personal information categories listed in Cal. Civ. Code § 1798.80(e)	Service providers Users or third parties you share with
Commercial information	Payment solutions partners
Internet or other electronic network activity	Service providers Users or third parties you share with
Geolocation data	Service providers
Inferences drawn from other personal information to create a profile about a consumer	Service providers

The categories of sources from which we collect personal information and our business and commercial purposes for using personal information are set forth above.

“Sales” of Personal Information under the CCPA. For purposes of the CCPA, we do not “sell” personal information, nor do we have actual knowledge of any “sale” of personal information of minors under 16 years of age.

Non-Discrimination. California residents have the right not to be subjected to discriminatory treatment by us for exercising their rights under the CCPA.

Authorized Agent. Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. To designate an authorized agent, please contact us as set forth below.

Verification. When you make a request, we will ask you to provide sufficient information to allow us to reasonably verify that you are the person about whom we collected personal information, or an authorized representative, which may include confirming the email address associated with any personal information we have about you.

If you are a California resident and would like to exercise any of your rights under the CCPA, please contact us at support@powero.app. We will process such requests in accordance with applicable laws.

11. Supplemental Notice for Virginia Residents

This Supplemental Virginia Privacy Notice only applies if you reside in the Commonwealth of Virginia. Where applicable, it describes how we use and process your personal data and explains your particular rights under the Virginia Consumer Data Privacy Act (“VCDPA”).

Disclosures about the use of your personal data. We may collect and use certain information about you, some of which may be personal data (such as your name, email address, IP address, or other information that may be reasonably linked to you), to operate the Services and to maximize your experience.

If you would like more information about the categories of your personal data we collect or the purposes for which we collect them, please read Sections 2 and 3. To learn more about the sharing of your personal data with our business partners and other third parties, please read Section 5.

Data Rights. Section 6 of our Privacy Policy describes the data rights we offer to all users and how to exercise these rights. This includes the right to access, review, correct, update your data, obtain a portable copy of your data, or delete data related to your stored preferences and your use of the Services. Before completing your request, we may require some information sufficient to authenticate your identity.

Additionally, VCDPA provides Virginia residents with these data rights:

- Opt out of the Processing of your Personal Data for Targeted Advertising. In order to exercise your choice as a Virginia resident, please contact us at support@powero.app with the subject line “Virginia Do Not Sell Request”. We will process such requests in accordance with applicable laws.

Please note that we do not process personal data for purposes of (1) the sale of personal data, as defined by the VCDPA, or (2) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

- Confirm whether your Personal Data is being Processed. You may confirm whether your personal data is being processed by emailing us at support@powero.app.
- Appeal a Case regarding your Request. If we declined to take action on your data rights request or rejected it, you may contact us at support@powero.app to appeal this decision. Please use the subject line “Appeal of Refusal to Take Action on Privacy Request” and provide the relevant information in the email. Once we receive your appeal, we will notify you in writing within 60 days of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision.

If your appeal is denied, you may contact the Office of the Virginia Attorney General by these means:

Office of the Attorney General | Virginia.gov
www.virginia.gov/agencies/office-of-the-attorney-general/#vagov
202 North Ninth Street
Richmond, VA 23219

12. Supplemental Notice for Nevada Residents

If you are a resident of Nevada, you have the right to opt out of the sale of certain personal information to third parties who intend to license or sell that personal information. You can exercise this right by contacting us at support@powero.app with the subject line “Nevada Do Not Sell Request” and providing us with your name and the email address associated with your account. Please note that we do not currently sell your personal information as sales are defined in Nevada Revised Statutes Chapter 603A.

13. Security measures

We employ reasonable and appropriate security measures to protect personal data from unauthorized access, use, or disclosure. These measures are designed to ensure the confidentiality, integrity, availability, and resilience of the systems and services that process personal data.

In particular, we:

- Employ advanced encryption for data both in transit and at rest;
- Securely store data with reputable cloud providers;
- Enforce a need-to-know access policy, limiting access to authorized personnel only;
- Utilize firewalls;
- Conduct regular data backups;
- Continuously review and enhance our security practices to align with evolving industry standards and best practices.

14. Cancellation and Account Deletion

You can delete your account at any time using the functionality found in “Settings” in the App or the Website, or by contacting us at support@powero.app. Upon your request, we will delete your account and all associated data, except for limited information, which will be stored for specific purposes and a limited period, as set forth in this Privacy Policy. The deletion process may take up to 30 days to complete.

Please note that once you initiate the deletion process, your account can no longer be used, and you will lose access to all subscription features. To avoid any additional charges, you must cancel your subscription prior to account deletion.

15. Data retention

We will store your personal data for as long as it is reasonably necessary for achieving the purposes set forth in this Privacy Policy (including providing the Services to you), which includes (but is not limited to) the period during which you have an account with the Services. We will also retain and use your personal data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. We may consider deleting the account and/or removing the data upon the written request, e.g., in case of violation.

16. How “Do Not Track” Requests are Handled

Except as otherwise stipulated in this Privacy Policy, this App does not support “Do Not Track” requests. To determine whether any of the third-party services it uses honor the “Do Not Track” requests, please read their privacy policies.

Contact Us

You may contact us at any time for details regarding this Privacy Policy and its previous versions. For any questions concerning your account or your personal data, please contact us at support@powero.app.

Last Update: December 12th, 2025.