

## **1. INTRODUCTION**

**Archelon Software LTD.** ("Company," "we," or "us") is committed to respecting your privacy and maintaining transparency regarding our data handling practices. This Privacy Policy explains how we collect, store, use, transfer, and disclose personal data from our users ("you") in connection with the Company's mobile applications, websites, and related services.

---

## **CONTACT INFORMATION**

**Company:** Archelon Software LTD.

**Registration:** Cyprus Limited Liability Company (Reg. No. HE 444026)

**Registered Address:** 3 Agisandrou, Office 102, Zakaki 3046, Limassol, Cyprus

**Email:** [contact@archelon.dev](mailto:contact@archelon.dev)

---

## **SCOPE OF THIS POLICY**

This Policy applies to the following applications and services (collectively referred to as the "Apps" and individually as the "App") operated by Archelon Software LTD.:

**Easy Fit:** Targeted, low-impact workouts with intuitive progress tracking. Designed for users following a bland diet to support digestion and help manage dietary restrictions.

Additionally, this Privacy Policy applies to all content made available through the Apps, our official website at <https://archelon.dev>, any related web pages, as well as our email communications and notifications (collectively referred to as the "Content").

---

## **HOW WE UPDATE THIS POLICY**

We may update this Privacy Policy from time to time. If any changes are made, we will notify you through one or more of the following methods:

- **Email Notification** – sent to the email address associated with your account.
- **In-App Notification** – displayed within the Apps and requiring your review and acceptance before continuing use.

- **Website Announcement** – for minor changes, an update notice will be posted on our website.

Where required by applicable data protection laws (such as the GDPR, CCPA, or other relevant frameworks), we may also seek your explicit consent before implementing new data processing practices or collecting additional Personal Data.

By continuing to use our Apps or website after an update becomes effective, you acknowledge and agree to the revised terms. If you do not agree with the updated terms, you must stop using the Apps and delete them from your devices.

---

## 2. PERSONAL DATA AND INFORMATION WE COLLECT ABOUT YOU

### 2.1. Types of Data We Collect and Process

We collect and process various types of data to operate, improve, and personalize our services. The table below outlines:

- The types of data we collect
- The purpose of data processing
- The source of the data
- The legal basis or business purpose for processing (as required by laws such as GDPR, CCPA, etc.)

Data We Process	Purpose of Processing	How We Collect This Data	Legal Basis / Business Purpose
<b>Account Information</b> (e.g., name, email, password)	To create and manage your account and provide service access	Directly from you during registration	Contractual necessity
<b>Profile Information</b> (e.g., age, gender, height, weight, dietary preferences, fitness goals)	To personalize your experience and features	Directly from you when setting up your profile	Contractual necessity

<b>Health-Related Information</b> (e.g., conditions, symptoms, menstrual cycle, hydration, activity)	To track progress and provide insights	Direct input in the app, with explicit consent	Explicit consent (sensitive data)
<b>Payment Information</b> (e.g., partial credit card details, transaction history)	To process subscriptions and purchases	Through payment providers (e.g., Stripe, Apple, Google)	Contractual necessity, Legitimate interest
<b>Usage Data</b> (e.g., time spent, features used, interactions)	To improve performance and user experience	Automatically collected	Legitimate interest
<b>Device Information</b> (e.g., IP address, OS, browser, language)	To maintain app functionality and security	Automatically collected	Legitimate interest
<b>Cookies &amp; Tracking Data</b>	To personalize experience and optimize marketing	Through cookies and similar technologies	Consent
<b>Advertising IDs</b> (e.g., IDFA, AAID)	To measure and optimize ad campaigns	From third-party login/auth systems	Consent
<b>Geolocation Data</b> (e.g., region, country)	To customize content, ensure security, prevent fraud	Automatically if location is enabled	Consent
<b>Marketing &amp; Ad Performance Data</b>	To assess and improve marketing effectiveness	From advertising partners	Legitimate interest
<b>Support &amp; Communication Data</b> (e.g., feedback, email/chat history)	To respond to support requests and product updates	Directly from you	Legitimate interest

---

## 2.2. Integration with Apple HealthKit and Google Health Connect

You may optionally allow the Apps to import or export health-related data from third-party services such as **Apple HealthKit** and **Google Health Connect**. This may include (but is not limited to):

- Workout and sports activity

- Body weight
- Calories burned
- Heart rate
- Step count or distance walked
- Other fitness-related metrics

This data enhances your health tracking experience and enables more accurate insights and personalized recommendations within the Apps.

---

### 2.3. Important Notes on HealthKit & Health Connect Data

- We **do not** use data from Apple HealthKit or Google Health Connect for advertising.
- We **do not** share such data with third parties without your express permission.
- We **do not** sell such data to advertisers, data brokers, or any third parties.

By enabling integration, you agree that your health data may be used within the Apps to provide enhanced functionality. You can revoke this access at any time via app settings or within your third-party service's privacy controls.

---

### 2.4. Information from Third Parties

We may also receive additional data about you from third-party sources, unless explicitly restricted by applicable law. This information is only used for the purposes for which it was shared with us.

We **do not collect or process sensitive personal data** unless explicitly permitted — as in the case of health data described in section 2.3.

---

### 2.5. Non-Personal and Aggregated Data

When data is aggregated or anonymized so that it can no longer reasonably identify a person, we may use it for any lawful business purpose. If any aggregated data is later re-identified, it will again be treated as Personal Data under this Privacy Policy.

## 3. HOW WE USE YOUR DATA

We use the information we collect to deliver, optimize, and personalize your experience across our Apps and services. Below is a summary of the main purposes for which we process your data:

---

### 3.1. Providing and Improving Our Services

We process your data to ensure that our services function effectively and meet your expectations, including:

- **Account Management** – Creating, maintaining, and updating your user account; enabling access to the Apps and related features.
  - **Personalized Experience** – Customizing content and tools (such as tracking features, fitness plans, and dietary guidance) based on your input (e.g., goals, symptoms, or preferences).
  - **Health & Fitness Tracking** – Processing your health-related inputs to help you track progress, set goals, and monitor key metrics (e.g., activity, weight, hydration).
  - **Recommendations** – Offering meal suggestions, exercise routines, and personalized adjustments aligned with your fitness and nutrition needs.
- 

### 3.2. Communication and Customer Support

We use your data to communicate with you and respond effectively to your inquiries:

- **Account Updates** – Sending important notifications related to your account (e.g., subscription changes, payment confirmations, or service alerts).
  - **Customer Support** – Responding to requests for assistance and resolving technical or account-related issues.
  - **Feedback Collection** – Gathering your input through surveys or feedback forms to improve our services and user experience.
- 

### 3.3. Health Insights and Recommendations

With your explicit consent, we use your health-related data to provide targeted support:

- **Health Trends Analysis** – Monitoring and analyzing changes in your health data to deliver relevant feedback and insights.

- **Personalized Guidance** – Sharing relevant content, tips, and suggestions tailored to your health status or conditions (e.g., symptom management, nutrition plans).
  - **Outcome Improvement** – Recommending adjustments to your wellness routines based on tracked progress to support long-term goals.
- 

### 3.4. Analytics and Product Development

We analyze data to enhance the performance and reliability of our services:

- **Service Optimization** – Studying usage behavior to improve functionality, responsiveness, and user satisfaction.
  - **Feature Innovation** – Informing the development of new features and services to better align with user needs.
  - **Research** – Using de-identified, aggregated data to conduct internal research (e.g., dietary or fitness trends). This data cannot be used to identify any individual.
- 

### 3.5. Marketing and Advertising

With your consent and in accordance with applicable regulations, we may use your data for marketing purposes:

- **Targeted Advertising** – Displaying personalized advertisements based on your usage behavior and preferences.
- **Promotions & Offers** – Sharing marketing content such as updates, special promotions, and feature announcements.
- **Performance Monitoring** – Measuring the effectiveness of marketing campaigns across platforms such as Google and Meta (Facebook).

You can manage or revoke your marketing preferences at any time via your App settings or by contacting us.

---

### 3.6. Legal and Regulatory Compliance

We may process your data when necessary to comply with our legal obligations or to defend our legal rights:

- **Regulatory Compliance** – Fulfilling obligations under applicable laws, including financial and tax reporting.
  - **Fraud Detection & Security** – Preventing, identifying, and addressing fraud, abuse, or security breaches.
  - **Dispute Resolution** – Enforcing our Terms of Service and Privacy Policy, responding to legal claims, and complying with law enforcement requests.
- 

### 3.7. Consent Management

For certain activities (such as processing sensitive health data or sending marketing communications), we rely on your explicit consent. You may withdraw your consent at any time without affecting the lawfulness of processing prior to withdrawal.

#### Ways to Withdraw Consent:

- **Emails** – Click the "unsubscribe" link in any marketing email you receive.
  - **Push Notifications** – Adjust your notification settings on your mobile device.
  - **App Settings** – Change your marketing or data preferences directly within the App.
  - **Contact Us** – You can email us at **support@shredybot.com** to request removal from promotional communications.
- 

### 3.8. Automated Decision-Making and Profiling

We may use automated processing and profiling to deliver personalized health and fitness recommendations. However, no decision with legal or similarly significant effects will be made solely based on automated decision-making.

If you wish to learn more about how we use automated tools or wish to challenge a decision, please contact us at **support@shredybot.com**.

---

## 4. YOUR RIGHTS

We respect your rights to privacy and provide you with meaningful control over your Personal Data. Depending on your place of residence, you may have specific legal rights regarding how your information is collected, processed, shared, and retained.

---

#### 4.1. Rights of U.S. Residents (CCPA and Similar State Laws)

If you reside in the United States, your privacy rights may vary depending on your state's legislation (e.g., CCPA, CPRA). These rights may include:

- **Right to Know** – You have the right to request information about the Personal Data we have collected, including the categories of sources, purposes of collection, categories of third parties with whom we share data, and the specific data collected about you.
- **Right to Data Portability** – You may request a copy of your Personal Data in a portable and structured format.
- **Right to Deletion** – You have the right to request deletion of your Personal Data we have collected from you, subject to certain legal exceptions.
- **Right to Correction** – You may request that we correct any inaccurate or outdated information we hold about you, subject to appropriate verification.
- **Right to Opt Out of Sale or Sharing** – You may opt out of the “sale” or “sharing” of your Personal Data, including data used for targeted advertising (as defined under applicable state privacy laws).
- **Right to Non-Discrimination** – You are entitled to exercise your privacy rights without being subject to discriminatory treatment.
- **Right to Restrict Use of Sensitive Information** – You may request that we limit the use and disclosure of sensitive categories of Personal Data.

---

#### 4.2. Do Not Sell or Share My Personal Information (CCPA Opt-Out)

Under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), California residents have the right to opt out of the “sale” or “sharing” of their Personal Data.

**Please note:**

- We **do not** sell Personal Data to third parties.
- We **do not** share health-related or sensitive Personal Data for advertising purposes.
- However, the use of certain third-party analytics or advertising tools may qualify as a “sale” or “sharing” under California law.



If you are a California resident and would like to exercise your right to opt out of the sale or sharing of your Personal Data, you may:

- Email us at **support@shredybot.com** with the subject line “**Do Not Sell My Personal Information**”
  - Disable cookies and tracking technologies via your browser or App settings
- 

#### 4.3. Rights of EU/EEA Residents (GDPR Compliance)

If you reside in a country within the European Union or the European Economic Area, the General Data Protection Regulation (GDPR) grants you the following rights:

- **Right to Rectification** – You may request correction of inaccurate or incomplete Personal Data.
- **Right to Access and Data Portability** – You may request access to your Personal Data and receive it in a structured, commonly used, machine-readable format.
- **Right to Erasure (Right to Be Forgotten)** – You may request deletion of your Personal Data where it is no longer necessary for the purposes for which it was collected, subject to certain legal obligations.
- **Right to Restrict Processing** – You may request limited use of your Personal Data under specific circumstances (e.g., when disputing its accuracy).
- **Right to Object** – You may object to our processing of your data for direct marketing or when processing is based on our legitimate interests.
- **Right to Withdraw Consent** – If processing is based on your consent, you may withdraw it at any time, without affecting the lawfulness of prior processing.
- **Right to Lodge a Complaint** – You may file a complaint with your local Data Protection Authority if you believe your rights under GDPR have been violated.

To protect your data and prevent unauthorized access, we may ask you to verify your identity (e.g., by providing an ID or other proof) when exercising these rights, especially when dealing with sensitive information such as health-related data.

---

#### 4.4. How to Exercise Your Rights

To exercise any of your privacy rights under this Policy or applicable data protection laws, you may contact us via:

- **Email:** support@shredybot.com
- **Mailing Address:** 3 Agisandrou, Office 102, Zakaki 3046, Limassol, Cyprus

We will take reasonable steps to verify your identity before processing your request. You can expect a response within one calendar month from the date of receipt (this period may be extended in complex cases).

If you have concerns regarding our handling of your Personal Data, you may also contact your local **Data Protection Authority** (for EU/EEA residents) or your **State Attorney General** (for U.S. residents).

---

## 5. SHARING YOUR PERSONAL DATA AND INFORMATION

We only share your Personal Data with third parties as outlined in this Privacy Policy and in full compliance with applicable data protection laws.

---

### 5.1. Categories of Third Parties with Whom We May Share Your Data

We may disclose your Personal Data to the following categories of third parties for the purposes described below:

Category of Third Party	Purpose of Sharing	Examples
<b>Service Providers &amp; Contractors</b>	To support essential business operations, such as payment processing, cloud hosting, customer service, and infrastructure maintenance.	Apple Pay, Google Pay, DigitalOcean, Google Cloud
<b>Analytics &amp; Performance Tools</b>	To better understand user behavior and improve App performance and usability.	Google Analytics, Firebase, Amplitude
<b>Advertising &amp; Marketing Partners</b> <i>(only with your consent)</i>	To serve personalized advertisements and evaluate the effectiveness of marketing efforts.	AppsFlyer, Meta (Facebook), X (formerly Twitter)
<b>Legal &amp; Regulatory Authorities</b>	To comply with legal obligations, court orders, and legitimate law enforcement requests.	Tax authorities, courts, law enforcement agencies

**Corporate Transactions**

In the event of a business sale, merger, reorganization, or acquisition, your data may be transferred as part of the transaction.

Acquiring companies or merger participants

---

## 5.2. Sharing with Third-Party Service Providers

We engage trusted third-party service providers who are contractually bound to:

- Use your Personal Data solely for the purpose of delivering agreed services on our behalf.
- Maintain strict confidentiality and data security practices.
- Adhere to applicable privacy and data protection regulations.
- Process data only as instructed and never for their own purposes.

Below are examples of third-party providers we may share your data with:

- **AppsFlyer** – A mobile marketing platform used for analytics and campaign performance. While we may share limited, non-sensitive personal information (never health-related data), this is strictly for campaign optimization. [Learn more](#)
- **Facebook (Meta)** – Used for serving targeted advertising across the Facebook network. Data shared is limited to behavioral information and does not include personally identifiable or sensitive data. [Advertising policy](#)
- **Crashlytics** – A crash reporting tool by Google used to detect, report, and fix app crashes. It may collect device-level technical data to help diagnose issues. [Crashlytics info](#)
- **Intercom** – A communication platform we use to manage customer service and user messaging. It may store your name, email, and interaction history to facilitate support. [Privacy policy](#)
- **X (formerly Twitter)** – Our advertising partner. X may use non-personal information to deliver interest-based ads. [Privacy policy](#)
- **Firebase** – A Google-owned analytics and infrastructure platform. Used for app performance monitoring, crash tracking, and event logging. It may collect device IDs and usage metrics. [Firebase info](#)
- **DigitalOcean** – Our cloud infrastructure provider, which stores and processes data necessary to deliver our services securely and reliably. [Privacy policy](#)

- **Stripe** – Our secure payment processor for handling transactions and preventing fraud. It may collect and store payment-related Personal Data. [Stripe privacy](#)
- 

### 5.3. Sharing of Aggregated or Anonymized Data

We may also share **aggregated, anonymized, or de-identified data** that cannot reasonably be used to identify you. This information may be used for research, statistics, publications, or other business purposes. For example:

- Publishing anonymized user trends in articles or reports
- Sharing general age group statistics or symptom trends across user bases

This type of data does **not** contain Personal Data and is not subject to this Privacy Policy once de-identified.

## 6. DATA SECURITY

We take the security of your Personal Data seriously and implement a combination of technical, organizational, and legal measures to protect it. Our security practices follow widely accepted industry standards, both during data transmission and at rest.

Key security measures include:

- **Encryption in Transit and at Rest** – All data transmissions between your device and our servers are encrypted using TLS/SSL protocols.
- **Vulnerability Scanning and Penetration Testing** – We regularly conduct security audits, penetration testing, and vulnerability assessments to identify and resolve potential risks.
- **Access Control and Confidentiality Measures** – Access to Personal Data is role-based and strictly limited to authorized personnel who require it for operational purposes. All employees are contractually bound to confidentiality obligations and are held accountable for any unauthorized access, disclosure, alteration, or misuse.
- **Privacy by Design and Default** – We perform regular Data Protection Impact Assessments (DPIAs) to ensure compliance with the principles of privacy by design and by default, as well as other internationally recognized privacy standards. In the event of a merger, acquisition, or other structural change, we commit to conducting a privacy audit.

Please note that no method of transmission over the Internet or method of electronic storage is completely secure. While we do our best to protect your Personal Data, we cannot

guarantee absolute security. If you have any concerns about security within our Apps, please contact us at [support@shredybot.com](mailto:support@shredybot.com).

---

## 7. RETENTION AND STORAGE OF YOUR PERSONAL DATA

We retain your Personal Data only for as long as necessary to provide you with services, or as required by law. Specifically:

- Your Personal Data will be retained while the App remains installed on your device or as long as your account is active.
- If you delete the App, your Personal Data will be removed from our active systems, with the exception of backup copies retained only as necessary to comply with legal obligations, resolve disputes, and enforce our agreements.

To cancel your account or request that we stop using your Personal Data, please contact us at [support@shredybot.com](mailto:support@shredybot.com).

All Personal Data is stored and processed on servers located in the **United States**.

---

## 8. CHILDREN'S PRIVACY

We are committed to protecting the privacy of children. Our Apps are **not intended for use by individuals under the age of 18**, and we do not knowingly collect or process Personal Data from anyone under 18.

If we become aware that we have inadvertently collected Personal Data from a child under the age of 18, we will promptly delete such information and, if applicable, terminate the associated account.

If you believe a child under the age of 16 is using the App or has submitted Personal Data, please notify us immediately at [support@shredybot.com](mailto:support@shredybot.com).

---

## 9. DATA PROTECTION OFFICER

If you have any questions about this Privacy Policy or how your Personal Data is handled, or if you wish to contact our **Data Protection Officer**, please email us at:  
[support@shredybot.com](mailto:support@shredybot.com)

---

## 10. CONTACTING US

If you have any questions, concerns, or complaints regarding your privacy, your rights under this Policy, or our data handling practices, you can contact us at:

**[support@shredybot.com](mailto:support@shredybot.com)**

---