

Privacy Policy

Safeguard Equipment Apps

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

- **Account** means a unique account created for You to access our Service or parts of our Service.
- **Affiliate** means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.
- **Application** refers to Safeguard App, the software program provided by the Company.
- **Business**, for the purpose of CCPA/CPRA, refers to the Company as the legal entity that collects Consumers' personal information and determines the purposes and means of the processing of Consumers' personal information, or on behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.
- **CCPA** and/or **CPRA** refers to the California Consumer Privacy Act (the "CCPA") as amended by the California Privacy Rights Act of 2020 (the "CPRA").
- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Safeguard Equipment, Inc., 4202 West Riverbend Ave, Post Falls, ID 83854. For the purpose of the GDPR, the Company is the Data Controller.

- **Cookies** are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses.
- **Consumer**, for the purpose of the CCPA/CPRA, means a natural person who is a California resident. A resident, as defined in the law, includes (1) every individual who is in the USA for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the USA who is outside the USA for a temporary or transitory purpose.
- **Data Controller**, for the purposes of the GDPR (General Data Protection Regulation), refers to the Company as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.
- **Device** means any device that can access the Service such as a computer, a cellphone or a digital tablet.
- **Do Not Track (DNT)** is a concept that has been promoted by US regulatory authorities, in particular the U.S. Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism for allowing internet users to control the tracking of their online activities across websites.
- **GDPR** refers to EU General Data Protection Regulation.
- **Personal Data** is any information that relates to an identified or identifiable individual.

For the purposes of GDPR, Personal Data means any information relating to You such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. For the purposes of the CCPA/CPRA, Personal Data means any information that identifies, relates to, describes or is capable of being associated with, or could reasonably be linked, directly or indirectly, with You.

- **Service** refers to the Application.
- **Service Provider** means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used. For the purpose of the GDPR, Service Providers are considered Data Processors.
- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- **You** means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable. Under GDPR, You can be referred to as the Data Subject or as the User as you are the individual using the Service.

Collecting and Using Your Personal Data

Types of Data Collected

Personal Data

While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

- First name and last name
- Phone number
- Geolocation data
- Usage Data

Usage Data

Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data. When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Cookies and Similar Technologies

We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service. The technologies We use may include:

Cookies or Browser Cookies. A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser.

We use both Session and Persistent Cookies for the purposes set out below:

Necessary / Essential Cookies

Type: Session Cookies

Administered by: Us

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

Cookies Policy / Notice Acceptance Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

Functionality Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

For more information about the cookies we use and your choices regarding cookies, please see the Cookies and Similar Technologies section of our Privacy Policy.

Information Collected while Using the Application

While using Our Application, in order to provide features of Our Application, We may collect, with Your prior permission:

- Geolocation data
- User settings
- Emergency contacts
- Emergency event data

We use this information to provide features of Our Service, to improve and customize Our Service. The information may be uploaded to the Company's servers and/or a Service Provider's server or it may be simply stored on Your device. You can enable or disable access to this information at any time, through Your Device settings.

Use of Your Personal Data

The Company may use Personal Data for the following purposes:

- **To provide and maintain our Service,** including to monitor the usage of our Service.
- **To manage Your Account:** to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- **For the performance of a contract:** the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.
- **To contact You:** To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
- **To manage Your requests:** To attend and manage Your requests to Us.
- **For business transfers:** We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.
- **For other purposes:** We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

- **For business transfers:** We may share or transfer Your personal 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.
- **With Affiliates:** We may share Your information with Our affiliates, in which case We will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
- **With other users:** when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
- **With Your consent:** We may disclose Your personal information for any other purpose with Your consent.

Retention of Your Personal Data

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to and maintained on computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Delete Your Personal Data

You have the right to delete or request that We assist in deleting the Personal Data that We have collected about You.

Our Service may give You the ability to delete certain information about You from within the Service.

You may update, amend, or delete Your information at any time by signing in to Your Account, if you have one, and visiting the account settings section that allows you to manage Your personal information. You may also contact Us to request access to, correct, or delete any personal information that You have provided to Us.

Please note, however, that We may need to retain certain information when we have a legal obligation or lawful basis to do so.

Disclosure of Your Personal Data

Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law Enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other Legal Requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public

- Protect against legal liability

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

Encryption

All personal data is encrypted at rest to ensure that the data is secure before being written to disk. Data is encrypted in transit using TLS (Transport Layer Security) protocols to protect data during transmission and prevent unauthorized access.

Detailed Information on the Processing of Your Personal Data

The Service Providers We use may have access to Your Personal Data. These third-party vendors collect, store, use, process and transfer information about Your activity on Our Service in accordance with their Privacy Policies.

Usage, Performance and Miscellaneous

We may use third-party Service Providers to maintain and improve our Service.

- **Auth0**
 - Their Privacy Policy can be viewed at <https://auth0.com/docs/secure/data-privacy-and-compliance>
- **Microsoft Azure Services**
 - Their Privacy Policy and related legal information can be viewed at <https://azure.microsoft.com/en-us/support/legal/>
- **Twilio**
 - Their Privacy Policy can be viewed at <https://www.twilio.com/en-us/legal/privacy>
- **Google Maps API's**
 - Their Privacy Policy can be viewed at <https://policies.google.com/privacy?hl=en>
- **Firebase Crashlytics**
 - Their Privacy Policy and related legal information can be viewed at <https://firebase.google.com/support/privacy/>

GDPR Privacy

Legal Basis for Processing Personal Data under GDPR

We may process Personal Data under the following conditions:

- **Consent:** You have given Your consent for processing Personal Data for one or more specific purposes.
- **Performance of a contract:** Provision of Personal Data is necessary for the performance of an agreement with You and/or for any pre-contractual obligations thereof.
- **Legal obligations:** Processing Personal Data is necessary for compliance with a legal obligation to which the Company is subject.
- **Vital interests:** Processing Personal Data is necessary in order to protect Your vital interests or of another natural person.
- **Public interests:** Processing Personal Data is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Company.
- **Legitimate interests:** Processing Personal Data is necessary for the purposes of the legitimate interests pursued by the Company. In any case, the Company will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Your Rights under the GDPR

The Company undertakes to respect the confidentiality of Your Personal Data and to guarantee You can exercise Your rights.

You have the right under this Privacy Policy, and by law if You are within the EU, to:

- **Request access to Your Personal Data.** The right to access, update or delete the information We have on You. Whenever made possible, you can access, update or request deletion of Your Personal Data directly within Your account settings section. If you are unable to perform these actions yourself, please contact Us to assist You. This also enables You to receive a copy of the Personal Data We hold about You.
- **Request correction of the Personal Data that We hold about You.** You have the right to have any incomplete or inaccurate information We hold about You corrected.
- **Object to processing of Your Personal Data.** This right exists where We are relying on a legitimate interest as the legal basis for Our processing and there is something about Your particular situation, which makes You want to object to our processing of Your Personal Data on this ground. You also have the right to object where We are processing Your Personal Data for direct marketing purposes.
- **Request erasure of Your Personal Data.** You have the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it.
- **Request the transfer of Your Personal Data.** We will provide to You, or to a third-party You have chosen, Your Personal Data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which You initially provided consent for Us to use or where We used the information to perform a contract with You.
- **Withdraw Your consent.** You have the right to withdraw Your consent on using your Personal Data. If You withdraw Your consent, We may not be able to provide You with access to certain specific functionalities of the Service.

Exercising of Your GDPR Data Protection Rights

You may exercise Your rights of access, rectification, cancellation and opposition by contacting Us. Please note that we may ask You to verify Your identity before responding to such requests. If You make a request, We will try our best to respond to You as soon as possible.

You have the right to complain to a Data Protection Authority about Our collection and use of Your Personal Data. For more information, if You are in the European Economic Area (EEA), please contact Your local data protection authority in the EEA.

California Residents

For more information regarding CCPA/CPRA for California residents, refer to the [CCPA/CPRA Privacy Notice](#) provided on the Safeguard Website.

EU-US Data Privacy Framework, UK Extension to the EU-U.S. DPF, and Swiss-U.S. Data Privacy Framework

Participation in the EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, and Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. We have certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF, and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. We have certified to the U.S. Department of Commerce that we adhere to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

Federal Trade Commission Enforcement

The Federal Trade Commission has jurisdiction over Us for compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Internal Complaint Recourse Mechanism

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, We commit to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, and UK, and Swiss individuals with inquiries or complaints regarding

our handling of personal data received in reliance on the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Us using the contact information provided in the Contact Us section.

Independent Complaint Recourse Mechanism

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, We commit to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

Binding Arbitration

For complaints regarding EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) compliance not resolved by any of the other EU-U.S. Data Privacy Framework (EU-U.S. DPF) mechanisms, You have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website: <https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction>

Onward Transfer Liability

We are responsible for the processing of the personal data We receive, under the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), and subsequent transfers to a third party acting as an agent on Our behalf. We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) principles with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF. and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF for all onward transfers of personal data including the onward transfer liability provisions.

Changes to this Privacy Policy

We may update Our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

Last updated: June 4, 2026

We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the "Last updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Privacy Policy Locations

1. This Privacy Policy is publicly available at: www.safeguardequipment.com/privacy-policy-apps/
2. The Privacy Policy for Our website is publicly available at: <https://www.safeguardequipment.com/wp-content/uploads/2024/05/Website-Privacy-Policy.pdf>

Contact Us

If you have any questions about this Privacy Policy, You can contact us:

- By email: support@safeguardequipment.com
- By visiting this page on our website: <https://www.safeguardequipment.com/contact-us>
- By phone number: 1.208.773.9263