Privacy Statement

This Privacy Statement for Sentry Products and Services ("Privacy Statement") describes information that Sentry collects, uses, shares, and stores, including personal information (i.e., information that personally identifies you, such as your name, email address or billing information, or other data that can be reasonably used to infer this information).

This document focuses on information related to the operation of Sentry products and services, including Sentry Smart Alerts. In this Privacy Statement, the expression "Sentry Products" also includes our Subscription Services as defined in our Terms of Service.

Our Pledge:

1. We will be transparent about the different types of information we collect and how we use them.
2. We will ask your permission before sharing your personal information with third parties for purposes other than at your request or to provide Sentry's Products, and to do so only when we think they will provide you with a welcome additional service.
3. We will use best-in-class data security tools to keep your data safe and protect the Sentry Products from unauthorized access.

Your Permission: Permission for data collection and processing. By using Sentry Products, you agree to allow us to collect and process information as described in this Privacy Statement.

International data transfers. Your personal information may be collected, processed and stored by Sentry in the United States and other countries where our servers reside. Please be aware that the privacy protections and legal requirements, including the rights of authorities to access your personal information, in some of these countries may not be equivalent to those in your country. If you are using Sentry Products in the European Economic Area or other regions with laws governing data collection and use that may differ from United States law, you agree to the transfer of your personal data to the United States and other countries where Sentry operates. We have provided you with more information below as to how we protect your personal data when it is transferred internationally: How does Sentry protect my personal information when it is transferred internationally?

What information does Sentry Smart Alerts collect?

Sentry collects the following:

- Setup information you provide
- Video and audio signals and data
- Facial recognition data to enable Familiar Face Alerts feature
- Technical information from the device
- Shared content

Information input during setup: When you install Sentry Smart Alerts, you'll be asked for certain basic information like your camera name, camera description, home address, ZIP/postal code, as well as where in your home you're installing Sentry Cam. This information is used to personalize your experience – for example, to tell you which device is triggering a notification.

Video and audio signals and data: When you enable Sentry Smart Alerts, we store and process images or video recordings from the device caused by motion alerts. The camera manufacturer determines whether an image or video clip is sent to Sentry for processing. This decision is not in the hands of Sentry. In order to improve your experience over time and help troubleshoot any problem you may encounter, we store the images or video clips provided by your camera manufacturer.

Computer vision to enable human detection: Sentry uses computer vision technology for the purpose of notifying you of human activity. Depending on where you live, you may need to get explicit consent to scan people visiting your home.

What additional information does Sentry collect and store when a user connects a Sentry Product to the Internet or creates an account?

Email Addresses: When you create a Sentry account, we collect and store your email address. From that point forward, your email address is used for communications from Sentry. In addition,

Basic Profile Information: Your account allows you to provide certain basic profile information like your name. Names may be shown to others in connection with the Services.

How does Sentry use the information it collects?

We use this information to provide, develop and improve Sentry Products and services, including to make assessments about products. We may use your contact details to send you this information, or to ask you to participate in surveys about your Sentry use, and to send you other communications from Sentry.

We may also use this information in a non-identified form for research purposes and to help us make product decisions. For example, we use aggregated user information about number of suppressed alerts to determine the effectiveness of our product.

We use industry-standard methods to keep this information safe and secure while it is transmitted over your home network and through the Internet to our servers. Depending on your location and type of data, Sentry may process your personal information on servers that are not in your home country.

In general for purposes of applicable law (e.g., GDPR), Sentry is a controller of the information collected in connection with the Products and Services.

Our legal bases for processing information

If European data protection law applies to the processing of your information, we process your information for the purposes described in this Privacy Statement, based on the following legal grounds:

When we're providing a product or service

We process your data to provide and support a product or service you've asked for under a contract, including but not limited to delivering our Terms of Service.

When we're pursuing legitimate interests

We process your information for our legitimate interests while applying appropriate safeguards that protect your privacy. This means we process your information for things like:

- offering and improving Sentry Products and services
- developing new products and features

- understanding how people use our products and services
- performing research that improves our services for our users and benefits the public
- sending you direct marketing and other communications from Sentry
- protecting against harm to the rights, property, and safety of Sentry, our users, and the public
- detecting, preventing or otherwise addressing fraud, abuse, security or technical issues with our services
- maintaining and improving the integrity of our computing systems, and protecting our users' data security
- enforcing legal claims, including investigation of potential violations of applicable Terms of Service

When we're complying with legal obligations

We process your data when we have a legal obligation to do so, for example, if we're responding to a legal process or an enforceable governmental request.

With your consent We ask for your consent to process your information for certain specific purposes and give you the right to withdraw that consent at anytime.

In what circumstances does Sentry share my information?

Under no circumstance do we share personal information for any commercial or marketing purpose unrelated to the activation and delivery of Sentry Products and services without asking you first. Period. We do not rent or sell our customer lists. The following are the limited situations where we may share personal information:

- With your permission: We may share personal information when we have your permission. One example of this would be if you invite another user to access the Products on your account as an additional authorized user. Another example is if you sign up for programs offered by our partners (e.g., video surveillance partners); if you do this, we may share certain information with the partner. This could include things like images where human activity was found.
- For external processing: We have vendors, service providers, and technicians who help with some of our processing and storage, including helping to answer your questions. They may also assist with monitoring our servers for technical problems. These technicians (as well as Sentry employees) can

access certain information about you or your account in line with this work but these technicians are not allowed to use this data for Sentry purposes. We also have strict policies and technical barriers in place to prevent unauthorized employee access to video data.

- As part of business transitions: Upon the sale or transfer of the company and/or all or part of its assets, your personal information may be among the items sold or transferred. We will request a purchaser to treat our data under the privacy statement in place at the time of its collection.
- For legal reasons: We will share personal information with third parties if we have a good faith belief that access, use, preservation or disclosure of the information is reasonably necessary to (i) meet any applicable law, regulation, legal process or enforceable government request; (ii) enforce Sentry policies or contracts, including investigation of potential violations; (iii) detect, prevent or otherwise address fraud, security or technical issues; (iv) protect against harm to the rights, property or safety of Sentry, our users or the public as required or permitted by law.

We may share non-personal information (for example, aggregated or anonymized customer data) publicly. For example, as we roll out our neighborhood watch functionality, videos associated with a burglar at one house could be leveraged to identify future suspicious behavior in the neighborhood. We may publish trends about energy use or elevated carbon monoxide levels in the home. This information may also be shared with other users to help them better understand their energy usage compared to others in the Sentry community, raise awareness about safety issues, or help us generally improve our system. We may also share non-personal information with our partners, for example, if they are interested in providing demand-response services or other incentive programs. We take steps to keep this non-personal information from being associated with you and we require our partners to do the same.

What choices do I have and how can I delete my personal information?

Sentry generally stores your personal information on Sentry's servers until you delete or edit it, or for as long as you remain a Sentry customer in order to provide you with Sentry Products. In addition, Sentry may store your personal information to

resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements and comply with applicable laws.

You can access, amend or delete your personal information from Sentry's servers through the controls in your account. Sentry customers can also request their Sentry data by emailing Support@smarthomesentry.com .

How does Sentry protect my personal information when it is transferred internationally?

When we transfer personal data from the European Economic Area and Switzerland to other countries, including to the United States, we use a variety of legal mechanisms to help ensure your data is appropriately protected. Sentry Inc. complies with the EU-US Privacy Shield Framework and the Swiss–US Privacy Shield Framework (the "Privacy Shield") regarding the collection, use, sharing, and retention of personal information from the European Economic Area and Switzerland to the United States, as described in our Privacy Shield certification. Sentry adheres to the principles contained in the Privacy Shield (the "Principles").

As part of our participation in Privacy Shield, if you have a dispute with us about our adherence to the Principles, you may refer a complaint to your local data protection authority and we will work with them to resolve your concern. (In certain circumstances, the Privacy Shield Framework provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the Privacy Shield Principles.) If you have a Privacy Shield-related complaint, please contact us at support@smarthomesentry.com.

Privacy Shield participants are subject to the investigatory and enforcement powers of the US Federal Trade Commission and other authorized statutory bodies.

We may share, as described in this Privacy Statement, information with our affiliates and subsidiaries, and third parties. We may disclose information in response to legal process and lawful requests by public authorities in the United States and other countries for the purposes of law enforcement and national security.

Minors.

Only individuals aged 18 and older are permitted to act as Owners of Sentry Accounts. Authorised Users must be over the age of 13 (or equivalent minimum age in the jurisdiction where they reside) and may use the Products and Services under the supervision of a parent or legal guardian and only if they agree to be bound by

these Terms on your behalf. Sentry Products and Services do not knowingly collect or store any personal information from anyone under the age of 13.

Can the Privacy Statement be changed?

Please note that this Privacy Statement may change from time to time. We will provide notice of any changes on the website or by contacting you.

How can I contact Sentry?

For users in the United States: Smart Home Sentry, 440 N Wolfe Rd #254, Sunnyvale, CA 94085

If you have any questions, you may submit an inquiry to our support team by emailing support@smarthomesentry.com.