# EUFY PRIVACY NOTICE

Last Updated: November 30th, 2023

This Privacy Notice is issued by Anker Innovations Technology Co., Ltd and its affiliates (together, “Anker”, “we”, “us” and “our”) and is addressed to individuals outside our organization with whom we interact, including customers, visitors to our Sites, users of our Applications, recipients of any of our other products or services (together, “you”). Defined terms used in this Privacy Notice are explained in Section (16) below.

This Privacy Notice applies to all of Anker’s brands, including Anker, AnkerMake, AnkerWork, Eufy, Mach, Nebula, Roav, and SoundCore, as well as any specific device, website, or application that references or links to this Privacy Notice.

We may update this Privacy Notice to reflect changes to our information practices. If we make any material changes, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on Anker's Application or Site you used prior to the change becoming effective. All changes shall be effective from the date of publication unless otherwise provided. We encourage you to periodically review this page for the latest information on our privacy practices.

You may also have certain rights regarding the information we collect about you. Specifically, the rights of Data Subjects under the GDPR are explained in Section (9) below. Similarly, U.S. residents in general and California Residents in particular may find information on their rights as a consumer in Section (15) below.

List of Contents

## 1. Collection of Personal Data

Depending on how you use our Sites, Applications, products or services, we may collect or obtain Personal Data about you from the following sources:

Data you provide to us: We obtain Personal Data when you provide those data to us (e.g., when you register an account with us; where you contact us via email, telephone, or by any other means; or when you provide us with your business card).
Account creation details: We collect or obtain Personal Data when you register or create an account to use any of our Sites or Applications.
Relationship data: We collect or obtain Personal Data in the ordinary course of our relationship with you (e.g., when we provide a service to you).
Site or Application data: We collect or obtain Personal Data when you visit or use any of our Sites or Applications, or use any features or resources available on or through our Sites or Applications.
Content and advertising information: If you interact with any third-party content or advertising on our Sites and/ or Applications (including third-party plugins and cookies) we allow the relevant third party providers to collect your Personal Data. In exchange, we receive Personal Data from the relevant third-party provider relating to your interaction with that content or advertising.
Data you make public: We may collect the content you publish, or otherwise manifestly made public about us through our Apps and platforms, your social media, or any other publicly available platforms.
Third party information: We collect or obtain Personal Data from third parties who provide it to us (e.g., single sign-on providers and other authentication services you use to connect to our services, third-party providers of integrated services, your employer, other Anker customers, business partners, Processors, and law enforcement authorities).
Data automatically collected: We and our third-party partners automatically collect information you provide to us and information about how you access and use our Sites, Applications, products or other services when you visit our services, read our emails, or otherwise engage with us. We typically collect this information through a variety of tracking technologies, including (i) cookies or small data files that are stored on an individual's computer and (ii) other, related technologies, such as web beacons, pixels, embedded scripts, mobile SDKs, location-identifying technologies and logging technologies (collectively, "tracking technologies") and we may use third-party partners or technologies to collect this information. Information we collect automatically about you may be combined with other personal information we collect directly from you or receive from other sources.
For more information on which data we collect, please also refer to the table in Annex 1.

2. Creation of Personal Data

We also Process and retain Personal Data about you in certain circumstances, such as records of your interactions with us, details of your past interactions with us, and inferences or predictions about your characteristics or interests. We may also link Personal Data collected from any of our Sites, Applications, products, or services, including where those data are collected from different devices.

3. Categories of Personal Data We Collect and Process

When you first register for an Anker account, we may collect the following categories of Personal Data about you: username and password, email addresses and/or phone numbers. After successfully creating your Anker account, you can use it to log in across Anker's various Sites and Applications without needing to create an account for each specific Site or Application.

When using our Sites, Applications, products, or services, we may also collect and/or process the following categories of Personal Data about you:

Contact information: including first and last name, preferred name, phone number, email address, mailing address.
Account information: including first and last name, date of birth / age, alias, user ID, country, language preferences, email address, phone number, employer, avatar, account credentials or one-time passcodes, single sign-on authentication tokens, loyalty and incentive program credits / rewards, and the products or services you purchased or have otherwise used.
Transaction information: including records of purchases and prices, consignee first and last name, shipping address and contact information, shipment tracking details, details of returns, and warranty details.
Payment details: such as invoice / payment records, payment amount, payment date, billing address, payment method. Please note that we use third-party payment providers, including Shop Pay, Stripe, Amazon Pay, PayPal, and Google Pay, to process payments made to us. We do not receive or retain any personally identifiable financial information such as payment card numbers; rather, all such information is provided directly by you to our third-party payment providers. The payment provider's use of your personal data is governed by their privacy policy.
Information collected from third-party authentication services or other third-party accounts you link to our services: some of our Sites, Applications, products, or services may allow you to log in through a third-party social network or authentication service, such as Amazon, Apple, Google, and Facebook. When you use these single sign-on services to access our Sites, Applications, products, or services, we do not receive your login credentials for the relevant third-party service. Instead, we receive tokens from the single sign-on service to help identify you in our system (such as by your username) and confirm you successfully authenticated with the single sign-on services. In addition to authenticating your identity, these services will, in most cases, provide you the option to share certain Personal Data with us, which could include your name, email address, address book, friend list and other contacts, or other information in your public profile (e.g., profile picture, age range, gender, language, country). The data we receive is dependent on that third party's policies and your privacy settings on that third-party site.
Product-specific information: we collect or otherwise facilitate the processing of the following types of information in connection with certain of our Sites, Applications, products and services, such as customer content, entertainment-related service information, home-related

services information, car-related services information, baby-related services information, health-related services information, biometric services information. The specific information collected may vary depending on the product you use. For more information on which product-specific data we collect, please refer to Annex 2.
Information about your device and network: including the device type, operating system, IP address, browser type, user ID and UUID, or your network (including, for example, a persistent device identifier or advertising ID).
Information about the way individuals use our services and interact with us: including the site from which you came, the site to which you are going when you leave our services, how frequently you access our services, whether you open emails or click the links contained in emails, whether you access our services from multiple devices, and other browsing behavior and actions you take on our services (such as the pages you visit, the content you view, the communications you have through our services, and the content, links and ads you interact with). We employ third-party technologies designed to allow us to collect detailed information about browsing behavior and actions that individuals take on our services, which may record your actions down to the level of mouse movements, scrolling, clicks, and keystroke activity on our services.
Event, contest, promotion, and survey information: including information provided when you sign up for an event, enter a contest or promotion, complete a survey or submit a testimonial.
Feedback and support information: including the contents of custom messages sent through the forms, email addresses, photographs or videos you submitted, or other contact information we make available to customers, as well as recordings of calls with us (where permitted by law).
To collect some of the Personal Data set forth above, we may need to request permission to access such Personal Data through your mobile device. You are in control of the permissions you grant us, and you may change your permission settings at any time in the setting dashboard of your device. Note that revoking permissions may affect the provision and performance of our Sites, Applications, products, and services.

Purposes of Processing
We may use the Personal Data we collect for the following purposes:

Fulfill our contractual obligations, to deliver the products and services you have requested, including facilitating your messages to other users or groups and for account and contract management (including customer support);
Communicate with individuals, including via email, text message, social media and/or telephone and video calls;
Review our business performance;
Market our products and services to businesses and individuals, including through email, direct mail, phone, text message or online advertising. This may include targeted advertising and retargeting;
Administer, improve and personalize our products and services, including by recognizing an individual and remembering their information when they return to our Services and analyzing our customer base;
Process payment for our services;
Conduct market research;
Opportunity tracking, conversion and lead generation;
Test, enhance, update and monitor the products and services, or diagnose or fix technology problems;
Help maintain the safety, security and integrity of our property, products and services, technology assets and business;

Enforce our contractual rights, including without limitation, and to the extent applicable, the Anker Terms of Service, General Terms and Conditions, Software Terms of Service; any addenda thereto or other applicable terms.
Resolve disputes, carry out our obligations and enforce our rights, and protect our business interests and the interests and rights of third parties;
Prevent, investigate or provide notice of fraud or unlawful or criminal activity; and
Enable functions of our Sites or Applications, including creating profiles, using our online-shop and rating products.
Display certain functionalities of our Sites or Apps in connection with third parties, such as the trusted shop banner, shipment tracking or product videos;
Enable you to use certain functionalities of our products;
Offer discounts to certain groups, such as students;
Decide whether to enter into a business partnership, such as the affiliate program or the merchant program;
Comply with legal obligations.
You can find more information about how we Process your Personal Data in the table in Annex 1.

5. Legal basis for Processing

The purposes for which we Process Personal Data, if you are Subject to the GDPR, and the legal bases on which we perform such Processing, are as follows:

Perform our contractual services or prior to entering into a contract with you: If you order products or services from us or if you contact us to request our products or services, we use your Personal Data to provide you with these products or services, including for account and contract management, to facilitate user benefits and services, including customer support and process payment for our products and services or with information that may be relevant for you to decide on whether you want to order our products and services;
Justified by our legitimate interests: The usage of your Personal Data may also be necessary for our own business interests. For example, we may use some of your Personal Data to update and monitor the services, or diagnose or fix technology problems; help maintain the safety, security and integrity of our property and services, technology assets and business; enforce our terms, resolve disputes, carry out our obligations and enforce our rights, and protect our business interests and the interests and rights of third parties; and prevent, investigate or provide notice of fraud or unlawful or criminal activity.
Consent: In some cases, we may ask you to grant us separate consent to use your Personal Data. In this case, you can revoke your consent at any time with effect for the future.
Compliance with legal obligations: We are obligated to collect or retain certain Personal Data because of legal requirements, for example, tax or commercial laws, or we may be required by law enforcement to provide Personal Data on request.
You can find more information on the legal basis in the table in Annex 1.

Disclosure of Personal Data
We may also share, transmit, disclose, grant access to, make available, and provide Personal Data with and to third parties, as described below.

Anker Affiliates: We share Personal Data amongst the legal entities that make up the Anker group, for legitimate business purposes and the operation of our Sites, Applications, products, and services for you, in accordance with applicable law. These legal entities may use your Personal Data in the manner described in this Privacy Notice.

Legal Obligations and Rights: We may disclose Personal Data to third parties, such as legal advisors and law enforcement agencies, regulators, other authorities and other third parties for legal reasons if we reasonably believe that such action is necessary:
- in connection with the establishment, exercise, or defense of legal claims;

- to comply with laws or to respond to lawful requests and legal process;

- to protect our rights and property and the rights, personal safety and property of others, including to enforce our agreements and policies;

- to detect, suppress, or prevent fraud or other criminal activity; or

- as otherwise required by applicable law.

Third party Processors: We share Personal Data with third party contractors and service providers subject to reasonable confidentiality terms. The services provided on our behalf by such third-party contractors and service providers may include email service providers; marketing/advertising service providers; call service providers; video shopping support and showroom service providers; text message service providers; venue operators; payment services providers; shipping companies; and postal carriers, subject to the requirements noted below in this Section (6). These Processors support us in processing the types of Personal Data described above in Sections (1), (2), and (3), and for the purposes described in Section (4). They only are authorized to process that information as necessary and as directed by us;
Advertising networks: To efficiently market our products and services to you, we may share Personal Data with so called advertising networks. These parties may collect information automatically from your browser or device when you visit our websites and other services through the use of cookies and similar technologies. This information is used to provide and inform targeted advertising, as well as to provide advertising-related services such as reporting, attribution, analytics, and market research. For more information about how these technologies work and certain choices you may have in relation to these technologies, please refer to Section (13) below;
Business and marketing partners: We may also disclose Personal Data with other business and marketing partners with whom we jointly offer products or services or who are part of our partner program. We may obtain your consent where required by applicable law.
Third party services integrated in our services (for instance, third party voice-assisted technologies may receive information you choose to share directly with them);
Individuals you choose, for example through our device-sharing function; we recommend you share information with only people you trust;
Independent advisors: We may disclose Personal Data to our independent advisors such as accountants, auditors, consultants, lawyers, and other outside professional advisors to Anker, subject to binding contractual obligations of confidentiality;
Corporate Transactions: if Anker is involved in a corporate business transaction, such as a merger, acquisition, or sale of all or a portion of our company assets, we may disclose Personal Data to a third party during negotiation of, in connection with or as an asset in such a corporate business transaction. If Anker completes such a corporate business transaction, you will be notified via email and/or a prominent notice on our website, of any change in ownership, uses of your Personal Data, and choices you may have regarding your Personal Data. Personal Data may also be disclosed in the event of insolvency, bankruptcy or receivership; and
We may also disclose your Personal Data to any other third party or publicly with your prior consent or direction.
If we engage a third-party Processor to Process your Personal Data, the Processor will be

subject to binding contractual obligations to: (i) only Process the Personal Data in accordance with our prior written instructions; and (ii) use measures to protect the confidentiality and security of the Personal Data; together with any additional requirements under applicable law. Please note that third parties and business partners may process your Personal Data in accordance with their own privacy policies and terms of service.

7. International Transfer of Personal Data

Because of the international nature of our business, we transfer Personal Data within the Anker group, and to third parties as noted in Section (6) above, in connection with the purposes set out in this

Notice. For this reason, we transfer Personal Data to other countries that may have different laws and data protection compliance requirements than those that apply in the country in which you are located, including China, the EEA, the UK, and the US.

In the event of a transfer by Anker, we ensure that international transfers of your Personal Data are made pursuant to appropriate safeguards, such as:

Ensuring that the Personal Data is only transferred to countries recognized as Adequate Jurisdictions. The current adequacy decisions can be found here. There is currently no adequacy decision for the United States and China; or
the transfer is made pursuant to appropriate safeguards, such as Standard Contractual Clauses adopted by the European Commission or UK Secretary of State (as applicable) in connection with appropriate supplementary measures. The decision and the template text of these Standard Contractual Clauses can be found here;
If you wish to enquire further about these safeguards, including the specific contracts entered into, used, please contact us using the details set out under Section (14) of this Privacy Notice.

Please note that when you transfer any Personal Data directly to any Anker entity established outside the UK, Switzerland, or the EEA (as applicable), this is considered a direct collection, to which the safeguards mentioned in this Section (7) may not apply. We will nevertheless Process your Personal Data, from the point at which we receive those data, in accordance with the provisions of this Policy.

Data Retention
We have implemented processes designed to ensure that your Personal Data are only processed for the minimum period necessary for the purposes set out in this Privacy Notice. The criteria for determining the duration for which we will retain your Personal Data are as follows:

we will retain Personal Data in a form that permits identification only for as long as:
(a) we maintain an ongoing relationship with you (e.g., where you are a user of our services, or you are lawfully included in our mailing list and have not unsubscribed); or

(b) your Personal Data are necessary in connection with the lawful purposes set out in this Privacy Notice, for which we have a valid legal basis (e.g., where your Personal Data are included in a contract between you and us, and we have a legitimate interest in Processing those Personal Data for the purposes of operating our business and fulfilling our obligations

under that contract; or where we have a legal obligation to retain your Personal Data),

the duration of:
(a) any applicable limitation period under applicable law (i.e., either any statutory retention periods as required by the law of the European Union or a member state of the EEA, or any period during which any person could bring a legal claim against us in connection with your Personal Data, or to which your Personal Data are relevant); and

(b) an additional two (2) month period following the end of such applicable limitation period (so that, if a person brings a claim at the end of the limitation period, we are still afforded a reasonable amount of time in which to identify any Personal Data that are relevant to that claim),

in addition, if any relevant legal claims are brought, we continue to Process Personal Data for such additional periods as are necessary in connection with that claim.
During the periods noted in paragraphs (2)(a) and (2)(b) above, we will restrict our Processing of your Personal Data to storage of, and maintaining the security of, those data, except to the extent that those data need to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once the periods in paragraphs (1), (2) and (3) above, each to the extent applicable, have concluded, we will either:

permanently delete or destroy the Relevant Personal Data; or
anonymize or deidentify the Relevant Personal Data.
Your Privacy Rights
Subject to applicable law, you may have the following rights regarding the Processing of your Relevant Personal Data:

the right not to provide your Personal Data to us (however, please note that we may be unable to provide you with the full benefit of our services, if you do not provide us with your Personal Data – e.g., we might not be able to process your requests without the necessary details);
the right to request access to, or copies of, your Relevant Personal Data, together with additional information, such as information regarding the nature, Processing and disclosure of those Relevant Personal Data;
the right to request rectification of any inaccuracies or incompleteness in your Relevant Personal Data;
the right to request, on legitimate grounds:
erasure of your Relevant Personal Data without undue delay; or
restriction of Processing of your Relevant Personal Data (limiting the purposes for which we Process your Personal Data);;
the right to have certain Relevant Personal Data transferred to another Controller, in a structured, commonly used and machine-readable format, to the extent applicable;
the right to request the deletion or removal of your Relevant Personal Data where there is no other legal basis for us to keep using it. Please note that we may not be able to immediately remove the information from the backup system due to applicable laws and regulations or technological limitations. If this is the case, we will isolate your Relevant Personal Data from further processing until the backup can be deleted or be anonymized / deidentified.
where we Process your Relevant Personal Data on the basis of your consent, the right to withdraw that consent (noting that such withdrawal does not affect the lawfulness of any Processing performed prior to the date on which we receive notice of such withdrawal, and

does not prevent the Processing of your Personal Data in reliance upon any other available legal bases).
Under the GDPR , you may also have the following additional rights regarding the Processing of your Relevant Personal Data:

the right to object, on grounds relating to your particular situation, to the Processing of your Relevant Personal Data by us or on our behalf, where such processing is based on Articles 6(1)(e) (public interest) or 6(1)(f) (legitimate interests) of the GDPR;
the right to object to the Processing of your Relevant Personal Data by us or on our behalf for direct marketing purposes； and
the right to lodge complaints regarding the Processing of your Relevant Personal Data with a competent Data Protection Authority (in particular, the UK Information Commissioner's Office, or the Data Protection Authority of the EU Member State in which you live, or in which you work, or in which the alleged infringement occurred. If you live in Germany, the relevant Data Protection Authority is the "Bayerisches Landesamt für Datenschutzaufsicht", Promenade 18, 91522 Ansbach). However, we encourage you to first contact us so that we can together solve any concerns you may have.
This does not affect your statutory rights.

To exercise one or more of these rights, or to ask a question about these rights or any other provision of this Privacy Notice, or about our Processing of your Personal Data, please use the contact details provided in Section (14) below. Please note that:

in some cases it will be necessary to provide evidence of your identity before we can give effect to these rights; and
where your request requires the establishment of additional facts (e.g., a determination of whether any Processing is non-compliant with applicable law) we will investigate your request reasonably promptly, before deciding what action to take.
Direct Marketing
We Process Personal Data to contact you via email, telephone, direct mail, or other communication formats to provide you with information regarding Sites, Applications, products, and services that may be of interest to you. If we provide Sites, Applications, products, or services to you, we may send or display information to you regarding our Sites, Applications, products, or services, upcoming promotions and other information that may be of interest to you, including by using the contact details that you have provided to us, or any other appropriate means, subject always to obtaining your prior opt-in consent to the extent required under applicable law.

You may unsubscribe from specific promotional email campaigns at any time by simply clicking on the unsubscribe link included in every promotional electronic communication we send, or you may unsubscribe from all Anker promotional emails by unsubscribing online at https://mulpass.anker.com/unsubscribe/?app=ankeruk. After you unsubscribe, we will not send you further promotional emails in connection with the email campaigns you have unsubscribed from, but in some circumstances we will continue to contact you to the extent necessary for the purposes of providing any Sites, Applications, products, or services you have requested or in connection with any email campaigns to which you remain subscribed.

You may unsubscribe from specific promotional text campaigns at any time by replying STOP via text message to any of the promotional text communications we send in relation to the specific campaign you would like to opt out from. After you unsubscribe, we will not send you further promotional text messages in connection with the text campaigns you have

unsubscribed from, but in some circumstances, we will continue to contact you to the extent necessary for the purposes of providing any Sites, Applications, products, or services you have requested or in connection with any text campaigns to which you remain subscribed.

11. Details of Controllers

For the purposes of this Privacy Notice, the relevant joint Controllers are:

Controller entity

Contact details

Anker Technology (UK) Ltd.

205 Kings Road, Fairgate House

Suite B

B11 2AA Birmingham

+49 (0) 69 9579 7960

Anker Innovations Technology Co., Ltd

Room701, Bldg 7, Zhongdian Software Park, 39 Jianshan Road, Hi-tech Zone, Changsha City, Hunan Province, China

Shenzhen Oceanwing Smart Innovations Technology Co., Ltd

B701-705, Jianxing Tech Bldg, Xinxing industrial park, 3151 Shahe West Road, Nanshan District, Shenzhen City

Fantasia Trading LLC

5350 Ontario Mills Pkwy, Suite 100, Ontario, CA 91764 Delaware

For general enquiries, or to exercise any of the rights set out in this Privacy Notice, please contact support@anker.com.

With respect to the Processing of Personal Data through our Site and Applications, the entities mentioned above can both access your Personal Data and decide on the means and purposes of the Processing. Therefore, they are jointly responsible for the Processing of your Personal Data.

Notwithstanding your ability to contact Anker, at support@anker.com, for all data protection related matters, Anker Innovations Technology Co., Ltd. offers to take care of all matters relating to your Personal Data. To this end, you may send any concerns, including requests to exercise your rights under Section (9) of this Privacy Notice, to Anker Innovations Technology Co., Ltd. at the contact information provided above or in Section (17).

12. Business Information and Links to Other Websites

Business information – In the course of using our Sites, Applications, products, and services, we may ask you to provide business information related to the company where you work. Business information may include information about your company's practices, policies, processes, and supporting documentation. This business information is stored on Anker systems, and we use it to provide the solutions you have contracted us to provide and in accordance with the terms and conditions set forth in agreements between Anker and your company,

Links to other websites – This Privacy Notice applies only to Anker practices, technologies, and services. Our online properties may include links to websites and online services that are operated by other companies not under the control or direction of Anker. If you provide or submit Personal Data to those websites or online services, the privacy policies on those websites or online services apply to your Personal Data. We encourage you to carefully read the privacy policies of any website you visit.

13. Cookies, Analytics and Tailored Advertising

Anker and its third-party partners and providers use cookies and similar technologies to automatically collect certain Personal Data when you visit or interact with our Sites and services to enhance navigation, analyze trends, administer the Sites, track users' movements around the Sites, gather demographic information about our user base as a whole, and assist with our marketing efforts and customer service. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our Sites and services.

Our Sites provide you the ability to adjust your preferences regarding our use of cookies and similar technologies by clicking the "Cookie Settings" link in the footer of our Sites. These cookie preference manager tools are website, device, and browser specific, so you will need to change your preferences on each device and browser you use when interacting with the specific Site you are visiting. You can also stop all collection of information via our web services by not using our Sites and services.

You may also be able to utilize third-party tools and features to further restrict our use of cookies and similar technologies. For example, cookies may generally be disabled or removed by tools available as part of most commercial browsers, and in some instances blocked in the future by selecting certain settings. Browsers offer different functionalities and options, so you may need to set them separately. In addition, you may be able to exercise specific privacy choices, such as enabling or disabling certain location-based services, by adjusting the permissions in your mobile device or internet browser. You may also exercise choice regarding the use of cookies from Google Analytics by going to https://tools.google.com/dlpage/gaoptout to download the Google Analytics Opt-out Browser Add-on. For information on how Google Analytics collects and processes data, as well as how you can control information sent to Google, review Google's website here: www.google.com/policies/privacy/partners/.

You may also opt-out of targeted advertising by companies that participate in the Digital Advertising Alliance ("DAA") AdChoices Program by visting optout.aboutads.info. For more information on the DAA AdChoices Program, please visit www.youradchoices.com. In addition, the Network Advertising Initiative ("NAI") has developed a tool that allows consumers to opt out of certain tailored advertising delivered by NAI members' advertising networks. To learn more

about opting out of such targeted advertising or to use the NAI tool, see https://optout.networkadvertising.org/.

Contact Us

If you have questions or concerns with respect to our Privacy Notice or privacy practices, you may contact us at support@anker.com or DPO@anker.com.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

ADDITIONAL UNITED STATES PRIVACY DISCLOSURES

These disclosures supplement the information contained in the main body of our Privacy Notice by providing additional information about our Personal Data processing practices relating to individual residents of certain states in the United States. For a detailed description of how we collect, use, disclose, and otherwise process Personal Data, please read the main body of our Privacy Notice.

Nevada Residents

If you are a resident of the state of Nevada in the United States, you have the right to opt out of the sale of certain of your Personal Data. Although we do not currently sell covered data of Nevada residents (as defined under Nevada law), you may submit a request to opt-out of the sale of your Personal Data by emailing us at support@anker.com.

California, Colorado, Connecticut, Utah, and Virginia Residents

If you are a resident of the state of California, Colorado, Connecticut, Utah, or Virginia in the United States the following supplementary disclosures apply to you.

Collection and Use of Personal Data

Personal Data

As described in more detail in Section (3) above, we collect the following categories of Personal Data:

Identifiers, such as first and last name, preferred name, phone number, email address, unique personal identifiers, and online identifiers.
Customer records, such as contact information, address book information, and account information.
Protected classification characteristics, such as age, gender, and health status.
Commercial information, such as records of purchases and prices, shipping address and contact information, and details of returns, and consumer histories and tendencies.
Biometric information, such as facial, fingerprint or other biometric recognition technology results processed and maintained solely on the user's device (see below for more detail).
Internet / network information, such as the device type, manufacturer, and model, operating system, IP address, browser type, Internet service provider, and unique identifiers associated with you, your device, or your network.
Geolocation data, including general geographic location, as well as more precise geolocation when you grant us access through your device settings (see below for more detail).

Audio, electronic, visual, thermal, olfactory, or similar information, including voice prompts / recordings and security /service images and video.
Professional / employment information, such as employer and job title.
Sensitive personal data, such as account credentials, biometric information, health data, and precise geolocation (as further described below).
Other Personal Data, such as your communication preferences, entertainment preferences, home configuration (for our home-related services), participation in our loyalty and incentive programs, and any other Personal Data you choose to share in custom messages sent through the forms, email addresses, or other contact information we make available to customers.
Inferences, including consumer preferences, predispositions, and characteristics.
As described in Section (1) above, we collect this Personal Data directly from you, automatically when you interact with our Sites, Applications, products, or other services, from third parties, and from public third-party platforms such as social media websites.

We collect Personal Data from and about you for a variety of purposes. For example, we use Personal Data to communicate with you; to facilitate, process, and fulfill orders you place with us or the services you request; to conduct surveys, sweepstakes, contests and other promotions; to analyze and improve the use of our Sites and Applications; to deliver marketing communications and personalized and non-personalized advertising; and to facilitate our customer services. For more information about our use of Personal Data, please refer to Section (4) above.

Sensitive Personal Data

The following Personal Data elements we collect may be classified as “sensitive” under certain privacy laws (“Sensitive Personal Data”):

Account credentials.
Payment card information (collected and processed solely by our third-party payment providers; Anker does not have access to this data).
Biometric information (collected and processed solely on the user’s device; Anker does not have access to this data).
Health metrics, including sleep patterns, movements, heart rate, height, weight, and body mass index .
Precise geolocation data.
We only use or disclose Sensitive Personal Data where reasonably necessary and proportionate for the purposes of performing services you have requested, verifying and improving the services we provide, detecting security incidents, fraud and other illegal actions, ensuring the physical safety of natural persons, performing services on behalf of the business, or short-term transient use. We only collect and process Sensitive Personal Data without the purpose of inferring characteristics about the relevant individual, and we do not sell Sensitive Personal Data or process or otherwise share Sensitive Personal Data for the purpose of targeted advertising (as further described below).

However, depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to limit, or withdraw your consent for, our processing of Sensitive Personal Data (as described in the Your Additional U.S. Privacy Choices section below).

Deidentified Information

We may at times receive, or process Personal Data to create, deidentified information that can

no longer reasonably be used to infer information about, or otherwise be linked to, a particular individual or household. Where we maintain deidentified information, we will maintain and use the information in deidentified form and not attempt to reidentify the information except as required or permitted by law.

Personal Data Disclosures, Sales, and Targeted Advertising

We may disclose the categories of Personal Data above to the following categories of third parties: the entities that make up the Anker group, Processors, ad networks and advertising partners, business and marketing partners, third-party providers with services integrating with our services, individuals you choose to share Personal Data with, and certain third parties where you have provided consent or where otherwise required or permitted by law. Please see Section (6) for more detail.

Our disclosure or making available of identifiers, customer records, commercial information, internet / network information, and inferences to ad networks and advertising partners may qualify as the sale of Personal Data or the sharing or processing of Personal Data for the purpose of displaying advertisements that are selected based on Personal Data obtained or inferred over time from an individual's activities across businesses or distinctly-branded websites, applications, or other services (otherwise known as "targeted advertising" or "cross-context behavioral advertising") under certain privacy laws.

Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to limit or opt-out of the sale of Personal Data or the processing of Personal Data for purposes of targeted advertising (as described in the Your Additional U.S. Privacy Choices section below).

Please note we do not sell the Personal Data of individuals we know to be less than 16 years of age or share such information for targeted advertising purposes. In addition, we do not sell Sensitive Personal Data, and we do not process or otherwise share Sensitive Personal Data for the purpose of targeted advertising.

Automated Decision-Making and Profiling

We do not conduct automated processing of Personal Data for the purposes of evaluating, analyzing, or predicting an individual's personal aspects in furtherance of decisions that produce legal or similarly significant effects. As a result, we do not provide a right to exercise control over such forms of automated decision-making and profiling.

Your Additional U.S. Privacy Choices

Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to exercise some or all of the following rights:

Right to Know. The right to confirm whether we are processing Personal Data about you and, under California law only, to obtain certain personalized details about the Personal Data we have collected about you, including:
The categories of Personal Data collected;
The categories of sources of the Personal Data
The purposes for which the Personal Data were collected;
The categories of Personal Data disclosed to third parties (if any), and the categories of

recipients to whom this Personal Data were disclosed;
The categories of Personal Data shared for targeted advertising purposes (if any), and the categories of recipients to whom the Personal Data were disclosed for these purposes; and
The categories of Personal Data sold (if any) and the categories of third parties to whom the Personal Data were sold.
Right to Access & Portability. The right to obtain access to the Personal Data we have collected about you and, where required by law, the right to obtain a copy of the Personal Data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
Right to Correction. The right to correct inaccuracies in your Personal Data, taking into account the nature of the Personal Data and the purposes of the processing of the Personal Data.
Right to Control Over Sensitive Personal Data. The right to exercise control over our collection and processing of certain Sensitive Personal Data.
Right to Opt-Out of Targeted Advertising. The right to direct us not to use or share Personal Data for certain targeted advertising purposes.
Right to Opt-Out of Sales. The right to direct us not to sell Personal Data to third parties.
Right to Deletion. The right to have us delete Personal Data we maintain about you (subject to certain exceptions).
Depending on your state of residency, you may also have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights. However, the exercise of the rights described above may result in a different price, rate or quality level of product or service where that difference is reasonably related to the impact the right has on our relationship or is otherwise permitted by law.

Submitting Privacy Rights Requests

Please submit a request specifying the right you wish to exercise by:

Completing our online form found here; or
Calling our toll-free U.S. telephone number: +1 (800) 988 7973.
To exercise your right to opt-out as it relates to the use of cookies and similar technologies that involve the sale of Personal Data or the use of Personal Data for targeted advertising purposes, please click the “Cookie Settings” link in the footer of the website and adjust your preferences accordingly. If you are visiting our Sites with the Global Privacy Control enabled, any cookies that constitute sales or are used for targeted advertising should already be turned off automatically in our cookie preference manager. Please note this opt-out tool is website, device and browser specific, so you will need to change your preferences on each device and browser you use to interact with the specific website you are visiting. In addition, you can also opt-out of cookie-based sales by businesses that participate in the Digital Advertising Alliance’s CCPA Opt-Out Tool by visiting https://www.privacyrights.info/. Lastly, you may follow the other steps set forth in Section (13) above to further exercise control over cookies and similar technologies.

Before processing your request to exercise certain rights (including the Right to Know, Access & Portability, Correction, and Deletion), we will need to verify your identity and confirm you are a resident of a state that offers the requested right(s). In order to verify your identity, we will generally either require the successful authentication of your account, or the matching of sufficient information you provide us to the information we maintain about you in our systems. As a result, we require requests submitted through our online form and toll-free number to include [requester’s name and email address, their relationship with Anker, the brands relevant to the request, and the data subject’s first and last name, home address, phone number, and

any comments you may have].

In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or where you are not a resident of one of the eligible states.

Submitting Authorized Agent Requests

In certain circumstances, you are permitted to use an authorized agent to submit requests on your behalf through the designated methods set forth above where we can verify the authorized agent's authority to act on your behalf. In order to verify the authorized agent's authority, we generally require evidence of either (i) a valid power of attorney or (ii) a signed letter containing your name and contact information, the name and contact information of the authorized agent, and a statement of authorization for the request. Depending on the evidence provided and your state of residency, we may still need to separately reach out to you to confirm the authorized agent has permission to act on your behalf and to verify your identity in connection with the request.

Appealing Privacy Rights Decisions

Depending on your state of residency, you may be able to appeal a decision we have made in connection with your privacy rights request. All appeal requests should be submitted by replying to the communication resolving your original request.

Financial Incentives and Loyalty Programs

We offer various financial incentives to our customers, including:

Discounts, coupons, and special offers via email when signing up for our email lists or creating an account;
Rewards when referring a friend who purchases our products or services; and
Loyalty programs, where customers earn / redeem rewards based upon their past transactions with us.
To obtain access to certain of these programs and other offerings, we may ask to collect your Personal Data, including name, contact information, professional information, account information, and transaction information. We consider the value of these programs and other offerings to be reasonably related to the value of the Personal Data to our business, based on our reasonable but sole determination. We estimate the value of the Personal Data by considering the expense incurred by the business related to the collection, storage, and retention of the Personal Data in the context of the financial incentive program and the expenses related to the provision of the financial incentive.

The terms applicable to each program and other offering are provided at the time an eligible customer is offered an opportunity to participate. Interested customers can opt-in to these programs and offerings by following the instructions presented at the time the offer is made. Participating customers may withdraw from our programs and other offerings at any time by unsubscribing from our emails (for email-based incentives), closing their accounts (for loyalty and reward program incentives), following the instructions provided in connection with each offering, or by emailing us at support@anker.com.

Definitions

“Adequate Jurisdiction” means a jurisdiction that has been formally designated by the European Commission as providing an adequate level of protection for Personal Data.

“Application” means any applications operated, or maintained, by us or on our behalf.

“California Resident” means (1) every individual who is in the State of California for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State of California who is outside the state for a temporary or transitory purpose.

“Cookie” means a small file that is placed on your device when you visit a website (including our Sites). In this Privacy Notice, a reference to a “Cookie” includes analogous technologies such as web beacons and clear GIFs.

“Controller” means the entity that decides how and why Personal Data are Processed. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.

“Data Protection Authority” means an independent public authority that is legally tasked with overseeing compliance with applicable data protection laws.

“EEA” means the European Economic Area.

“GDPR” means the General Data Protection Regulation (EU) 2016/679.

“Personal Data” means information that is about any individual, or from which any individual is directly or indirectly identifiable, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

“Process”, “Processing” or “Processed” means anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).

“Profiling” means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

“Relevant Personal Data” means Personal Data in respect of which we are the Controller.

“Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration. A business does not sell personal information when:
A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party;
The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information;
The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purposes if both of the following conditions are met:
The business has provided notice that information being used or shared in its terms and

conditions consistent with Section 1798.135 of the CCPA; and
The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose; or
The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with Sections 1798.110 and 1798.115 of the CCPA.
“Standard Contractual Clauses” means template transfer clauses adopted by the European Commission or adopted by a Data Protection Authority and approved by the European Commission.
“Site” means any website operated, or maintained, by us or on our behalf.
Annex 1 Details of Processing

Processing activity and Processed Personal Data

Purposes

Legal basis for Processing

Provision of Sites or Applications:

· IP address

· Usage logs

· Website from which access occurred (referrer URL),

· Unique identifiers（UUID）

· Browser used (incl. type, ID and configuration) and your computer’s or phone's operating system, if applicable, as well as the name of your access provider.

· To ensure we can provide a smooth connection to our Sites or Applications

· To ensure users can comfortably use our Sites or Applications

· To assess system security and stability

· For further administrative purposes

Our legitimate interest to provide secure, needs-based Website.

Creating user account:

· Email addresses

· Passwords, and/or

· Phone numbers

Via Google/ Facebook/Apple/ Amazon account：

· Login information: logging in using a Google account, Facebook account, or Apple account

· Provision of a user account, with address management, order overview

· Organization of the email-preferences · Security of the account · Evaluation of our users

The Processing is necessary for entering or performing a contract with you.

Payment and Transaction:

· Transaction information: records of purchases and prices, consignee first and last name, shipping address and contact information, shipment tracking details, details of returns, and warranty details.

· Payment details: such as invoice / payment records, payment amount, payment date, billing address, payment method.

· Receiving renumeration that we are owed

· Implementation of the contract concluded with you

The Processing is necessary for entering into or performing a contract with you.

Binding devices with Applications：

· Information about your device and network

· Product-specific information

· Usage data: device and App log files, settings (including settings history), usage history, device and service settings, and device status

· To ensure users can use our Applications to connect, control and operate the Anker products you have purchased.

The Processing is necessary for entering or performing a contract with you.

Contacting us:

· first and last name

· preferred name

· phone number

· email address

· mailing address

· Processing of your request

· Performance of the communication

· Analyzing errors and improving our services

Depending on the reason you are contacting us:

· The Processing is necessary for entering or performing a contract with you. or

· Our legitimate interests in Processing your request and performance of the communication.

Notification of changes, product security communications and product recalls:

· Name

· E-mail address

· Address (including region)

· Phone number

· Information about the communication we made to you and any following communications.

· Informing you about changes or security communications

· notification of the need for a product recall and the manner in which such a recall will be conducted

Depending on the reason you are contacting us:

· The Processing is necessary to fulfil a legal obligation, or

· The Processing is necessary for performing a contract with you, or

· Our legitimate interests in informing you about a change or security communication.

Comments and opinions, if they are expressed directly to us:

· communications data, depending on the way of contact (see above)

· Your comments and opinions.

· Responding to and address your queries, issues and concerns,

· Improving our products and services

· Informing our marketing strategies

Our legitimate interests, namely communicating with current or prospective customers and others about our products and services.

Contract data (via our Sites or Applic ations):

· Name

· E-mail address

· Address (including region)

· Phone number

· If applicable: Deviating delivery address

· Payment information

· Processing your order

· Fulfilling the contract

· Communicating with you about our products and services,

· Enabling you to utilize our products and services ·Responding to any queries, issues or concerns you may have

The Processing is necessary for entering or performing a contract with you.

Newsletter:

· Email

· Tracking information (open and click rates)

· Informing you about new developments concerning Anker, our products, services and promotions

· Insight into what content is of interest to you to improve our newsletter

·Advertising our products and services

· The Processing is based on your consent, or, where we have obtained your email address in the course of you ordering our services,

· based on our legitimate interest in sending you offerings to products/services similar to the ones you have purchased from us.

Displaying advertisements:

· IP address of the requesting computer,

· Date and time of access,

· Website from which access occurred (referrer URL),

· Unique identifiers (UUID),

· Browser used (incl. type, ID and configuration) and your computer's operating system, if applicable, as well as the name of your access provider

· Interests, based on the use of our services and Sites/ Applications and the information provided by our ad-network partners. For more information about advertising and tracking, please also see our Cookie Notice.

· Informing you about new developments concerning Anker, our products, services and promotions

· Advertising our products and services

Insofar as the Processing is aimed at tailoring our advertisements to your interests,

· The Processing is based on your consent. Otherwise,

· The Processing is based on our legitimate interests, namely to market and advertise our products and services.

Analyzing trends, usage and activities:

· IP address of the requesting computer or phones,

· Date and time of access,

· Website from which access occurred (referrer URL),

· Unique identifiers (UUID),

· Browser used (incl. type, ID and configuration) and your computer's operating system, if applicable, as well as the name of your access provider

· Session recordings

· Website to which you leave our Site

· Items viewed, actions performed during a browsing session

· Analyzing trends, usage and activities

· Improving our services

· Tailoring our advertisements

· Insight into what content is of interest to you

·Analyzing errors and improving our services

The Processing is based on your consent.

Maintaining IT security (including audits):

· IP address of the requesting computer or phones,

· Date and time of access,

· Name and URL of the accessed file,

· Website from which access occurred (referrer URL),

· Unique identifiers (UUID),

· Browser used (incl. type, ID and configuration) and your computer's operating system, if applicable, as well as the name of your access provider

· Behavior while using our Sites, Applications, products and services.

· To ensure users can comfortably use our Sites, products and services

· To assess system security and stability · Finding and eliminating security vulnerabilities

· Monitoring and demonstrating of our safety level, also to achieve external certifications

· The Processing is necessary for entering or performing a contract with you. or

· Our legitimate interests in ensuring the safety of our Sites, products and services.

Surveys:

· Name and title

· E-mail-address

· Your responses

· Analyzing errors and improving our Sites, products and services

· Obtaining customer feedback

Our legitimate interests in obtaining customer feedback and improving our Sites, products and services.

Shipment tracking:

· Order Number

· Email or Phone number Or

· Tracking Number

· Providing shipment tracking

Our legitimate interest in providing you with shipment tracking.

Refer friends:

If you refer a friend:

· Name

· Email address

· Purchases made though link

· Information about rewards

If a friend refers you:

· Your Personal Data is Processed as shown above

· Purchases are attributed to the link you were invited with

· Increasing sales of our products and services

· Enabling participation in our refer a friend program

· Paying out rewards for participation in the program

Our legitimate interest in advertising our products through a refer a friend program.

Discount networks (e.g., Studentbeans):

· Authorization to use the discount

· Personalized discount codes

· Purchased products

· Enabling a discount for faculty and students.

· Improving the sale of our products to these groups

Our legitimate interest in advertising our products through special discount codes.

Warranty application:

· E-mail address

· Name

· Order number, or screenshot of order or receipt

· Product description

· Address

· Phone number

· Description of defect

· File or purchase receipt

· Verification of the warranty claim

· Implementation of the warranty claim

· Documentation of the defect

The Processing is necessary for entering or performing a contract with you

Live Chat with Support:

· Name

· E-mail address

· Contents of the chat

· provision of the live chat

· security of the live chat

· feedback on and improvement of our products

· The Processing is necessary for entering or performing a contract with you or

· Our legitimate interest in providing a live chat.

Community Forum：

· Profile name

· Posts (including if they are edited), and anything contained therein, such as pictures

· Community level

· Providing a forum for discussion of our products

· Support for engagement in this forum

· Ensuring compliance with the terms of the forum

The Processing is necessary for entering or performing a contract with you

1V1 Video Shopping：

· Device type

· Browsing history

· Recipient information provided by users, such as name, contact number, and delivery address.

· Session length

· Video recording

· Chat history

· Processing your orders

· Enhance our services

· The Processing is necessary for entering or performing a contract with you， and/or

· The Processing is based on your consent.

Testing Club:

· Name

· Email

· Test plan

· Product reviews, including photos and videos.

· Survey (if test requires so).

· Review of applications and selection of suitable testers

· Provision of free products for testing

· Obtaining reviews of the products

· Improvement of the test products

· Promotion of the products to be tested

· The Processing is necessary for entering or performing a contract with you Or

· The Processing is necessary for our legitimate interest in improving and promoting our

products.

Legal:

· All of the above

· Complying with regulatory obligations

· Litigation

· Exercise, enforcement and defense of claims

· The Processing is necessary for our legitimate interest in compliance with regulatory obligations, and exercising, enforcing and defending of claims.

Annex 2 Product-specific information

Customer content: including any files, documents, audio, videos, images, data, or communications you choose to input, upload, or transmit to our Sites, Applications, products and services. In addition, certain of our Sites, Applications, products, and services may allow you to collect or process additional customer content directly on your device without transferring such content back to Anker. For example, you may generate voice prompts when you use one of our voice-assisted technologies, such as our smart speakers, and transfer your voice prompts to your third-party voice-assistant service account (such as Amazon's Alexa or Google Assistant) as a command. We may also enable you to collect images and video through certain of our products, such as the Roav Dash Cam and eufy security cameras. Note that depending on where you live, the surveillance laws in effect in your jurisdiction, and how you configure our services, you may need to obtain explicit consent from individuals before using our products to create and save video or images of them or provide notice informing visitors to your home that our products or services are in use. It is your responsibility to ensure that you comply with all such applicable laws.
Entertainment-related service information: when you use our entertainment-related services, include our Nebula Smart Projectors and SoundCore speakers and headphones, we collect information about your entertainment preferences, including audio / video settings, and the entertainment services you like to engage with. With your permission, we will also read call status for the SoundCore music player so that music played before a call can be paused and resumed after the call ends. With your permission, the SoundCore app may also seek permission to access your mobile device's microphone to enable you to take advantage of certain speech-based speaker / headphone features. You may refuse or withdraw your permission at any time through the privacy settings of your mobile device.
Home-related services information: when you use our home-related services, including eufy Clean, eufy Pet and eufy Security, we collect information about your home and your activities around your home, including the location of your home, home environment data (such as level of dirt, smart device movement, floorplans and room names, existence and types of objects within the home, and floor type), pet information (such as pet type and activity), home occupancy data (such as the presence or absence of individuals within your home zone or specific areas of your home at any given time), home monitoring audio, images and videos (such as alerts triggered by your home security system). Note that depending on where you live, the surveillance laws in effect in your jurisdiction, and how you configure our services, you may need to obtain explicit consent from individuals before using our products to create and save

video or images of them or provide notice informing visitors to your home that our products or services are in use. It is your responsibility to ensure that you comply with all such applicable laws.
Car-related services information: when you use our car-related services, including Roav DashCam, SmartCharge and Viva, information about your vehicle, such as the first nine digits of your VIN to confirm your vehicle's make, model and year, and your driving experience, including the precise location of your vehicle, engine start/stop and idle times, your vehicle's speed, braking and acceleration metrics, and your driving route, are collected locally on your device and/or mobile application.
Baby-related services information: when you use our baby-related services, including the eufy Baby Monitor and Smart Sock, we collect information that you choose to share about your baby, including your baby's name, gender, due date or date of birth, weight, photographs, monitor images and video, and, when using the eufy Smart Sock, sleep patterns, nap patterns, movements, heart rate, and blood oxygen levels.
Health-related services information: when you use our health-related services, including the eufy Smart Scale, eufy Blood Pressure Monitor, and SoundCore health-connected devices, information that you choose to track in relation to your personal health, including weight, height, body mass index, body fat percentage, muscle mass, heartrate, water content, basal metabolic rate, visceral fat, lean body mass, body fat, bone mass, body age, protein, subcutaneous fat percentage, body type, skeletal muscle mass, blood pressure, blood oxygen, posture, calories burned, duration of exercise, and sleep metrics, such as estimated sleep time through real-time monitoring of sleep environment sound (though we will not store the underlying sound file), are collected by us or are otherwise maintained locally on your device and/or mobile application.
Biometric services information: certain of our services leverage biometric technologies (such as facial recognition tools) when a user chooses to turn on biometric-related features, such as face images and underlying face prints. In particular, we may provide you the ability to (i) log in to our Applications or authenticate yourself using facial, fingerprint or other biometric recognition technology available through your mobile device, or (ii) leverage facial recognition technology on your eligible eufy device to determine whether an individual in the device's field of vision is a "familiar face" or a stranger. We do not store or have access to this biometric information. Instead, the applicable biometric assessment process is conducted entirely on your device. We may, however, receive confirmation of the results of the biometric assessment, such as in the form of a token from your mobile device indicating you successfully authenticated using biometric recognition technology or an alert attached to your security account indicating your camera saw a "familiar face" or a stranger. Depending on where you live, the laws in effect in your jurisdiction, and how you configure our services, you may need to obtain explicit consent from individuals before using our products to create, save and analyze video or photographic images of them (including to conduct biometric processing of their images) or provide notice informing visitors to your home that our products or services are in use. It is your responsibility to ensure that you comply with all such applicable laws.