

Privacy Policy

Last modified: August 31, 2026

Effective date: August 31, 2026

1. Introduction

This policy applies to information we collect:

- when you install, register with, access, or use the VeSync App (“App”); the VeSync.com, Cosori.com, Levoit.com, or Etekcity.com websites (“Websites”); and the services offered in VeSync Account;
- when you use smart products and/or their functionalities connected to, or through, the App;
- when you interact with our advertising and applications on third-party websites and services, if those applications or advertising include links to this policy;
- when you subscribe to our newsletters, promotions or other marketing initiatives; and
- when you contact or interact with us, for example, in email, text, and other electronic messages between you and our Websites, App, or our Customer Service team.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, or do not want us to collect the information, do not download, register with, or use the App or Websites. This policy may change from time to time (see Changes to Our Privacy Policy below). Your continued use of our App, Websites, or services after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

2. Information We May Collect and How We Collect It

Information we may collect

When You Use Our App, Websites, or Related Products and Services, We May Collect the Following Information:

This Privacy Policy for VeSync describes how Vesync (US) Corporation, Vesync Technology Corporation, and Arovast Corporation (collectively, "VeSync", "our", "us" or "we") collects, uses, shares, and stores information. Our goal is to provide you with a positive experience when using our Websites, App, products, and services, while at the same time keeping your personal data secure.

- 1) Profile Data**, this means your VeSync Account Profile, which can include username, password, email address, gender, birthdate, and region.
- 2) Logistics Data**, such as receiver’s name, phone number, delivery address, postal code, and related product information.
- 3) Financial Data**, before placing orders, you'll be asked to provide financial data, including card numbers, card expiration dates, CVC codes, account holder name, and billing addresses.

Importantly, it is securely processed by our credit card payment service providers, such as PayPal or Stripe.

4) Technical Data, such as your mobile device data, smart device data and internet connection data, including mobile phone model, terminal ID, mobile phone brand, operating system version, browser type, language, region, smart device model, smart device ID, MAC address, IP address, Wi-Fi name, Wi-Fi signal quality, network operator, network type.

5) Usage Data, such as details of your use of any of our devices, the Websites, and the App, including, but not limited to, history of operation, search queries, and length of visits to certain pages.

6) Consumer Preference Data, such as products purchased, motivation for purchase, your preferences in receiving marketing from us and third parties, your responses to surveys, and other purchasing behavior and preferences.

- Depending on the focus of user study, survey responses may include general demographic or health information, such as age range, income bracket, education level, or basic health status (for example, yes/no questions about allergies).

7) Communications Data, such as your communication preferences, your contact information, the audio recordings of calls when you call the Customer Service team, and records and copies of your correspondence (including email addresses and phone numbers), if you contact us.

- The correspondence may include information like proof of identification, gender, employment, medical information, or health insurance information when needed for Customer Service team to provide related support.

8) Location Data, such as your precise location disclosed by GPS technology and other similar technologies.

9) Content Data, such as the content you post on the Websites or the App. The content data that you post on public areas of the Websites may be transmitted to other users of the Websites or third parties at your own risk. Therefore, we cannot and do not guarantee that your content data will not be viewed by unauthorized persons.

10) Wellness Data:

Rest assured, we do not collect or share your wellness data unless you manually and voluntarily choose to do so. There are three ways you can make this happen:

a) Directly from You, via Use of Our Products:

Our VeSync App will only collect wellness data when you use one of our compatible smart products and manually connect and sync it with the VeSync App. Once synced, your wellness data will be collected and stored on the App's cloud server after each use. For example, by using and syncing a smart body scale, you can record your weight and BMI in the App; by using and syncing a smart blood pressure monitor, you can record your blood pressure and pulse in the App.

b) Directly from You, via Use of Wellness Services:

You may voluntarily choose to manually enter your health data or wellness data within our wellness services. This is completely optional, and you control what data to input.

c) From Third-Party Services:

You may choose to sync your health data or wellness data from third-party services such as Apple Health or Google Health Connect with VeSync App. To do this, you must enable the

connection through your device/phone settings. Similarly, you can allow the VeSync App to sync data with other third-party health trackers, such as MyFitnessPal or Fitbit. These connections will only occur if you actively configure and allow them.

Below is list of wellness data associated with each category of our products:

If you use our wellness products such as smart scales or smart kitchen appliances, you can voluntarily sync the following information with the VeSync App:

Weight, height, metabolic age, gender, body composition such as BMI (Body Mass Index), muscle mass, body water, skeletal mass, BMR, body fat, subcutaneous fat, visceral fat, bone mass, protein, etc., cooking history, food name, food weight, and food nutrition information such as calories, fat, sugar, protein, carbs, trans fat, saturated fat, cholesterol, sodium, potassium, dietary fiber, iron, VD, VA, VC, polyunsaturated fat, monounsaturated fat, calcium, etc.

If you use smart trackers and smart watches, you can voluntarily sync the following information with the VeSync App:

Weight, height, metabolic age, gender, stride, distance, duration, number of steps, sleep status, calories, workout records, sleep records, heart rate records, and blood oxygen records.

If you use smart blood pressure monitors, you can voluntarily sync the following information with the VeSync App:

Systolic pressure, diastolic pressure, and pulse.

If you use smart pulse oximeter, you can voluntarily sync the following information with the VeSync App:

Oxygen saturation, perfusion Index, and pulse.

If you use wellness services in our App and Websites, we may collect the information you voluntarily provide, such as:

- Exercise-related information (e.g. exercise preference, exercise plan, exercise record);
- Body measurements (e.g. birthday, height, weight, waist, bust size, hip size);
- Diet-related information (e.g. diet plan, diet preference, food list, diet record); and/or
- Health-related information (e.g., blood pressure, heart rate, blood glucose, allergies).

11) Aggregated Data

We may store and use any anonymized or aggregated data such as statistical or demographic data that incorporates or is derived from your personal data, which is not itself personal data (“Aggregated Data”); however, we will not do so in a way that identifies you personally. For example, we may aggregate users’ behavioral data to calculate the percentage of users accessing a specific App feature, as well as facilitate and measure the effectiveness of advertisements. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

Cookies and Similar Technology

The Technologies We Use for Automatic Information Collection May Include (for more information, see [Cookie Policy](#)):

- Cookies (or browser cookies).
- Web Beacons.

- Flash Cookies.
- Click-through URL.
- And other similar technologies.

We also may use these technologies to collect information about your online activities over time and across third-party websites or other online services (behavioral tracking).

The information we collect automatically may include personal data. It helps us to improve our Websites or App and to deliver a better and more personalized service, including by enabling us to:

- Estimate our audience size and usage patterns.
- Store information about your preferences, allowing us to customize our Websites and App according to your individual interests.
- Speed up your searches.
- Recognize you when you return to our Websites or App.

Most Websites will prompt you before accepting cookies. You may also change your cookies settings in your browser. Note, depending on your device or browser, it may not be possible to disable all tracking mechanisms. Also, if you set your browser to reject all cookies, parts of the Websites may not work for you. For more information, please see our [Cookie Policy](#).

Artificial Intelligence (AI)

We may use artificial intelligence (AI) technologies as part of our operations, including for data analysis, product or service optimization, or user interaction support. Where AI is used, it may involve the automated processing of personal data in accordance with applicable law.

Categories of Personal Data We Collected

Our App or Websites has collected the following categories of personal data from consumers within the last 12 months:

Category	Examples	Collected
Identifiers.	Profile Data, Logistics Data, Technical Data, or Communication Data.	YES
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Profile Data, Logistics Data, Financial Data, or Communication Data.	YES
Protected classification characteristics under California or federal law.	Profile Data, Consumer Preference Data or Communication Data.	YES, only when you voluntarily provide it in your profile, or needed in a specific survey study, or conversation with Customer Service for related support.
Commercial information.	Logistics Data, or Consumer Preference Data.	YES
Biometric information.	Wellness Data.	YES.
Internet or other similar network activity.	Usage Data.	YES
Geolocation data.	Location Data.	YES

Sensory data.	Communication Data.	YES
Professional or employment-related information.	Communication Data.	YES, only when needed in conversation with Customer Service for related support.
Inferences drawn from other personal information.	Consumer Preference Data.	YES

3. How We Use the Collected Information

We use information that we collect about you or that you provide to us, including any personal data, generally based on the following purposes:

Types of Data	Specific Purpose	Legal Basis for Processing under GDPR (for EEA and UK Users)
Profile Data	<ul style="list-style-type: none">• To allow you to register and log in to your VeSync Account.• To enable you to place orders.• To investigate and prevent fraud.• To enable you to personalize your profile and provide you with region-available services.• To include you in the Programs.• To improve or develop our products and new technologies via analytics.	<ul style="list-style-type: none">• Your consent;• Performance of a contract with you;• Necessary for our legitimate interests (for developing our products/services, running and growing our business, to prevent fraud).
Logistics Data	<ul style="list-style-type: none">• To fulfil your orders and deliver products to you.• To process warranty, returns and/or repairs.	<ul style="list-style-type: none">• Performance of a contract with you;• Necessary for our legitimate interests (to keep records updated and to analyze how customers use our products/services).
Financial Data	<ul style="list-style-type: none">• To process payments.• To detect and prevent fraud.	<ul style="list-style-type: none">• Performance of a contract with you;• Necessary for our legitimate interests (to prevent fraud);• Necessary for compliance with legal obligations.
Technical Data	<ul style="list-style-type: none">• To operate, maintain, and provide you with the features and functionalities.	<ul style="list-style-type: none">• Your consent;• Performance of a contract with you;

	<ul style="list-style-type: none"> • To identify your device for diagnostic purposes and fraud prevention. • To improve or develop our products and new technologies via analytics. • To personalize the product functionalities and services and improve our marketing strategies. • To include you in the Programs. 	<ul style="list-style-type: none"> • Necessary for our legitimate interests (for developing our products/services, running and growing our business, provision of administration and IT services, network security).
Usage Data	<ul style="list-style-type: none"> • To operate, maintain, and provide to you the features and functionalities, to identify your device for diagnostic purposes and fraud prevention, to improve or develop our products and new technologies via analytics, and to personalize the product functionalities and improve our marketing strategies. • To enable you to manually input and track your wellness data, tailor available features to your particularized needs, and provide you with personalized recommendations, product offerings and promotions. • To provide personalized recommended services. • To provide customer services, such as dealing with any enquiries and complaints • To include you in the Programs. 	<ul style="list-style-type: none"> • Your consent; • Performance of a contract with you. • Necessary for our legitimate interests (for developing our products/services, running and growing our business, provision of administration and IT services, network security).
Consumer Preference Data	<ul style="list-style-type: none"> • To provide personalized recommended content and services which you can turn 	<ul style="list-style-type: none"> • Your consent; • Necessary for our legitimate interests (for developing our

	<p>off through visiting privacy settings in the App.</p> <ul style="list-style-type: none"> • To develop new products and features available through our service or otherwise improve our service. • To include you in the Programs. 	products/services, running and growing our business).
Communication Data	<ul style="list-style-type: none"> • To communicate with you. • To provide customer services, such as dealing with any inquiries and complaints. • To provide new promotions to you and to provide you with information on new products and/or services. 	<ul style="list-style-type: none"> • Your consent; • Necessary for our legitimate interests (for developing our products/services, running and growing our business); • Necessary for compliance with legal obligations.
Location Data	To operate, maintain, and provide to you the features and functionalities, to improve or develop our products and new technologies via analytics, and to personalize the product functionalities and improve our marketing strategies.	<ul style="list-style-type: none"> • Your consent; • Necessary for our legitimate interests (for developing our products/services, running and growing our business, provision of administration and IT services, network security).
Content Data	To operate, maintain, and provide to you the features and functionalities, to improve or develop our products and new technologies via analytics, and to personalize the product functionalities and improve our marketing strategies.	<ul style="list-style-type: none"> • Your consent; • Necessary for our legitimate interests (for developing our products/services, running and growing our business).
Wellness Data	<ul style="list-style-type: none"> • To operate, maintain, and provide to you the features and functionalities, to improve or develop our products and new technologies via analytics, and to personalize the product functionalities and 	Your consent.

	<p>improve our marketing strategies.</p> <ul style="list-style-type: none">• To enable you to manually input and track your wellness data, tailor available features to your particularized needs, and provide you with personalized recommendations, product offerings and promotions.	
--	---	--

4. Personal Data Sharing and Disclosures

We may disclose personal data that we collect or you provide in the following ways:

- **Sharing with consent:** with your consent or at your request, we will share your personal data within the scope of your consent/request with specific third parties or categories of third parties authorized or designated by you. For example, when you decide to sync your information with other apps such as Apple Health, Google Health, etc.
- **Sharing within VeSync Group:** we may share your personal data with our subsidiaries, parents, affiliates only for explicit, and legitimate purposes, and the sharing is limited only to information required by services. For example, we verify the global uniqueness of VeSync Accounts before allowing them to be registered.
- **Sharing with service providers:** we also may disclose your data to contractors, service providers, or third parties we use to support our business. They usually perform certain business-related functions for us, such as website hosting, data analysis, payment and credit card processing, infrastructure provision, IT services, customer support service, e-mail delivery services, marketing, analytics, financial incentive programs, and other similar services. These service providers are contractually restricted from using or disclosing the information, except as necessary to perform services on our behalf or to comply with legal requirements.
- **Sharing with advertising, marketing, and analytics providers:** we may disclose your data with other companies that conduct marketing and advertising services to promote products and services. This includes advertisers, publishers, social media platforms, advertising technology providers, and analytics vendors that help us offer and measure the effectiveness of our advertising and other marketing offers targeted advertising and other marketing offers. Personal data received by these companies may also be subject to their privacy policies. More information on sharing through tracking tools and your choices are described in our [Cookie Policy](#).
- **Sharing for complying with the law or legal process:** we may be required to respond to a subpoena, court order, search warrant, administrative or judicial process, requests by law enforcement agencies, or other requests that we must respond to under applicable law. We may disclose your personal data in response to any of these requirements.

- Sharing for protection of our legal rights and/or those of others: we may disclose your personal data to preserve the security of our VeSync App, Websites, or social media accounts; resolve disputes; or assess any possible wrongdoing.
- Sharing during asset transfer: to a buyer or other successor in the event of 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 App users is among the assets transferred.
- To enforce our rights arising from any contracts entered into between you and us, including the Terms of Use, and for billing and collection.
- To fulfill the purpose for which you provide it.
- For any other purpose disclosed by us when you provide the information.

We will ensure that the lawfulness of this sharing and, if applicable, sign stringent non-disclosure agreements (NDAs) and/or data processing clauses with the companies, organizations, and individuals with whom personal data is shared, requiring them to comply with this policy and take appropriate confidentiality and security measures when processing personal data.

If we transfer personal data received under the EU-US DPF, UK Extension to the EU-US DPF, and the Swiss-US DPF to a third-party processor, the third-party processor's access, use, and disclosure of the personal information must also be in compliance with our DPF obligations, and we will remain liable under the EU-US DPF, UK Extension to the EU-US DPF, and the Swiss-US DPF for any failure to do so by the third party unless we prove we are not responsible for the event giving rise to the damage.

Note: We will not disclose data regarding text messaging opt-in and consent to any third parties for their own marketing purposes.

In the preceding twelve (12) months, the Company has sold and/or shared personal data with the categories of third parties indicated in the chart below.

***Disclosure of "Sale" and "Sharing" of Personal Data as defined in Applicable States in the U.S.**

We do not sell your personal information for money. However, under the CCPA and similar U.S. state privacy laws, some of our advertising activities may be considered a "sale" or a "sharing" of personal information for cross-context behavioral advertising, whether or not money is exchanged. These activities include:

- Cookie-based advertising. We use cookies and similar technologies, and make personal information available to advertisers and advertising platforms through third-party cookies, for cross-context behavioral advertising. You can decline these cookies through our cookie banner.
- Audience matching and "look-alike" advertising. We disclose identifiers such as your email address to third-party advertising platforms so that they can match you to their users, build "look-alike" audiences of people with similar characteristics, and deliver advertising for our products to you and to those audiences across other apps and websites. You have the right to opt out of this sale and sharing at any time. To opt out, click "Do Not Sell or Share My Personal Information" at the bottom of the Website and submit your email address or adjust your

settings in the VeSync App by clicking More > Settings > Privacy > Data Sharing for Look-Alike Advertising.

Personal Data Category	Category of Third-Party Recipients	Sales and/or Sharings
Identifiers.	Affiliates, Parent, subsidiary organizations or service providers/processors.	Internet cookie data recipients like Google Analytics. See Cookie Policy . Advertising networks and platforms. Purpose: cross-context behavioral advertising, audience matching, and look-alike audience targeting.
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Affiliates, Parent, subsidiary organizations or service providers/processors.	For identifiers, we use Internet cookie data recipients like Google Analytics. See Cookie Policy . For Financial Data, none. Our Websites collect payment card or banking information to complete product purchases, but we do not store such information. All payments are processed by our payment service providers, PayPal and Stripe.
Protected classification characteristics under California or federal law.	Affiliates, Parent, subsidiary organizations or service providers/processors.	None
Commercial information.	Affiliates, Parent, subsidiary organizations or service providers/processors.	Internet cookie data recipients like Google Analytics. See Cookie Policy .
Biometric information.	Affiliates, Parent, subsidiary organizations or service providers/processors.	None
Internet or other similar network activity.	Affiliates, Parent, subsidiary organizations or service providers/processors.	Internet cookie data recipients like Google Analytics. See Cookie Policy .
Geolocation data.	Affiliates, Parent, subsidiary organizations or service providers/processors.	Internet cookie data recipients like Google Analytics. See Cookie Policy .
Sensory data.	Affiliates, Parent, subsidiary organizations or service providers/processors.	None

Professional or employment-related information.	Affiliates, Parent, subsidiary organizations or service providers/processors.	None
Inferences drawn from other personal information.	Affiliates, Parent, subsidiary organizations or service providers/processors.	Internet cookie data recipients like Google Analytics. See Cookie Policy .

5. Retention of Personal Data

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

This (Section 5) does not apply to anonymized, deidentified or Aggregated Data.

6. How We Secure Personal Data

VeSync implements reasonable and appropriate industry-standard security controls to protect personal data in its possession. VeSync's administrative, physical, and technical safeguards:

- Provide assurances of the integrity and confidentiality of personal data covered by this policy.
- Protect against reasonably anticipated threats or hazards to the security or integrity of personal data, and unauthorized uses or disclosures of such personal data; and
- Facilitate compliance with legal frameworks of requirements under applicable data protection laws.

To this end, we take the following measures:

- We take reasonable and feasible measures to ensure that the personal data collected is minimal and relevant to what is necessary in relation to the purposes for which they are processed. We retain your personal data for no longer than is necessary for the purposes stated in this policy and privacy notice of specific product or service, unless extending the retention period is required or permitted by law.
- We use a range of technologies such as cryptographic technologies to ensure the confidentiality of information in transmission. We implement trusted protection mechanisms to protect data and data storage servers from attacks.
- We deploy access control mechanisms to ensure that only authorized personnel can access your personal data. In addition, we control the number of authorized personnel and implement hierarchical permission management on them based on service requirements and personnel levels.

- We strictly select business partners and service providers and incorporate personal data protection requirements into commercial contracts, audits, and appraisal activities that are at least as stringent as the ones VeSync itself uses, consistent with this policy.
- We hold security and privacy protection training courses or other equivalent publicity activities to raise employees' personal data protection awareness.

The security of your data also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our services, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. We urge you to be careful about giving out data in public areas of the App like Forum. The information you share in public areas may be viewed by any user of the App.

Although we do our best to protect your personal data, unfortunately, no security measures can provide absolute protection. To cope with possible risks, such as personal data leakage, damage, and loss, we have procedures in place to deal with suspected data security breaches. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us in accordance with Contact Information below.

7. Notice of Financial Incentives

We offer various financial incentive programs (the “Programs”) that allow participants to earn or receive rewards, points, and discounts, in exchange for registering and/or making purchases, including:

- Spend-based incentives, where you earn points based upon spend levels
- Periodic promotional discounts and offers

You can sign up for the Programs by registering on our Apps or Websites. We collect and use the categories of personal data described in the “Information we may collect” section. Registration requires you to provide your email address, and you may also elect to provide other information, including your phone numbers. We will then associate that and other categories of personal data with your account, such as Technical Data, Usage Data, or Consumer Preference Data, to identify you as a member of the Programs and provide you with relevant messaging, discounts, and points. These financial incentives are reasonably related to the value of the information you provide.

Full terms for the Programs are available [here](#).

You may withdraw from the Programs at any time and forfeit any ongoing incentives by contacting us using the contact information below. Please also note that if you submit a request to delete your personal data, this will also automatically withdraw you from the Programs and will result in the forfeiture of your incentives, including your points that you may have accumulated. Requesting the deletion of your personal data may result in the deletion of your account and accumulated incentives because we require your personal data (e.g., your name, email address, and log-in information) to be able to associate you to your account. You may elect to rejoin the Programs at any time, at which time we will once again begin collecting your personal data.

Based on our reasonable and good faith estimate, we receive value from the Programs in increased customer loyalty and patronage, though any value will vary by members depending on purchases made, which offers a member takes advantage of, and many other factors.

8. How We Protect Children's Personal Data

a. Marketing and Sales to Adults

The Websites, App, and services are not intended for children under the age of 18 or the equivalent age as specified by law in your jurisdiction. We do not knowingly collect personal data from children for purposes of marketing or sales. We also do not collect any personal data from children under the age of 18 without their parent's or guardian's consent. If we learn we have collected or received personal data from a child without parental consent, we will take steps to delete that information as soon as possible. If you believe that we have unknowingly collected information about a child in connection with our marketing or sales operations, please contact us using one of the methods in the Contact Information below for us to delete it.

b. Personal Data of Children Collected in Connection with the Use of Smart Devices

While our App and services are available only to registered adult users, we recognize that family and household members of registered users may be children. We also recognize that registered adult users may, from time to time, permit their family and household members, including children, to use their VeSync products. For example, parents or guardians of a child may allow their child to use the smart scale or other fitness products and configure their VeSync Accounts to track fitness data about their child. Parents or guardians may also add a child's name, weight, age, and birthday into their VeSync Accounts. Therefore, online accounts maintained by VeSync, as used by registered adult users, may include personal data of children. Note, persons under the age of 18, or any higher minimum age in the jurisdiction where that person resides, are not permitted to create VeSync Accounts, and we do not ask a child to supply any information to us directly. Rather, a parent or guardian must provide the child's personal data and consents to the collection and disclosure of their child's information through his or her account and in accordance with this Privacy Policy.

When children's personal data is collected based on the consent of the parent or guardian, we will only use or disclose the information in accordance with [VeSync Privacy Policy for Children](#). Parents or guardians who need to access, modify, or delete the personal data of their children or people under guardianship can do so directly in their VeSync Accounts. Alternatively, contact us via the channels provided in the Contact Information below.

9. Your Rights and Choices

Data protection laws in your country of residence may give you a number of legal rights in relation to the personal data that we hold about you. Subject to limitations set out in applicable laws, these rights may include:

Right to Know, Correct and Data Portability

You can access, correct, or modify the information you provided to us by editing your profile and adjusting your account settings.

You can export the information you provided to us in VeSync App settings (More > Settings > Privacy > Download Your Data).

You can also click [here](#) or contact us to submit your right to access, correct, modify, or export your information.

To protect your privacy and maintain security, we take steps to verify your identity before granting you access to your personal data or complying with a deletion, portability, or other related request. We may, in certain situations, reject your request for access, correction, or portability, for example, we may reject access where you are unable to verify your identity.

Right to Delete

You can delete your VeSync Account or data in VeSync App settings (More > Settings > Account & Security > Delete Account or Data), or you can delete them using our link [here](#).

You can also click [here](#) or contact us to submit your right to delete your information. Please note that if you request deletion of your personal data, or if you delete your account, we may retain your personal data for the purposes of satisfying any legal, regulatory, tax, accounting, or reporting requirements. Also, because we take measures to protect data from accidental or malicious loss and destruction, residual copies of your personal data may not be removed from our backup systems for a limited period of time.

Right to Opt-Out

We strive to provide you with choices regarding the personal data you provide to us. We have created mechanisms to provide you with the following control over your information:

- **Tracking Technologies.** You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent, please see our [Cookies Policy](#) here.
- **Audience Matching and "Look-alike" Advertising.** You can opt out in either of these ways: (a) VeSync App: toggle off " Data Sharing for Look-Alike Advertising " in the VeSync App > More > Settings > Privacy; (b) Website: click "Do Not Sell or Share My Personal Information" at the bottom of the Website and submit your email address.
- **Promotional Offers from the VeSync.** You may utilize the unsubscribe function in each promotional email. You may also submit your request to opt-out by clicking [here](#) or sending us an email stating your request to support@vesync.com.

This opt-out does not apply to information provided to us as a result of a product purchase, warranty registration, product service experience or other transactions.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. You can also opt out of receiving targeted ads from members of the Network Advertising Initiative ("NAI") on the NAI's [website](#).

Right to Request a List of Third Parties

If applicable under states' law or other regulations, you may have the right to request a list of third parties whom we have shared your personal data with.

Right to Appeal a Refusal

If we can't confirm your identity or authority to make a request, or if the information is legally required to be retained, we may not be able to honor your request. If your request is denied, like in cases where we can't verify your identity, you can appeal our decision by contacting us.

Non-Discrimination

We won't treat you differently for exercising your rights and choices. However, please note that some features or functionality on our App or Websites may change or become unavailable to you

based on the information you provide.

If you are a user in the EEA, UK, or Switzerland, you may have additional rights

Right to restriction of processing

For users in the EEA, UK, or Switzerland, you have the right to restrict the processing of your personal data in accordance with applicable laws.

Right to object

For users in the EEA, UK, or Switzerland, you can object to the processing of certain personal data concerning you for any reason relating to your particular situation.

Right to limit the use and disclosure of your personal data

For users in the EEA, UK, or Switzerland, we generally offer you the opportunity to choose whether your personal data may be (i) disclosed to third-party controllers or (ii) used for a purpose that is materially different from the purposes for which the data was originally collected or subsequently authorized by you. To the extent required by the DPF Principles, we obtain opt-in consent for certain uses and disclosures of sensitive data.

Withdraw consent

For users in the EEA, UK, or Switzerland, you have the right to withdraw consent at any time when we are relying on consent to process your personal data. However, this may not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you.

You can exercise your rights by clicking [here](#) or contacting us directly. You can also lodge a complaint with the data protection regulator if you think that any of your rights have been infringed by us.

10. Links to Other Parties' Websites, Products, and Services

The Websites, App, and services may contain links to third-party websites, products, and services of interest. All links to third-party websites, products, and services are provided for users' convenience only. You need to determine your interaction with such links on your own. We cannot be responsible for the protection and privacy of any information which you provide while visiting or using such third-party websites, products, and/or services and they are not governed by this policy. You should exercise caution and look at the privacy statement applicable in question.

In addition, when you download the App, certain third parties may use automatic data collection technologies to collect information about you or your device. These third parties may include: 1) your mobile device manufacturer, like Apple, Samsung and Google; and 2) your mobile service provider. These third parties may use tracking technologies to collect information about you or your online activities over time and across different websites, apps, and other online services websites. We do not control these third-party tracking technologies or how they may be used. If you have any questions, you should contact the responsible provider directly.

11. International Data Transfer

We share your personal data within the VeSync Group to carry out the activities specified in this Privacy Policy. We may also subcontract the data processing to third parties located outside your

country. Whenever we transfer personal data outside of your country of residence, we will ensure that the data is transferred in accordance with this Privacy Policy and as permitted by the applicable laws on data protection.

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 we adhere 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 [Data privacy framework website](#).

In compliance with the 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. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF should first contact us at: privacy@vesync.com.

In compliance with the 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) and 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. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

Under certain conditions, EU and UK and Swiss individuals can invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms. Please see [ANNEX-I-introduction](#) for additional information.

The Federal Trade Commission has jurisdiction over our 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. Data Privacy Framework (Swiss-U.S. DPF).

Please contact us if you want further information.

12. Do Not Track Disclosures

With regard to Do Not Track (DNT), we currently don't respond to DNT signals in browsers because no DNT standard has been adopted.

13. Entire Privacy Policy

We may provide you with separate privacy notices for specific products and services, and such privacy notices are incorporated into herein by reference. If there is any inconsistency between

specific privacy notices and this general Privacy Policy, the specific privacy notice shall prevail.

14. Changes to Our Privacy Policy

We may update this Privacy Policy periodically to reflect changes in how we collect and use your personal data or changes in applicable laws. It is important that you check back often for updates to the Privacy Policy. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

15. Contact Information

If you would like to make a privacy right request, you may contact us by using our webform, at <https://www.vesync.com/legal/privacy/privacy-rights-request>.

You can also contact our privacy team by email or postal mail at the following contact information:

Attention: Legal Department

Email: privacy@vesync.com

Postal Address: 1775 FLIGHT WAY, SUITE 150, TUSTIN, CA 92782 US

If you are EEA and UK users, please contact us via the following address:

Legal representative in EEA: Vesync Germany GmbH

Postal Address: Prinzenallee 11a, 40549 Düsseldorf, Germany

Legal representative in the UK: VESYNC (UK) LIMITED

Postal Address: Unit G2 Havebside Industrial Estate, Fishtoft Road, Boston, PE21 0AH, United Kingdom