

ONECOOPER WELLNESS PLATFORM PRIVACY POLICY

A. ABOUT THIS POLICY

In this OneCooper Wellness Platform Privacy Policy (**Privacy Policy**)

- references to **we, us** or **our** means Cooper Companies, Inc. and/or the Affiliates (defined below) and
- references to **you** and **your** or **data subjects** are to any users of the OneCooper Wellness Platform (**Platform**).

This Privacy Policy outlines when, why and how we collect, use and otherwise handle (collectively **process**) your personal data within the OneCooper Wellness platform (**Platform**). **Personal data** (within the meaning of Art 4 No 1 General Data Protection Regulation (**GDPR**)) is any information relating to you, which can be used to personally identify you, either directly or indirectly. We will process your personal data, as described in this Privacy Policy and as described when we collect personal data from you. This Privacy Policy must be read together with any other legal notices or terms and conditions provided or made available to you when we collect personal data from you (or at a later stage) or that are available on other pages of the websites of Cooper or its Affiliates.

The Platform is an all-in-one corporate platform used to deliver customized health and wellness programs to those of our employees who are granted access to the Platform. This Privacy Policy applies to the personal data we collect and process, as data controller, when you register on and use the Platform (**Personal Data**). We take your privacy very seriously and ask that you read this Privacy Policy carefully as it contains important information about our processing of your Personal Data and your rights.

We may change this Privacy Policy from time to time. A current version is available on the Platform. Please visit the Platform regularly and inform yourself about the applicable data protection provisions.

B. WHO IS RESPONSIBLE FOR YOUR DATA?

The Cooper Companies, Inc. incorporated and registered in the United States of America with company number 0888132 whose registered office is at 6101 Bollinger Canyon Road, Suite 500, San Ramon, CA 94583, United States of America (**Cooper**) is the data controller of your Personal Data for the purposes of processing set out in Section C of this Privacy policy.

We can be contacted by email at: CooperWellness@cooperco.com or by post using the address set out above.

Where Cooper shares Personal Data with Cooper Affiliates (**Affiliates**, which means our subsidiaries, our ultimate holding company and its subsidiaries), the Affiliates are also data controllers as explained in this Privacy Policy. Details of the Affiliates, including their locations, are listed [here](#).

C. WHAT PERSONAL DATA DO WE PROCESS AND WHY?

We set out below a table below which provides a non-exhaustive list of the types of Personal Data that we collect, the purposes for which we process that Personal Data, the legal basis we rely upon to process such Personal Data and the storage duration.

Data Subject category	Type of Personal Data	Purposes of processing	Legal basis of processing
I. Current and former employees of Cooper and its Affiliates who use the Platform.	1. Registration data <ul style="list-style-type: none"> • Username (HCMID) • FirstName • LastName • Password • Email • Phone number • Country • Building, Department, Company, Locale • Eligibility to participate in the programs 	Providing services in connection with the use of the Platform, including to disable accounts when existing users of the Platform stop using or are no longer eligible to use the Platform.	The processing takes place on the basis of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws. We have a legitimate interest to ensure that the relevant employees have access to and can use the features on Platform and that accounts are disabled when existing users of the Platform stop using or are no longer eligible to use the Platform.
	2. Participation data <ul style="list-style-type: none"> • Steps and activity history (if you sync a wearable) • Data relating to any challenges and chats that you may participate in. If you choose to track the following data on the Platform:	Providing services in connection with the use of the Platform	Your consent (Art 6 Para 1 lit a) GDPR or other similar provisions under other applicable data protection laws

	<ul style="list-style-type: none"> • Wellness goals • Physical activity information, • Sleep and weight information • Fruit and vegetables intake • Hydration details • Energy levels • Digital detox details • Lifestyle Interests <p>Should Health Risk Appraisals be made available on the platform and you choose to take part in them:</p> <ul style="list-style-type: none"> • Height • Weight • waist measurement • blood pressure • cholesterol values 		
	<p>2. Automated data collection when accessing the Platform</p> <ul style="list-style-type: none"> • URL of the page accessed • The latency of the network connection • Date and time 	<ul style="list-style-type: none"> • Load balancing, i.e. to distribute the access to the Platform across several devices and to be able to offer you the fastest possible loading times • Ensuring the security of our IT systems, for example, to prevent 	<p>The processing takes place on the basis of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws.</p>

		<p>specific attacks on our systems and to identify attack patterns</p> <ul style="list-style-type: none"> • Ensuring the proper operation of our IT systems, for example if errors occur that we can only remedy by storing the IP address • To enable criminal prosecution, security or legal prosecution if there are specific indications of criminal offenses 	
<p>II. Employees of Cooper and its Affiliates who are granted administrative rights to the Platform.</p>	<p>1. Registration data</p> <ul style="list-style-type: none"> • Cooper Co Employee ID • First Name • Last Name 	<p>Providing administrative access to the Platform.</p>	<p>The processing takes place on the basis of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws. We have a legitimate interest to ensure that the relevant employees have access to the Platform so that they can administer the Platform.</p>
	<p>2. Automated data collection when accessing the Platform</p> <ul style="list-style-type: none"> • URL of the page accessed • The latency of the network connection • Date and time 	<ul style="list-style-type: none"> • Load balancing, i.e. to distribute the access to the Platform across several devices and to be able to offer you the fastest possible loading times • Ensuring the security of our IT systems, for example, to prevent 	<p>The processing takes place on the basis of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws.</p>

		<p>specific attacks on our systems and to identify attack patterns</p> <ul style="list-style-type: none">• Ensuring the proper operation of our IT systems, for example if errors occur that we can only remedy by storing the IP address• To enable criminal prosecution, security or legal prosecution if there are specific indications of criminal offenses	
--	--	--	--

- **Additional information on 1. Registration data:**

Your registration data is required to set up and manage a user account for you and so that you can use all the features of the Platform and to disable your account when you stop using or are no longer eligible to use it.

In order to have access to and use the Platform, you have to provide us with this data. However, you are not legally obliged to provide the data.

In addition, you may be given the option to provide further voluntary information as part of the registration. This information is voluntary and not necessary to register you. We collect this data in order to be able to provide you with the corresponding functions of the Platform.

The processing takes place on the basis of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws.

- **Additional information on 2. Automated data collection when accessing the Platform**

Personal data also includes information about your use of the Platform. In this context, we use cookies to store your session/login information and track your selected language. You can find more information about cookies below.

D. HOW AND WHEN DO WE SHARE PERSONAL DATA WITH THIRD PARTIES?

a) Data sharing within Cooper group

Cooper may share your Personal Data with its Affiliates:

- where we need to do so in order to provide the services or information that you have requested or provide technical support or maintenance; for example, we may transfer your Personal Data to CooperVision Inc. in the United States of America to handle your basic enquiries and troubleshoot simple issues; or
- internal governance and administration, where necessary; or
- to comply with our legal or regulatory obligations, where applicable.

The legal basis for processing is processing is necessary for the purposes of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws or the processing is necessary for compliance with a legal obligation to which we are subject (Art 6 Para 1 lit c) GDPR or other similar provisions under other applicable data protection laws or.

b) Data sharing with service providers

We share your Personal Data with our third party service providers, whom we engage to provide various services in connection with the Platform:

- provision of software for the Platform;
- hosting and maintaining the Platform;
- provision of technical support for the Platform; and
- IT services and solutions (e.g. providing data storage, assisting us with database management).

CoreHealth Technologies Inc. is the service provider that is currently engaged by us to provide the

software and the hosting and maintenance services for the Platform.

The legal basis for processing the processing is necessary for the purposes of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws.

c) Data sharing with your Buddies

Where you have allowed other users of the Platform to send you Buddy Quick-Add Requests, we will also share your Personal Data with such other users.

The legal basis for processing is that the processing is necessary for the purposes of our predominant legitimate interests (Art 6 Para 1 lit f) GDPR or other similar provisions under other applicable data protection laws.

d) Data sharing with other recipients

We may also share your Personal Data with:

- our accountants, auditors, lawyers or other professional advisers when we ask them to provide us with professional advice;
- any other third party if we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation, or to protect the rights, property and/or safety of Cooper, any of its Affiliates, its personnel and others;
- any other third party for the purposes of acting in accordance with the requirements of a court, regulator or government agency, for example, complying with a court order or acting in accordance with an applicable law or regulation;
- police and other law enforcement agencies in connection with the prevention and detection of crime; or

The legal basis for processing is that the processing is necessary for compliance with a legal obligation to which we are subject (Art 6 Para 1 lit c) GDPR or other similar provisions under other applicable data protection laws).

E. INTERNATIONAL TRANSFERS OF PERSONAL DATA

The transfer of your Personal Data to and between the Affiliates, service providers or other recipients may involve your Personal Data being transferred to a third country/territory that is prohibited by or not deemed adequate pursuant to the data protection laws applicable to that transfer. In particular, your Personal Data will be transferred to the United States of America where the Platform is hosted. Where we transfer Personal Data to such a third country/territory, we will implement appropriate and suitable safeguards to ensure that such Personal Data will be protected as required by applicable data protection laws. For example where your Personal Data is transferred to Cooper Affiliates, the safeguards which we typically put in place are the European Standard Contractual Clauses as permitted by data protection law and in particular Article 46 Para 2 GDPR.

You can request further details about the safeguards that we implement by contacting our data protection officer at: dpo@coopervision.com.

F. HOW LONG DO WE STORE PERSONAL DATA?

It is our policy to retain your Personal Data for the length of time required for the specific purpose or purposes for which it was collected (e.g. for the fulfilment of an agreement with you). However, we may be obliged to store some Personal Data for a longer time, taking into account factors including:

- legal obligation(s) under applicable law to retain data for a certain period of time (e.g. compliance with tax, accountancy or regulatory requirements);
- the establishment, exercise or defence of legal claims (e.g., for the purposes of a potential dispute).

If you would like to find out how long we keep your Personal Data for a particular purpose, you can contact us at: dpo@coopervision.com.

For more information on how long cookies are stored, please refer to our [Cookie Policy](#).

G. HOW DO WE PROTECT YOUR PERSONAL DATA?

We implement technical and organisational security measures to protect your Personal Data against the risk of loss, misuse, or unauthorised alteration or destruction. Such measures may include the use of firewalls, encryption (where appropriate), access rights management processes, careful selection of processors and other technically and commercially reasonable measures to provide appropriate protection for your Personal Data. Where appropriate, we may also make backup copies and use other such means to prevent accidental damage to or destruction of your Personal Data.

Please note however that where you are transmitting information to us over the internet this can never be guaranteed to be 100% secure.

H. YOUR RIGHTS

You have certain rights with respect to your Personal Data under the data protection laws. The rights may only apply in certain circumstances and are subject to certain exemptions. If you wish to exercise any of the below rights, please contact us using the details in the "HOW TO CONTACT US" section. We aim to respond to your request within one month after receiving your request, but we may extend this period with another two months in which case we will inform you of this extension within one month after receiving your request. However, if we are required to respond within a shorter period under applicable laws, we will respond within the period required under applicable laws.

You have the following rights under applicable data protection law with respect to Personal Data concerning you:

- **Right of access to your Personal Data**

You can request information from us at any time about whether and which Personal Data we store about you. The provision of information is free of charge for you.

The right to information does not exist or is subject to limitations if and to the extent that confidential information, such as information that is subject to professional secrecy, would be disclosed.

- **Right to rectify your Personal Data**

If your Personal Data stored by us is inaccurate or incomplete, you have the right to obtain rectification of this data from us at any time.

- **Right to erasure of your Personal Data**

You have the right to request that we erase your Personal Data if and to the extent that the data is no longer needed for the purposes for which it was collected or, if the processing is based on your consent, you have withdrawn your consent. In this case, we must stop processing your Personal Data and remove it from our IT systems and databases.

A right to erasure does not exist insofar as:

- the data may not be deleted due to a legal obligation or must be processed due to a legal obligation;
- the data processing is necessary for the assertion, exercise or defence of legal claims.

- **Right to restrict the use of your Personal Data**

You have the right to suspend our use of your Personal Data in certain circumstances. For example (i) where you think your Personal Data is inaccurate and only for such period to enable us to verify the accuracy of your Personal Data; (ii) the use of your Personal Data is unlawful and you oppose the erasure of your Personal Data and request that it is suspended instead; (iii) we no longer need your Personal Data, but your Personal Data is required by you for the establishment, exercise or defence of legal claims; or (iv) you have objected to the use of your Personal Data and we are verifying whether our grounds for the use of your Personal Data override your objection.

- **Right to data portability**

You have the right (under certain data protection laws, to the extent applicable) to receive from us the data you have provided in a structured, common and machine-readable format, as well as the right to have this data transferred to another controller. This right only exists if

- you have provided us with the data on the basis of consent or on the basis of a contract concluded with you; and
- the processing is carried out by automated means.

- **Right to object to the use of your Personal Data: If the processing of your data is based on Art 6 para 1 lit f) GDPR or other similar provisions under other applicable data protection laws, you may object to the processing at any time.**
- **Right to withdraw consent**
You have the right to withdraw your consent at any time where we rely on consent to use your Personal Data. You can withdraw your consent at any time with effect for the future at no additional cost.
- **Right to complain to the relevant data protection authority**
To the extent that Art 77 GDPR or similar provisions under other data protection laws are applicable, you have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your Personal Data infringes data protection law.

I. THIRD PARTY LINKS

The Platform may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for how they handle your Personal Data. When you leave the Platform, we encourage you to read the privacy notice of every website, plug-in and application you visit or enable connection to.

J. HOW TO CONTACT US

If you wish to request further information regarding this Privacy Policy or the way we use your Personal Data or if you wish to exercise any of the above rights set out in Section H. you can contact our data protection officer at: dpo@coopervision.com.

K. ADDITIONAL COUNTRY AND REGIONAL SPECIFIC PROVISIONS

Where Cooper is subject to certain privacy requirements in the United States in the State of California, the following also applies:

Do Not Track. Your browser may allow you to set a “Do not track” preference. Unless otherwise stated, the Platform does not honor “Do not track” requests. However, you may elect not to accept cookies by changing the designated settings on your web browser or, where available, by referring to our Cookie Policy. Cookies are small text files placed on your computer while visiting certain sites on the Internet used to identify your computer. If you do not accept cookies, you may not be able to use all or certain functions and features of the Platform.

In accordance with the disclosure requirements under the California Consumer Privacy Act (“CCPA”), Cooper we do not (and during the last 12 months, we did not) sell, rent, or trade personal information with third-parties for their commercial purposes.

The CCPA grants you certain rights that you can exercise. This section explains those rights and how to exercise them.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive your request and verify you as the person whose information is being requested (see Exercising Access, Data Portability, and Deletion Rights), we will disclose to you:

- The categories of personal information we collected about you
- The categories of sources for the personal information we collected about you
- Our business or commercial purpose for collecting or selling that personal information
- The categories of third parties with whom we share that personal information
- The specific pieces of personal information we collected about you (also called a data portability request)
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
 - sales, identifying the personal information categories that each category of recipient purchased
 - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained

Deletion Request Rights

You have the right to request us to delete any of your personal information that we collected and retained, subject to certain exceptions. Once we receive and verify you as the person whose information is being requested (see Exercising Access, Data Portability, and Deletion Rights), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities
- Debug products to identify and repair errors that impair existing intended functionality
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.)

- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us
- Comply with a legal obligation
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us toll-free at (855) 526-6737; or
- Making a request at <https://coopervision.com/ccpa-common-request-form>

Only you, or a person that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it

Before assessing any of your requests, we may request additional information in order to verify your identity. If you do not provide the requested information and, as a result, we are unable to identify you, we may refuse to action your request.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We will consider and respond to a verifiable consumer request within forty-five (45) days of its receipt. However, if we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will provide requested personal information in a structured, commonly used and machine-readable format and for it to be transferred to you or another organization, where it is technically feasible.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Where Cooper is subject to the requirements of the Brazilian General Data Protection Law, the following also applies:

Cooper has appointed a Data Protection Officer for Brazil. Written inquiries, requests or complaints to our Data Protection Officer may be addressed to:

Name: Oerton Fernandes de V. e Silva

Email: dpobrasil@coopervision.com

Where Cooper is subject to the requirements of the Personal Information Protection Act of the People's Republic of China, the following also applies:

“Sensitive Personal Data” is Personal Data that, once divulged or illegally used, may easily cause harm to the dignity of natural persons or endanger personal or property safety. According to the functions you actually use and the Platform permissions granted to us, your Sensitive Personal Data processed by us may include your steps and activity history (if you sync your wearables with the Platform), health risk appraisal information, such as your height, weight, waist measurement, blood pressure and cholesterol values (should health risk appraisals be made available to you on the Platform), geographical location information, information about your visits to and use of the Platform. It is necessary for us to process your Sensitive Personal Data in order to perform the specific functions you request from us and for other purposes described in this Privacy Policy. We will process your Personal Data (including Sensitive Personal Data) in a way that has the least impact on your personal rights and interests.

You acknowledge and agree that we will share your Personal Data with other parties, and transfer your Personal Data out of the PRC in accordance with this Privacy Policy, based on your consent or other legitimate legal bases to the extent permitted by applicable laws.

The right to request explanation - You have the right to request us to explain about our rules as to the processing of your Personal Data. If you wish to make such request, please contact us through the contact information provided in this Privacy Policy (See How to Contact Us).

The right to portability - You may request us to transfer your Personal Data that we hold about you to another personal information processor that is designated by you. We will review your request, and if such request meets the requirements under applicable laws, we will duly provide you with the channel for the transfer.

Where Cooper is subject to the requirements of Singapore's Personal Data Protection Act, the

following also applies:

Cooper has appointed a Data Protection Officer for Singapore. Written inquiries, requests or complaints to our Data Protection Officer may be addressed to:

Email: info@sg.coopervision.com