

Privacy Notice

We at Andrina Santoro (“we”, “us”, “our”) respect your concerns about privacy.

This Privacy Notice explains how we use any personal data we collect about you and your rights in relation to the information. "Personal data" means any information that identifies you as an individual or is capable of identifying you as an individual.

For the purpose of applicable data protection laws, including the General Data Protection Regulation (the “GDPR”) and the California Consumer Privacy Act (“CCPA”) the data controller is Andrina Santoro with email address info@andrinasantoro.com.

Information covered by this Privacy Notice

This Privacy Notice covers all personal data collected and used by us.

This includes your name, age, postal address, email address, phone number, credit card number, details of the preferences you express to us, your comments and questions, and technical information from the devices you use to access our website. It also includes information on your body and wellbeing, including height, weight (including information on obesity), body statistics, workouts, mood, meals, nutrition and general health and wellbeing, that you decide to disclose to us on this website or through the use of our app.

Personal Data we obtain

We (and our service providers) collect this personal data from you when you:

- purchase products or services from us, including a coaching subscription.
- submit any information through this website.
- create an account with us, or otherwise sign up for our services.
- opt in to or otherwise receive marketing from us or our representatives.
- choose to participate in our customer feedback surveys.
- communicate with us via third-party social media websites.
- contact us, correspond with us, or otherwise provide information to us.

We also work closely with third parties (such as business partners and analytics providers) and may

receive other personal data about you from those third parties, which we may combine with the information you have provided to us. We process all data we obtain from such other sources in accordance with this Privacy Notice.

When you visit our website, we (and our service providers) may use cookies and other technologies to automatically collect the following information on you:

- technical information, including your IP address, your login information, browser type and version, device identifier, location and time zone setting, browser plug-in types and versions, operating system and platform, page response times and download errors.
- information about your visit, including the websites you visit before and after our website and products you viewed or searched for.
- length of visits to certain pages, page interaction information (such as scrolling, clicks and mouseovers) and methods used to browse away from the page.

How we use the information we obtain

We use the personal data we collect from and about you for the following purposes:

- to set up and manage your online account.
- to provide our services to you, which may include
 - designing tailored meal and workout plans.
 - monitoring changes or adaptations in your body to improve your coaching cycle, and to combine information we receive and collect (e.g. from updates you provide on your body transformation) to provide you with a more personalised experience and to make informed decisions about future coaching to best facilitate your improvement. This also provides vital statistics which we use to better understand the efficacy of different approaches to dieting and workouts.
- to provide you with information about our products and services (provided you have either consented to this or we by other means are allowed to reach out to you for marketing purposes).
- to process your payments, keep internal records and manage our relationship with you.
- to keep our website safe and secure.
- to keep an up-to-date suppression list where you have asked not to be contacted, in order for us to not inadvertently re-contact you.
- to notify you of any changes to our services that may affect you.

The legal bases for which we collect, use, transfer or disclose your personal data include:

- the performance of our contract obligations with you (see article 6(1)(b) of the GDPR).
- our legitimate interests (see article 6(1)(f) of the GDPR), which include: improving our offerings as a business; personalising our services and interactions with you, to better meet your needs as a customer; and detecting and preventing fraud.
- compliance with our legal obligations.
- to the extent we send you information on our products and services for marketing purposes, we will either ask for your consent (in accordance with article 6(1)(a) of the GDPR) before processing your information in this way or process your personal data based on our legitimate interests (in accordance with article 6(1)(f) of the GDPR - the legitimate interests are stated above).

The use of consent for processing of your health data

In order for us to be able to deliver customized meal- and workout plans to you, we may process certain health data provided by you, including information on allergens, information that might reveal obesity or specific injuries or other relevant information related to your physical or mental health status. The legal basis for our processing of your health information is Article 9 (2) a cf. Article 6 (1) b) of the GDPR, which means that we will ask you for your explicit consent to allow us to process your health data prior to you becoming a client with us.

You may at any time withdraw your consent to us processing your health data. However, you should be aware that if we are prevented from processing relevant personal data, including information on any allergens, information that might reveal obesity or specific injuries or other relevant information related to your physical or mental health status, we will not be able to provide you with our services (customized meal- and workout plans based on your unique needs).

Third Parties, including processing by Lenus eHealth ApS

The security of your personal data is extremely important to us. We do not sell your personal data to any third parties, and we never will.

Access to your personal data is only provided to carefully selected third parties, including:

- our service providers who help us to provide our services to you, such as our infrastructure and IT service providers. These include Lenus eHealth ApS and Stripe, who support our business by

providing technical infrastructure services, analysing product performance, providing technical assistance and facilitating payments. We note therefore that Lenus eHealth ApS may process your personal data as data processor on behalf of us. However, Lenus eHealth ApS may also act as an independent data controller in limited cases. You can read more about Lenus eHealth's processing of your personal data as data controller (including cookies) here: <https://lenusehealth.com/privacy-policy/>.

- our regulators, or organisations to whom we are required to disclose your personal data by law.
- third parties connected with business transfers, such as in connection with a reorganisation, restructuring, merger, acquisition or transfer of assets, provided that the receiving party agrees to treat your personal data in a manner consistent with this Privacy Notice.

Our website may, from time to time, contain links to and from the websites of our partners, or affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy notices and that we have no control over how they may use your personal data. You should check the privacy notices of third party websites before you submit any personal data to them.

How long we retain your personal data for

Your personal data will only be stored for as long as necessary for the purposes for which they were collected and only to the extent permitted by applicable laws. When we no longer need to use your information, we will remove it from our systems and records and / or take steps to promptly anonymise it so that you can no longer be identified from it (unless we need to keep your information to comply with legal or regulatory obligations to which we are subject).

We adhere to the retention periods listed in the below table. As a general rule, we erase or anonymise your personal data according to the time limits stated below unless it is necessary that we continue to store them, e.g. for the purpose of particular cases or the like.

Processing purposes	Retention period
Management of your account	12 months after your last activity
Delivery of coaching services	12 months after your last activity

Marketing purposes	12 months after your last activity
E-mails to/from you	6 months after your last activity

Third country data transfers

The personal data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA and who work for us or for one of our service providers.

We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this Privacy Notice and applicable data protection laws, including, where relevant, entering into EU standard contractual clauses (or equivalent measures) with the party outside the EEA receiving the personal data.

Keeping your information secure

We have implemented technical and organisational security measures in an effort to safeguard personal data in our custody and control. Such measures we have implemented include, limiting access to personal data only to employees and authorised service providers who need to know such information for the purposes described in this Privacy Notice, as well as other technical, administrative and physical safeguards.

While we endeavour to always protect our systems, sites, operations and information against unauthorised access, use, modification and disclosure, due to the inherent nature of the Internet as an open global communications vehicle and other risk factors, we cannot guarantee that any information, during transmission or while stored on our systems, will be absolutely safe from intrusion by others, such as hackers.

To provide you with increased security, certain personal data stored in your online account is only accessible via your username and password. You are responsible for maintaining the confidentiality of your online account credentials, and we strongly recommend that you do not disclose your online account username or password to anyone. We will never ask you for your password in any unsolicited communication. Please notify us immediately (see "Contact us" section below) of any unauthorised use

of your online account credentials or any other suspected breach of security.

Your Personal Data Rights

You have various rights in connection with our processing of your personal data:

- Access. You have the right to request a copy of the personal data we are processing about you, which we will provide back to you in electronic form.
- Rectification. You have the right to have incomplete or inaccurate personal data that we process about you rectified.
- Deletion. You have the right to request that we delete personal data that we process about you, except we are not obligated to do so if we need to retain such data in order to comply with a legal obligation or to establish, exercise or defend legal claims.
- Restriction. You have the right to restrict our processing of your personal data where you believe such data to be inaccurate, our processing is unlawful or that we no longer need to process such data for a particular purpose. Where we are not able to delete the data due to a legal or other obligation or because you do not wish for us to delete it, we would mark stored personal data with the aim of limiting particular processing for particular purposes in accordance with your request, or otherwise restrict its processing.
- Objection. Where the legal justification for our processing of your personal data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for the processing which override your interests and rights, or if we need to continue to process the data for the establishment, exercise or defence of a legal claim.
- Withdrawing Consent. Where we process certain personal data on the basis of your consent, you have the right to withdraw your consent, including with regard to direct marketing. In relation to the consequences of your withdrawal of consent for us to process your health data, please see above under "The use of consent for processing of your health data".

If you wish to exercise one or more of the above rights, please contact us with your request at info@andrinasantoro.com, and include your name, email and postal address, as well as your specific request and any other information we may need in order to provide or otherwise process your request.

In some situations, we may refuse to act or may impose limitations on your rights, as permitted by law. Before we can provide you with any information or correct any inaccuracies, we may ask you to verify your identity and/or provide other details to help us respond to your request. For the exercise of your rights, please contact us using the contact information provided below in the "How to Contact Us" section.

In all cases, you have a right to file a complaint with your local data protection authority if you believe that we have not complied with applicable data protection laws.

United States - California

If you are a consumer located in California, we process your personal data in accordance with the California Consumer Privacy Act (CCPA). This section provides additional details about the personal information we collect and use for purposes of CCPA.

a. How We Collect, Use, and Disclose your Personal Information

The **Personal Data We obtain** section describes the personal information we may have collected about you within the last 12 months, including the categories of sources of that information. We collect this information for the purposes described in the **How we use the information we obtain** section. We share this information as described in the **Third Parties, including processing by Lenus eHealth ApS** section.

b. Your CCPA Rights and Choices

As a California consumer and subject to certain limitations under the CCPA, you have choices regarding our use and disclosure of your personal information:

- **Exercising the right to know:** You may request the following information about the personal information we have collected about you:
 - the categories and specific pieces of personal information we have collected about you;
 - the categories of sources from which we collected the personal information;
 - the business or commercial purpose for which we collected the personal information;
 - the categories of third parties with whom we shared the personal information; and
 - the categories of personal information about you that we disclosed for a business purpose, and the categories of third parties to whom we disclosed that information for a business purpose.
- **Exercising the right to delete:** You may request that we delete the personal information we have collected from you, subject to certain limitations under applicable law.
- **Exercising the right to opt-out from a sale:** You may request to opt out of any “sale” of your personal information that may take place. We do not use, share, rent or sell the personal information of our customers for interest-based advertising. We do not sell or rent the personal information of our customers or our site visitors.

- **Non-discrimination:** The CCPA provides that you may not be discriminated against for exercising these rights.

How to contact us

If you have any questions about this Privacy Notice and/or about the privacy policies and practices of our service providers, please contact us at info@andrinasantoro.com.

Last updated: 5/21/2021