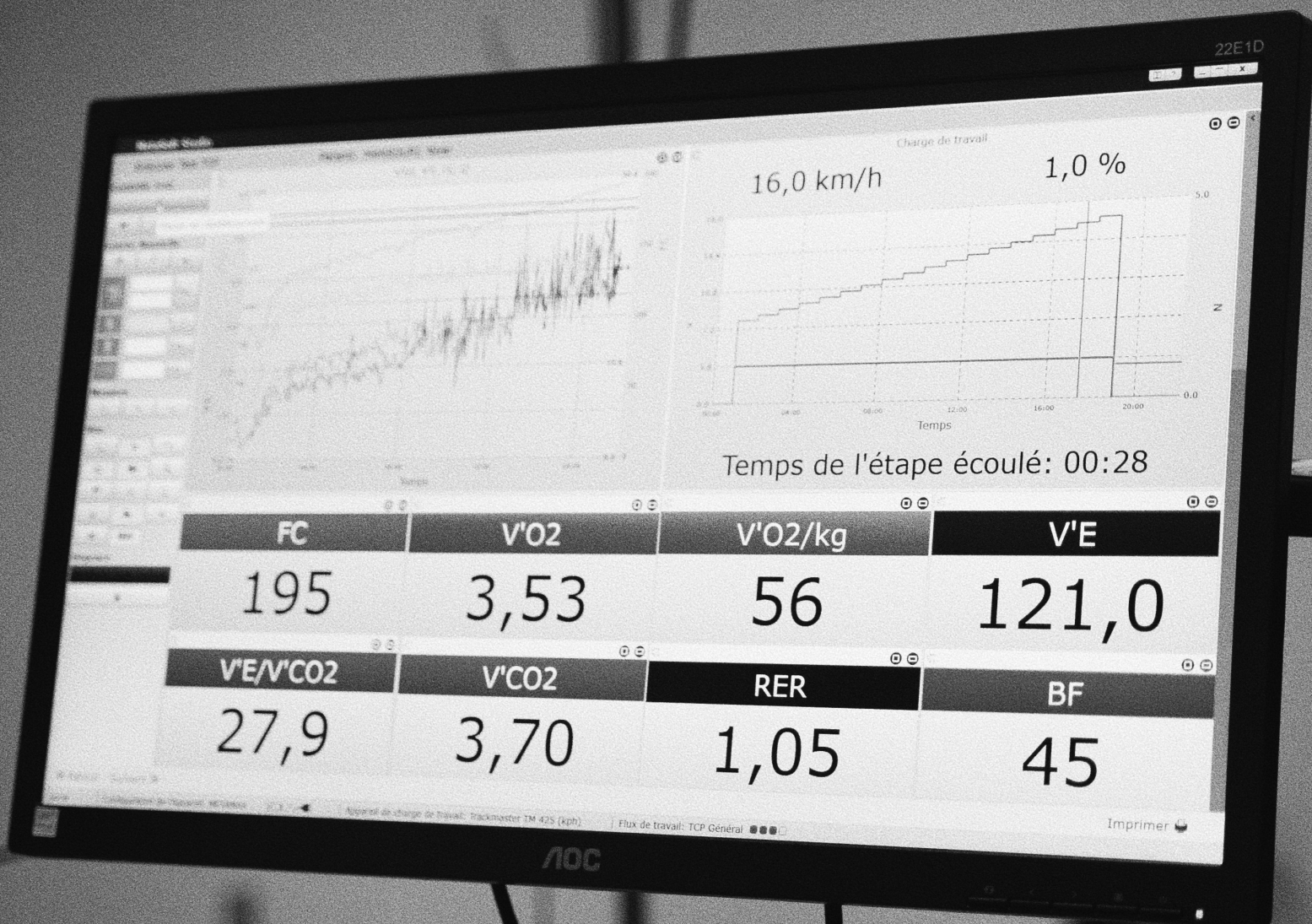




VERSTARCARE CONFIDENTIALITY STATEMENT

This is the privacy statement of VerstärCare and all its Partner Clinics worldwide.

Responsible for the processing of personal data:

Our head office - VerstärCare - Itxaropena Arima SL

Calle Luis Martínez 21

39005 Cantabria, Spain

Registered in the Spanish Commercial Register under Chamber of Commerce number

We will begin this statement with an overview of your contact details so that you can exercise your privacy rights.

This is followed by a detailed explanation of the categories of personal data we process and why and how we do so.

1. CONTACT INFORMATION

What is it used for?	For whom	Where to go
Privacy rights Deletion Rectification Access Data portability Questions	Members Customers	You can contact us at: • customer service (via the website), or • chat with us to be redirected, or • send an email directly to privacy@verstarcare.com We will respond to your request within a maximum of 4 weeks.
This is a fine for access fraud. File an objection against the fine. Request access to the photo from the turnstile.	Members	Request access to the photo or file an objection to the fine by sending an email to: privacy@verstarcare.com

Incidents/violations When evidence is required, such as camera footage or data on potential violations or in the event of serious incidents.	Police or other relevant public institutions	The police or other relevant public institutions can contact: privacy@verstarcare.com Please note! <u>Requests for images from members sent to these email addresses will not be answered!</u> Members cannot request images of other people, such as perpetrators or potential offenders, on the basis of the GDPR. If you are a victim, you must first notify the police, after which the police are authorized to request this information from us.
Regarding investigations, violations, questions, or complaints related to the GDPR.	Data protection authorities, members, and customers.	Contact our data protection officer at privacy@verstarcare.com
Regarding confidential medical documents	Medical Data	Secure document delivery via medicaldocuments@verstarcare.com

2. CATEGORIES OF PERSONAL DATA

2.1 Subscription data

By becoming a member of VerstärCare, you will enter into a subscription agreement. In order to provide you with our fitness services, we need to process certain personal data that you provide to us during the subscription process. This includes your name, home address, phone number, email address, bank account number, gender, and date of birth. We will provide you with your subscription number and your VerstärCare access details

When you subscribe, we record your visits to our Application, your payments, your subscription type, and the number of options you have chosen, such as “Sessions Specific Training.” We also record our communication with you if you contact us with questions or issues related to your subscription via Chat.

2.2 My VerstärCare Account

VerstärCare offers its members an online environment where you can access your own personal data and subscription information by logging in with your password.

The data in the VerstärCare app shows the data as recorded in our subscription management system. You can log in via the VerstärCare app. You can also adjust certain data or settings yourself at any time.

2.3 VerstärCare app

Our app is designed to support our members in their fitness journey, provide them with a self-service tool to manage their membership, and inform them about our services and products. Most of the data visible in the app displays your account information. After activating an account, you can customize the app as much as you like, based on your own goals and interests. If you do not wish to customize the app, you can simply skip these questions. We can distinguish the following categories of personal data in our app:

1. Data for creating an account and using the app

If you are a VerstärCare member, you can easily install and log in to the app by providing your VerstärCare membership credentials. Your subscription data, normally visible in VerstärCare, will automatically be visible on your app.

2. Data to achieve your fitness goals and personalize your app

Our app can help you achieve your fitness goals if you wish. Therefore, you can add information such as your height, weight, goals, interests, fitness preferences, and scheduled and completed workouts. Your BMI will be calculated automatically. You can also use the Body Analyzer (Smart Scale) at a Partner Facility, and the results will automatically be visible in the app.

3. Other additional options

The app allows you to upload a profile photo, which you can delete or change at any time; this photo is also visible to your friends and your online personal trainer.

It also offers a personal coaching dashboard, virtual lessons, product/sports nutrition recommendations, dietary advice, and recipes. We also offer a “Location” option where you can give permission to use your geolocation data. VerstärCare does not store location data.

4. Analytical data.

We analyze app usage to improve its functionality and security, as well as for personalization and marketing purposes. We analyze using a unique identifier that can only be interpreted by VerstärCare and do not use any user or device data for this purpose. VerstärCare uses Google/Apple analytics and has entered into a data processing agreement with Google in this regard. Google uses device data such as the IMEI number for identification purposes.

5. Application security

Application data and personalized Body Analyzer data are stored in pseudonymized form in a separate secure database. This database itself does not contain any data that can be linked to an individual. This data is not stored in our member management system and is only visible to the app user themselves on their own device. All data traffic relating to the app is secured using encryption techniques.

2.4 Online Coaching

App users can take advantage of an online personal coaching program, thanks to our personal coaches, who will guide you throughout your subscription to help you achieve your fitness goals. This feature is only available to Members. A chat function is available for coaching. These discussions are intended solely for the online coaching period and will not be used for any other purpose. Chat messages will be deleted 2 months after the end of the coaching period. Only in the event of a complaint regarding the coaching period may the discussions be kept for a little longer, i.e., up to 2 months after the complaint has been processed.

2.5 Access

We offer the option of granting access with personal codes on your own device. In order to ensure that Access works properly, to secure it, and to prevent fraud (Access is personal and cannot be transferred to anyone else), we process your device ID. A device ID is a string of numbers and letters that uniquely identifies a mobile device.

2.6 Body Analyzer

The Body Analyzer. This is a special smart scale that measures several parameters: body weight and body composition, such as fat mass, muscle mass, bone mass, and body water. Once the Body Analyzer has been used, the results are automatically displayed on the Body Analyzer screen and must be sent to us.

It will be included in your application profile. The Body Analyzer data is stored in a separate, secure, and pseudonymized database. This database itself does not contain any data that can be linked to an individual. VerstärCare does not store this information in its member management system.

2.7 Marketing, sales, and communication

During the subscription process, you can choose your marketing settings. During your VerstärCare subscription, you can adjust your settings at any time via the unsubscribe link provided in our communications. Depending on your choices and settings, VerstärCare will send you emails, text messages, or notifications on your app.

With regard to the necessary information concerning the subscription, prices, etc., we do not communicate on the basis of consent, but on the basis of the proper execution of the contract with our members and the importance of the information concerning certain issues.

For marketing and communication purposes, VerstärCare uses personal data to select the correct target group, such as the relevant club, country, region, etc. VerstärCare does not engage in profiling that leads to automated decision-making.

2.8 Surveys

We sometimes contact our members to participate in a survey in order to improve our services. This is always voluntary and only with the member's consent. We also clearly indicate in advance whether the survey is anonymous or not.

2.9 Camera protection

We have cameras in and around our clinics, but we use the images for limited security purposes. We are aware that camera protection also affects the privacy of our members and employees, which is why we monitor it with the utmost care. For example, there is no camera protection in the changing rooms or sanitary facilities. Camera surveillance is only used reactively for alarm verification purposes. To learn more about how our camera security system works, please see our camera protection policy on our website.

2.10 Access fraud

VerstärCare has included in its terms and conditions that it is not permitted to grant another person access to the app. A fine (the value of a subscription at its full price + additional administrative costs) will be charged. If access fraud occurs repeatedly, the subscription may be terminated. The member (access owner) will receive an email from us requesting payment of the fine.

2.11 Official warnings or bans from the Clinic

When members do not comply with the rules and regulations, cause nuisance, behave inappropriately, or put our specialists/partners or other members at risk, we may send the member an official warning or ban them from accessing the Application or the Clinic. The Clinic employee on duty will note the time, location, and details of the incident. Our customer service department will evaluate this report and determine whether further investigation is necessary. For example, checking camera footage or interviewing witnesses. A warning or ban from the App/Clinic will be sent to the member and the case will be recorded in our member system. In the event that the member is banned from the club, their name, email address, phone number, and IBAN will be included in an internal list to prevent the member from re-registering with VerstärCare App for a period of 2 years following the end of their membership due to expulsion.

2.12 Payment issues

When a member fails to pay the subscription fee, payment reminders are initially sent by email. If there is no response, a reminder will be sent by SMS to the phone number specified by the member. If there is still no rectification or payment, the case will be transferred to the collection agency. At that point, the collection agency becomes the “data controller” of the data we transfer to them for further processing of the case. The data will be processed and stored in accordance with the relevant procedures and regulations to which collection agencies are subject.

2.13 Social media

VerstärCare uses social media such as Facebook, Instagram, LinkedIn, and TikTok, with its own profile page. Through these channels, you can follow VerstärCare and respond to our communications and information feeds. The privacy policy of the relevant platform applies to this.

You can also contact us via our private messaging service with any questions or issues regarding your subscription after identifying yourself as one of our members. These private messages will be handled by our customer service or marketing experts via our own member system. This means that we centralize all our communications via different channels in our member system. Information regarding your subscription will only be communicated via the private messaging option and never via public messaging.

2.14 Analysis and (market) research

VerstärCare only uses anonymized aggregate data for statistical analysis, management reports, and market research purposes. We may select certain target groups for marketing content based on data such as country, region, and subscription type. We want members to receive only content that is relevant to them.

2.15 Clinic intercom calls

The intercom is intended for use only in the event of an emergency or incident in the Clinic. An intercom call with our 24/7 intercom team may be recorded for training purposes.

It will be kept for a maximum of one month and you will be informed in advance by a message that the call will be recorded. When you call our intercom, our intercom agent can see you on camera via a live connection.

This allows you to show your ID card, or in an emergency, the intercom agent can monitor your immediate surroundings for your safety. You have the right to cover the camera with your hand if you do not want to be visible to the intercom agent.

2.16 Website and cookies

You can read about the types of cookies used by VerstärCare for its websites in the VerstärCare cookie statement on our website. In the cookie banner that appears when you open our website, you can choose your own settings. Only necessary functional cookies are enabled by default.

2.17 Personal trainers

Our personal trainers are professionals who work on a freelance basis and are often hired by us on a service contract basis. Occasionally, we enter into service contracts directly with independent personal trainers. The Head Trainer (or independent personal trainer) is required to enter certain personal data via our partner portal, including name, photo, and level of knowledge/experience. This data is published on our website and in the app so that our members can choose a personal trainer based on their fitness goals. In most European countries, we are also required to provide information about our personal trainers' qualifications and certifications. In addition, VerstärCare registers personal trainers in the access management system in order to issue them with access codes. When the service contract is terminated, the personal trainer's data is no longer accessible. The data will be deactivated and shielded in our system, and automatically deleted after two years. Regarding the rights of access, rectification, and deletion of this personal data, we refer personal trainers to their Head Trainer, as they are responsible for updating this data.

2.18 Specialists/Group Course Instructors

Our specialists and group course instructors work on a freelance basis, as freelancers or are employed directly by VerstärCare. Depending on the situation, they can exercise their privacy rights with the agency they work for or through VerstärCare's human resources department. Data retention periods depend on the relevant national labor and tax law regulations. They generally vary between 2 and 5 years after the end of the contract. In addition, VerstärCare registers specialists and group course instructors in the access management system in order to issue an access code (the retention period for this specific data is 2 years after the end of the contract).

3. WHAT ARE OUR LEGAL BASES AND THE PURPOSES OF PROCESSING?

We can only process your personal data if there is a legal basis for this data in accordance with the GDPR. We rely on the following principles:

Data necessary for the membership contract and the services we offer. The legal basis is Article 6 (1) (b) of the GDPR; "processing is necessary for the performance of a contract."

- Additional data, such as your height, weight, BMI, fitness goals, or other similar information, is used solely to create a fitness profile for you in order to offer you personalized content and help you on your personal fitness journey. This processing is based on Article 6(1)(a) of the GDPR: "the data subject has given consent to the processing." This means that you can easily request that your data be deleted.

- When it comes to our marketing and sales activities for our own products and services, the legal basis is Article 6(1) (f) of the GDPR: "for the purposes of the legitimate interests pursued by the controller." We always offer the right to object to this by giving you the option to unsubscribe during the subscription process or at any time by sending a written request to the following email address: support@verstarcare.com and via the unsubscribe links in our communications.

- With regard to our marketing and sales activities related to our partners and third parties, the legal basis is Article 6 (1)(a) of the GDPR: “the data subject has given consent to the processing.” These settings are optional by default, and you can activate them yourself when you subscribe via the Application.

4. HOW DO WE PROTECT YOUR DATA?

VerstärCare takes appropriate measures to protect personal data against loss, unauthorized access or modification, or any other form of unlawful processing.

We do this through physical, technical, and organizational measures. The measures vary depending on the system or data collection, based on the specific risks. For example, data transfer between the website and the VerstärCare app is encrypted, and data is secured through a 2FA authentication system. In terms of organizational measures, we have an information security management system, an internal control framework, and a GDPR compliance program. We also regularly conduct risk assessments, security tests, pen tests, and audits.

5. DATA RETENTION

After you cancel your subscription, we will automatically delete all your personal data and your subscription after 2 years. You will no longer have access unless you subscribe again, up to 1 year after the termination of your first subscription (and so on for any future subscriptions). Your app data will be automatically deleted 2 months after your subscription is terminated and the app is deleted from your device. Subscription payment data is retained for longer in accordance with national tax legislation. This data is stored in pseudonymized form and cannot be used for any other purpose.

6. THIRD PARTIES OR TRANSFER OUTSIDE THE EU

When VerstärCare outsources processing to a subcontractor, security and confidentiality standards are always assessed and a data protection agreement is concluded. Member data is not processed or stored outside the EU and is never sold to third parties. With the exception of Google Analytics, which is based in the United States, we use the privacy settings of Google Analytics and conclude the necessary “Standard Contractual Clauses” provided by the European Commission.

7. COMPLAINTS – DATA PROTECTION AUTHORITIES

If you have a complaint regarding your privacy, you should first contact VerstärCare's data protection officer (privacy@verstarcare.com). If you feel that your complaint is not being handled properly, you can also file a complaint with the data protection supervisory authority in your country. Our main supervisor is based in Spain, as our headquarters are also based in Spain and our data processing mainly takes place there. You can find an overview of all relevant data protection authorities here.

Spain

Agencia Española de Protección de Datos
www.aepd.es