Privacy Statement - OxyCity
CompuFit – BE03

1. Organization of data protection and assignment of responsibilities for data protection

The careful protection of personal data of its customers is one of the core values of CompuFit BVBA (hereinafter referred to as CompuFit). CompuFit BVBA commits to strict compliance with all relevant laws and regulations concerning the storage and processing of personal data.

CGM SE, the parent company of CompuFit, has established a central data protection management system ensuring a consistent high level of protection of personal data and compliance with corresponding data protection laws across all CGM companies.

This Privacy Statement provides information about the handling of data within CompuFit. This data protection statement specifically refers to OxyCity.

At any time, you will have access to the latest version of this Privacy Statement within OxyCity itself.

The data protection statement for the website can be opened and retrieved via the following link: https://www.oxycity.be/PrivacyStatement_en.pdf

2. OxyCity

OxyCity is a patient platform allowing you to access multidisciplinary practices (search for healthcare providers, online booking of appointments, exchange of parameters, …). OxyCity offers dedicated user rights management allowing you to determine the data you want to share and with which practice/healthcare provider.

3. Processing of personal data by CompuFit

"Personal data" means any information relating to a natural person (human being). It concerns all persons who can be identified, directly or indirectly, with the information available to us, such as a name, an identification number, location data, an online identifier or informations about the physical, genetic, mental, economic, social or cultural identity of that natural person.

When using the proposed products and/or services, the following types of data are stored by CompuFiton our server:

- **Registration data**
- **Data from technical operations**

In accordance with data protection laws, we are obliged to delete all registration data, log data and data from technical operations after termination of your membership.

If you decide to terminate your membership, all data that you entered yourself, will be deleted. Data that you eventually have already exchanged with your healthcare providers (appointments, parameters, …), are NOT deleted, in the interest of your health record. For that, you need to contact the corresponding healthcare provider(s).

3.1 Registration data

Registration data identify and manage the relationship between you, your healthcare providers and CompuFit. This data includes:

- Data related to yourself
  - Name
  - E-mail address
  - Password

Non-mandatory information which may be added

- Address
- Gender
- Date of birth
- eID data
- Language
- Telephone number (private)
- Telephone number (mobile)

Storing and processing personal data disclosed to CompuFit during the membership serves and is limited to the purpose of services and customer support.

Data will not be transferred or sold to any third party, unless explicitly permitted by means of a consent declaration. As an example, it may be necessary for CompuFit to transmit contact data to a healthcare provider when making an appointment.

Registration data are stored in the private cloud of CompuFit.

You have the right to be informed about your data stored, the right to rectification, the right to restriction of processing and the right to erasure of this data. You can find more information about your rights below under the title "Your rights".

3.2 Data from technical operations

Data from technical operations is needed for the provision of services. CompuFit collects data from technical operations only for this purpose. CompuFit regularly examines that only data that is required to provide and enhance the technical operations of your product / services are collected, stored and processed by CompuFit.

Data from OxyCity is only collected by CompuFit after declaring your consent.

When using our online services, the following data required to maintain system integrity and security is stored temporarily by CompuFit:

- IP address of the client computer
- Access date and time
- Operating system
- Browser + version
- Screen resolution
- Model of device

Data from technical operations is stored in the private cloud of CompuFit. Data collected while using our online services is deleted within a period of 365 days after the end of the membership.

4. Processing of personal data by OxyCity on the servers of CompuFit

- Your master data
- Other data
  - Appointments
  - Sensible data

This data is stored in the private Cloud of CompuFit.

4.1 You rmaster data

Your master data is stored to allow the relationship with your healthcare providers (online booking system, overview unpaid invoices, messages, …). Mandatory master data in OxyCity is marked accordingly. These master data includes:

- Name
- E-mail
- Address
- Gender
- Date of birth
- eID data
- Language

Master data is needed when using different software modules to execute actions and it is utilized automatically. The transmission to third parties is carried out after prior consent declaration or user interaction. Rectification, restriction of processing or erasure of this data is possible but data that eventually has already been exchanged with your healthcare providers (appointments, parameters ,…) are NOT deleted in the interest of your health record. For that, you need to contact the corresponding healthcare provider(s). Descriptions concerning the rectification, restriction of processing or erasure of data are part of the latest version of the user manual.

4.2 Other data

The storage, use and processing of your data is only permitted with your consent. Your data is not automatically generated in OxyCity. Tour data are collected and registered in OxyCity by the practice respectively by the healthcare provider/the personal working at the practice or yourself.

Appointments: Your appointments are stored and manually registered by yourself or your healthcare providers.

A distinction is made between data necessary (mandatory) for the services on one hand and additional non-obligatory data disclosed by you on the other hand.

Mandatory information include:

- Date and time
- Duration
- Agenda
- Practice
- Discipline

Non-obligatory additional data include:

- Patient photo
- Telephone number
- Date of birth
- Address data (street, house number, postal code, city, country)
- Description of demand of care/disorder/problem
- Extra additional information

Sensitive data: Medical data are a special category of personal data and are subject to higher protection by data protection regulation.

Integrating data into the patient's medical record are derived from the legal obligation of the attending healthcare provide to document all measures and respective results relevant to the current and future treatment of the patient.

This data includes:

- Gender
- Parameters (BMI, heart rate, weight, …)
- Disorder, demand of care
- Reason consultation
- Appointment data
- Exercise programs
- Messages
- Invoice data such as:
  - Invoices
  - Payment data

Rectifications and changes to your record are possible. The original content is accessible and may be consulted if need be. Erasure is possible within the limitations of legal retention periods. Export of data is possible (data portability) in a structured, commonly used and machine-readable format and can be handed-out to you upon request. The corresponding procedures and functionalities are described in the manual of OxyCity.

5. Data transmission / transfer

Electronic data transfer is carried out by OxyCity only after user interaction or automatically - if permission has been granted.

Electronic data transfer based on consent

Exchange of data with a healthcare provider when making an appointment or adding a parameter.

Import of Fitbit data if configured by you.

6. Commitment to confidentiality, trainings on data protection

OxyCity has been extended with different functionalities so that you can work in conformity with the GDPR.

The staff working at CompuFit has signed a confidentiality clause. Strict procedures have been drawn up to impose GDPR compliancy. These procedures are continuously updated. Yearly, refresher courses on GDPR are organized for the staff.

7. Security measures / risk avoidance

CompuFit takes all necessary technical and organizational security measures to protect your personal data from unauthorized access, alteration, disclosure, loss, destruction and other forms of abuse. These measures include internal screenings and checks of our processes for data collection, storage and processing as well as security measures to protect IT systems on which we store contractual data and data from technical operations from unauthorized access.

8. Technical and organizational measures

To ensure data security CompuFit regularly reviews the state of the art of security technologies. This includes determining typical damage scenarios, deriving corresponding security needs / levels of security for different types of personal data, clustered by categories of possible damage as well as carrying out risk assessments.

Further on, dedicated penetration testing is performed to regularly test, assess and evaluate the effectiveness of these technical and organizational measures ensuring the security of the processing.

The following guidelines shall govern the implementation of appropriate technical and organizational measures:

- **Data backup**

  In case of databases, a partial backup is made every hour and a complete backup every week.

- **Privacy by design**

  CompuFit ensures that data protection / privacy and data security principles are taken into account throughout the design and development processes of IT systems.

  The goal is to prevent costly and time consuming additional programming that would be required if data privacy and security requirements had to be implemented after deployment of IT systems. Measures like deactivation of certain software features, authentication or encryption are taken into account at the beginning of the development process.

- **Privacy by default**

  CompuFit products come with factory settings that are optimized for data privacy, so that only personal data necessary for the respective purpose is processed and configurable security options are set by default as a safe value.

- **Communication by e-mail (OxyCity/CompuFit)**

  In case you want to contact CompuFit by e-mail please be aware that privacy of the transmitted information cannot be guaranteed as the content of e-mails may be seen by third parties. We recommend not to use e-mail whenever you want to transmit confidential information.

9. Your rights

Your personal data

You have the right to be informed about data stored about you as well as the right to access this data, you have the right to rectification, to erasure, to restriction of processing, to data portability and the right to object to processing of your personal data.

You have the right to withdraw your consent at any time. The withdrawel takes effect for the future.

You have the right to lodge a complaint with the responsible supervisory authority if you think that we are processing your data inappropriately.

We commit to deleting all data, log data and all data from technical operation after termination of your membership without your prior request.

Data that eventually has already been exchanged with your healthcare providers (appointments, parameters ,…) are NOT deleted in the interest of your health record. For that, you need to contact the corresponding healthcare provider(s).Data from technical operations is stored only as long as technically necessary and is deleted at the latest after termination of your membership.

10. Enforcement

Compliance with the data protection rules described herein is examined regularly and continuously by CompuFit.

Should CompuFit receive a formal complaint, the company will contact the complainant in order to resolve any concerns related to the processing of their personal data.

CompuFit commits to working cooperatively with the competent administration including the supervisory authority.

11. Amendments to this privacy statement

This privacy statement will be subject to amendments and supplements in the future. We will identify each new version of this privacy statement by its date and version number in the footer of the statement.

12. Responsible for CompuFit

Rik Lingier, Elisabethlaan 441, 8400 Oostende

Data Protection Officer

Please contact the Data Protection Officer for questions related to the processing of your personal data and for the reception of your information requests or complaints. Fred Hilgers: dpo.be@cgm.com

13. Competent Supervisory Authority

The competent supervisory authority for CompuFit is

Commission for the protection of privacy https://www.privacycommission.be

Rue de la Presse 35, 1000 Brussels