

1. Organisation and Allocation of Responsibilities in Data Protection

CompuGroup Medical Software GmbH considers the responsible handling and respect for the protection of personal data to be its highest principle. Software GmbH always ensures strict compliance with all relevant laws when storing and processing personal data.

CompuGroup Medical SE & Co. KGaA, as the parent company, has introduced a central data protection management system that guarantees a uniform and high level of protection of personal data within all CGM companies and ensures compliance with the relevant data protection laws. With this data protection declaration, we fulfil our information obligations and provide you with information about the handling of data at CGM. This Privacy Policy applies to CGM DATASAFE. You will always find the latest version of this Privacy Policy in CGM DATASAFE itself and on the CGM DATASAFE website.

The privacy statement for the website can be found [here](#).

2. CGM DATASAFE

CGM DATASAFE is a cloud backup solution. With the help of CGM DATASAFE customers can store data, especially of the CGM information systems as well as additional CGM add-on products. These backups are stored locally on the customer's computer and on servers of CompuGroup Medical SE & Co. KGaA. The doctor has the possibility to restore and view his local and cloud data with the help of CGM DATASAFE. All data backups of a customer, which are on the system of CompuGroup Medical SE & Co. KGaA, are encrypted. CompuGroup Medical has no possibility to see the content of these backups.

3. Processing of personal Data by CGM

Personal data is individual information about personal or factual circumstances of a specific or determinable natural person. CGM Software GmbH stores the following types of data on its servers when using CGM DATASAFE:

- Contract and registration data
- Technical operation data
- Anonymized data

In accordance with the Data Protection Act, we undertake to delete all contractual data, all protocol data and all data relating to technical operation after the termination of your contract. However, we are legally obliged to observe commercial and tax retention periods which may extend beyond the duration of the contractual relationship. Data relating to technical operation will only be retained for as long as is technically necessary but will be deleted at the latest after the termination of your contract.

3.1 Contract and Registration data

Contract and registration data are used to assign and support a contractual relationship concluded between the practice and Software GmbH. These data include:

- Salutation / Title
- First name / Surname
- Gender
- Date of birth
- Email address

Personal data disclosed within the scope of the contractual and business relationship shall only be stored and processed by CGM to the extent that is necessary for the execution of the contract, in particular for order processing and customer service. This data may also be used for product-related surveys and marketing purposes only with the prior consent of the affected.

The passing on, sale or other transmissions of personal data to third parties does not take place unless this is necessary for the purpose of contract processing or explicit consent is given. For instance, it may be necessary to pass on the address and the order data to sales and service partners when ordering products.

The contract data is stored on the CGM server in Germany. You have the right to receive information about your stored data and to demand a correction, blocking or deletion of this data.

3.2 Cookies

Use of Cookies

"Cookies" are small files that allow us to store specific information related to you, the user, on your computer while you are visiting our website. Cookies help us to gather information about the frequency of use and the number of visitors on our website, as well as enhancing ease of use and efficiency for you as a user. The purpose of using these cookies is to provide you with optimal user guidance as well as to "remember" you to be able to present you the most varied internet page and new content when you visit us next time. The content of a cookie is limited to an identification number. Name, IP address, etc. will not be stored. An individual profile of your usage behavior does not take place.

Session Cookies

On our website we use temporary or transient cookies (so-called session cookies). Session cookies are stored exclusively for the duration of your use of our website. Session cookies serve exclusively to identify you during your visit to our website. Session cookies are deleted at the end of each session.

Session cookies are absolutely necessary for the function of our website and cannot be deactivated. You can set your browser to block session cookies or to notify you of their use. However, some areas of the website may not work. Session cookies are used in accordance with Art. 6 Para. 1 lit. f) DSGVO.

3.3 Technical operation data

Technical operation data is required to be able to provide the services guaranteed in a contract. CGM collects data for the technical operation only for this purpose and regularly checks that only the data necessary to provide and improve the technical operation of its products/services is collected, stored and processed. Data will only be collected on the practice system if you give the CGM the permission to do so.

If you use our online services, the following data will be temporarily stored for the purpose of system security:

- Domain names
- The IP address of the requesting computer
- The access date or time
- The file request of the client (file name and URL)
- The number of bytes transferred during the connection.

The data for technical operation is stored on the CGM server in Germany. Data collected during the use of the online services will be deleted within 365 days. As a rule, IP addresses are not stored.

3.4 Statistical Data

In addition, the following statistical data is collected within the framework of the use of CGM DATASAFE:

- Day/time of the last log-in
- Version information
 - o CGM DATASAFE Version
 - o Operating system
 - o Host/computer name
- Local hard disk information (per hard disk)
 - o Memory size
 - o Size of the memory used
 - o State of the hard disk
- Online Storage Information
 - o Size
 - o Used memory
 - o Free memory
- Last online backup
 - o Job name
 - o Size of the backup
 - o Number of files
- Last execution (day/time)
 - o Status of the last execution

The data is used in particular for a statistics platform (CGM DATASAFE Statistics) in order to minimize the control effort of the user of CGM DATASAFE. The data remains on the servers of CompuGroup Medical for the duration of the contract. After termination of the contract, these will be deleted within 4 weeks.

4. Data Transfer

CGM DATASAFE will not transfer data to a third country without the express consent of the data subject. A transfer may take place in the context of an internet speed test after the data subject has given his or her consent. In this case, a small file with neutral content will be uploaded to a European server and downloaded again. The Internet speed test is carried out by OOKla LLC.

5. Commitment to confidentiality, data protection training

Patient data, in particular, health data, are obligated to confidentiality and the requirements of data protection laws (GDPR) but also to strict requirements from the Criminal Law (StGB) and the Social Law (SGB) and are treated with particular sensitivity by CGM.

We restrict access to contract data, protocol data and technical operation data to CGM employees and contractors for whom this information is absolutely necessary in order to provide the services under our contract. These persons are obliged to comply with this data protection declaration and confidentiality obligations (DSGVO, §203 StGB). The violation of these confidentiality obligations can be punished with termination and prosecution. Employees are regularly trained in data protection.

6. Safety measures/avoidance of risks

CGM takes all necessary technical and organizational security measures to protect your personal data as well as your customer data (patient data) against unauthorized access, unauthorized changes, disclosure, loss, destruction and other misuses. This includes internal checks of our approach to data collection, storage and processing, as well as security measures to protect against unauthorized access to systems on which we store contract data or data for technical operation.

7. Technical and organisational measures

In order to guarantee data security, CGM regularly checks the state of the art. Among other things, typical damage scenarios are determined and then the need for protection for individual personal data is derived and divided into damage categories. In addition, a risk assessment is carried out. Furthermore, differentiated penetration tests are used to regularly review, evaluate the effectiveness of these technical and organizational measures to ensure the security of the processing. The following principles are standardized for the implementation of suitable technical and organizational measures:

Backup

To prevent data loss, the data is backed up regularly.

Privacy by Design

CGM ensures that data protection and data security are already taken into account in the planning and development of IT systems. This prevents the fact that data protection and data security requirements only have to be implemented after IT systems have been made available through expensive and time-consuming additional programming. Possibilities such as deactivation of functionalities, authentication or encryption are already taken into account during production.

Communication by E-Mail (Practice / CGM)

Should you desire to contact CGM by e-mail, we point out that the confidentiality of the information transmitted is not guaranteed. The content of e-mails can be viewed by third parties. We, therefore, recommend that you to send us confidential information exclusively by post.

Privacy by default

Furthermore, the products of CGM are already pre-set in the delivery state to be data protection-friendly, so that only the

personal data necessary for the purpose pursued are processed.
The default settings are as follows:

1. The CGM DATASAFE Installer is usually installed in the folder "C:\CGM\DATASAFE\Installer".
2. The local backup folder is usually set up under "C:\CGM DATASAFE 5 Backups".
3. The CGM DATASAFE installation location is usually located here: "C:\Program Files (x86)\CGM DATASAFE 5"
4. The schedule for the backups is by default: Monday to Friday at 21:00.
5. The replication schedule is by default "After successful local backup".

Other settings or paths are also possible, the described paths are only standard paths suggested by CGM DATASAFE during an installation.

8. Rights of the Affected

Personal Data of the Physician and the Practice Employees

You have the right to receive information about your stored personal data as well as the right for correction, restriction of processing, objection, blocking or deletion of this data. You have the right to revoke your consent to CGM at any time with effect for the future. In addition, you have the right to complain to the data protection supervisory authority responsible for you if you are of the opinion that we are not processing your personal data correctly.

It is not possible to disclose stored patient information within backups. It is only possible to tell the patient what type of data is backed up by viewing the file paths. In addition, it is possible to delete the backups within a short period of time (1 week).

We undertake to delete all contract data, all protocol data and all data relating to technical operation after the termination of your contract without being requested to do so. However, we are legally obliged to observe commercial and tax retention periods which may extend beyond the duration of the contractual relationship. Data relating to technical operation will only be retained for as long as it is technically necessary but will be deleted at the latest after termination of your contract.

9. Storage Duration and Deletion of Data

In accordance with the Federal Data Protection Act, we undertake to delete all medical data, all contract data, all protocol data and all data relating to technical operation after the termination of your contract. However, we are legally obliged to observe commercial and tax retention periods which may extend beyond the duration of the contractual relationship. Data relating to technical operation will only be retained for as long as it is technically necessary but will be deleted at the latest after termination of your contract.

10. Enforcement

CGM regularly and consistently checks compliance with these data protection regulations. If CGM receives formal complaints, it will contact the author regarding his concerns in order to resolve any complaints regarding the use of personal data. CGM undertakes to cooperate with the relevant authorities, including data protection authorities.

11. Changes to this Privacy Policy

Please note that this Privacy Policy may be amended and modified from time to time. If the changes are material, we will provide a more detailed notice. Each version of this Privacy Policy can be identified by its date and version in the footer of this Privacy Policy. In addition, we archive all previous versions of this Privacy Policy for your review upon request to the CompuGroup Medical SE & Co. KGaA Privacy Officer.

12. Data Protection Officer

If you have any questions regarding the processing of your personal data, you can contact the data protection officer, who is at your disposal in the event of requests for information or complaints.

Hans Josef Gerlitz
CompuGroup Medical SE & Co. KGaA
Maria Trost 21
D-56070 Koblenz

[Hans Josef Gerlitz](mailto:hans.josef.gerlitz@compu-group.com)

13. Competent Supervisory Authority

For the CGM

The State Commissioner for Data Protection and Freedom of Information

Rhineland-Palatinate
Hintere Bleiche 34
55116 Mainz

as the supervisory authority.