The translation serves only as an aid to understanding. The legally binding form is the German.

1. Data protection organization and allocation of responsibilities in data protection

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

CompuGroup Medical SE & Co. KGaA has introduced a central data protection management system that ensures 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 fulfill our information obligations and provide you with information about the handling of data at CGM. This data protection declaration refers to the provision and use of the customer portal CGM PORTAL.

2. Purpose and legal basis of data processing

CGM PORTAL is an e-commerce platform used by CompuGroup Medical SE & Co. KGaA to create customer contact points and customer service more efficiently. CompuGroup Medical SE & Co. KGaA uses the SAP Commerce Cloud platform for this, which is provided by CompuGroup Medical SE & Co. KGaA.

The processing of personal data takes place for the following purposes:

- master data management (viewing and editing of master data)
- ticket management (viewing of the status of existing and creating new support tickets)
- document provisioning (viewing of billing and contract copies)
- customer communication about products, offers, and news (information and customer contacts)
- processing of orders and payments
- personalizing of content and offers
- improving the service quality
- analyzing the KPIs (viewing and evaluating of the agreed service level agreements)

The legal basis for the processing of personal data is given by Art. 6 (1) lit. B GDPR, as the processing is necessary for the performance of a contract or for the implementation of pre-contractual measures. If necessary, we obtain your consent for certain data processing operations on the basis of Art. 6 (1) lit. a, e.g. for promotional communications. You have the right to revoke your consent at any time.

3. Type of data processed

We process the personal data listed as follows:

Personal data of CGM employees

- personal master data (name)
- contact data (e-mail address, phone number) Sales only!
- authentication data for accessing the CGM PORTAL (user name, hash value)
- device information (IP address, system information)

Personal data of customers as well as their employees

- personal master data (name)
- address data (street, ZIP code, city, country)
- contact data (e-mail address, phone number, fax number)
- customer data (identification data)
- payment information (IBAN, SEPA mandate)
- order history and purchasing behavior
- communication preferences and consent to promotional communication
- device information and data on technical operation (IP address, system information, file requests, UID, user status)
- usage data, such as pages visited and click behavior

In addition, local storage technology can be used to customize the user interface and adapt CGM PORTAL to personal needs. Here, data is stored locally in the browser memory. After closing the application, it will be deleted automatically. The data stored in the local storage cannot be accessed by third parties. It is not passed on to third parties and not used for commercial purposes. You may manage local storage contents in the browser via the settings for "Chronicle" or "Local data," depending on which browser you use. Please note that this may result in functional restrictions.

4. Storage location

The data is stored in the data center of CGM SE & Co. KGaA in Frankfurt (Germany).

5. Storage duration

Personal data is stored for the duration of the contractual relationship. In addition, data is retained for a reasonable period of time to allow for future referencing, unless there are legal retention obligations or legitimate interests that require longer retention.

Deletion takes place automatically after the expiry of the retention obligations.

6. Data transmission

We will only disclose your personal data to third parties if this is necessary to fulfill the contract for the use of CGM PORTAL (e.g: payment service providers and shipping service providers) or if we are required to do so due to legal obligations. In doing so, we ensure that appropriate data protection measures are taken to protect your data.

7. Commitment to confidentiality

Handling health data

In addition to the security requirements of the data protection laws (GDPR and Federal Data Protection Act new), patient data, in particular health data, is also subject to strict requirements of the German Criminal Code (German Strafgesetzbuch, StGB) as well as the German Social Codes (German Sozialgesetzbücher, SGB) and are treated particularly sensitively by CGM.

We restrict access to contractual and protocol data and data on technical operation to employees and contractors of CGM for whom such information is absolutely necessary to perform the services under this contract. These persons are bound to comply with this data protection declaration and confidentiality obligations (GDPR, §203 German Criminal Code, §35 German Social Code I, §88, German Telecommunications Act). Violation of these confidentiality obligations may be punishable by termination and criminal prosecution.

Employees are regularly trained in data protection.

Important note

We expressly point out that uploading attachments containing non-anonymized patient data and any other personal data of third parties, as well as entering patient data in the description of the tickets, is expressly prohibited. There is no technical possibility on the part of CGM at this point to check and prevent an upload of files.

8. Data security

We take appropriate technical and organizational measures to ensure the security of personal data and to prevent unauthorized access, loss, misuse, or disclosure. This includes

- role-based authorization concept with password-based authentication
- access control via single sign-on based on the Keycloak open source software product using standards and protocols such as OAuth 2.0 and OpenID Connect.
- encrypted storage of the password in the database using hash value
- operation of the application in a data center environment
- encrypted data transmission via HTPPS protocol based on TLS 1.2
- encrypted storage of data stored in the data center
- monitoring data traffic for suspicious activity through firewalls and intrusion detection prevention (IDP) systems

9. Technical and organizational measures

In order to guarantee data security, we regularly check the state of the art. For this purpose, typical damage scenarios are determined and then the protection requirements for individual personal data are derived and divided into damage categories, among other things. A risk assessment is also carried out.

Furthermore, differentiated penetration tests serve to regularly check, assess, as well as evaluate the effectiveness of these technical and organizational measures to ensure the security of the processing.

10. Rights of the data subjects

You have the right to information about your personal data stored as well as, if applicable, rights to correction, restriction of processing, objection, blocking, or deletion of this data.

In the case of consents granted to CGM, you have the right to revoke them 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 believe that we do not process your personal data correctly.

We undertake to delete all contractual data, all protocol data, and all data on technical operation after termination of your contract without being asked to do so.

However, we are legally obligated to observe retention periods under commercial and tax law, which may extend beyond the duration of the contractual relationship. Data on technical operation will only be kept as long as it is technically necessary, but deleted upon termination of your contract.

11. Enforcement

We regularly and consistently monitor compliance with these data protection regulations. If CGM receives formal complaints, it will contact the author regarding their concerns to resolve any complaints regarding the use of personal information. CGM undertakes to cooperate with the relevant authorities, including data protection supervisory authorities, to this end.

12. Changes to this data protection declaration

Please note that this data protection declaration may be supplemented and amended from time to time. If the changes are significant, we will issue a more detailed notification. Each version of this data protection declaration can be identified by its date and version status in the footer of this data protection declaration (status). In addition, we archive all previous versions of these data protection declarations for your inspection upon request at the data protection officer's of CompuGroup Medical SE & Co. KGaA.

13. Use of the Chatbot

1. Categories of data subjects

- Users of the CGM PORTAL

2. Categories of processed personal data

- Email address
- First and last names
- SAP ID
- Contact SAP ID
- CGM products the customer is actively contracting with us

3. Purpose of data processing

To use the chatbot, the user must be actively logged into the portal. Boost.Ai AF retrieves the user's login data via an OpenID Connect integration to determine whether a user is considered "logged in" or not. Boost.Ai AF has no information about the user other than what the identity provider provides as a token, as mentioned above. Boost.Ai AF stores what is needed to maintain the conversation in an authenticated state.

4. Description and scope of data processing

The CGM chatbot is a software solution developed by Boost.Ai AF (Grenseveien 21, 4313 Sandnes, Norway), which has been integrated into the CGM PORTAL to answer user questions. This solution uses both a large language model (LLM) for free text inputs and a conversational AI solution based on fixed rules, intents, and workflows to produce specific outputs. This enables efficient and accurate responses to inquiries. Example inputs include:

- Where can I find my invoices?
- How can I manage my contacts?

This duality of technology allows for flexible interaction, which can handle complex inquiries through the LLM and support standardized processes effectively via rule-based conversational AI.

5. Hosting

The chatbot is hosted by AWS in Ireland.

6. Legal basis for data processing

The described processing is based on Art. 6 para. 1 GDPR (a).

By using the chatbot, the user consents to the processing of personal data.

7. Purpose of data processing

The entered data is processed to provide information on services, locations, or topics of the CGM PORTAL in chat format. The processing takes place in a dialogue, similar to a conversation, and on the chatbot's side, it is fully automatic or in real-time with a support agent.

8. Storage duration

The data entered by the user will be anonymized after 60 minutes. This anonymization refers to numbers, names, and email addresses. The entire conversation history will be anonymized after 14 days.

14. Sinch Integration Live Chat

Live chat with a CGM support employee is possible through the integration of Sinch. The data (chat events, chat subject, and the chat transcript) is stored by CompuGroup Medical SE & Co. KGaA. After the retention period of 30 days, all data is automatically anonymized or deleted. Anonymizing conversation data means that the data is altered so that the event can no longer be linked to a person. Anonymization, instead of deletion of the event, is carried out to ensure that the statistics display correct figures.

The following list explains which data is anonymized and which is deleted:

- Call events are anonymized, and any possible call recording is deleted.
- Processed email conversations are anonymized, and the subject and content of the email are replaced with the text {Anonymized by DPO}. Possible attachments are deleted. This also applies to other email-type elements, such as tasks and XRI elements.
- Chat events and chat subjects are anonymized, and the chat transcript is deleted. This also applies to other chat-type subchannels such as SMS and Facebook Messenger. Possible attachments are deleted.
- If a script is linked to a conversation element, the free text contents of the script are deleted.
- If internal notes were added to a conversation, the notes are replaced with the text {Anonymized by DPO}.
- If attached data (CAD) was added to a conversation, the data is replaced with the text {Anonymized by DPO}.
- Completed or expired outbound campaigns:
  - When a retention period expires, the campaign and the corresponding call events are deleted.
  - When data is deleted upon request, the customer data and call events in the campaign are deleted.

- Directory data and consent information are not removed after the retention periods expire but only upon request.

CompuGroup Medical SE & Co. KGaA still recommends not entering personal data when asking questions!

15. Responsible party

The responsible party for data processing in connection with the use of CGM PORTAL is:

CompuGroup Medical SE & Co. KGaA
Maria Trost 21
56070 Koblenz

E-mail address: info@cgm.com
Phone number: +49 261 8000-0

The responsible party is the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data.

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 case of requests for information or complaints

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

E-mail: HansJosef.Gerlitz@CGM.com

16. The responsible data protection supervisory authority

for CompuGroup Medical SE & Co. KGaA is

The State Commissioner for Data Protection and Freedom of Information Rheinland-Pfalz
Hintere Bleiche 34
55116 Mainz.