

Data Protection Declaration CGM ANALYTIX

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

The business unit CompuGroup Medical Lab AB (CGM LAB in the following) considers the protection of personal data and handling it responsibly to be a leading principle. CGM LAB commits to strict compliance with all relevant laws and regulations concerning the storage and processing of personal data.

The corporation CGM SE 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 data protection statement serves to fulfil the legal information obligations by providing information about the handling of data within CGM SE. This data protection statement specifically refers to CGM LAB's product CGM ANALYTIX.

A customer that uses CGM ANALYTIX is data controller for all information stored in CGM ANALYTIX (CGM LAB stores no information in customer installations of CGM ANALYTIX).

CGM LAB urges their clients to establish business routines that ensures that the personal data stored by the customer in CGM ANALYTIX is administered in a way that meets the demands in GDPR. CGM LAB wishes to point out that healthcare data is a special category of personal data and subject to higher protection by data protection regulation.

2. CGM ANALYTIX

CGM ANALYTIX is an administrative process support for clinical laboratories or laboratory organisations in chemistry, micro biology and histology/cytology (referred to as "customer" in the following). CGM ANALYTIX supports the business operations for customers who have to adhere to legal requirements in their work, have structured documentation, invoicing etcetera and adheres to additional requirements that can be met using available accessories for CGM ANALYTIX.

CGM ANALYTIX contains support for managing user authorisations and limits access to software and available accessories to authorised persons. Beyond access control to the software and modular software extensions, user rights management also controls management of read and write access to data stored and processed within the system.

CGM ANALYTIX contains support for administration of personal data in accordance with GDPR, including selective deletion, deletion and export.

When in use CGM ANALYTIX stores the following types of information which may contain personal data on the customer's server:

- Information about patients

- Information about staff members
- Information box about request sources
- Technical information from processing

3. Processing of personal data by CGM LAB

Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In accordance with data protection laws, we oblige to delete all contract data, log data and data from technical operations after termination of your contract.

However, we are also obliged by commercial and fiscal law to respect legal retention periods that may extend beyond the termination of your contract. Data from technical operations is stored as long as technically necessary and is deleted at the latest after termination of your contract.

3.1 Contract and registration data

Contract and registration data identify and manage the contractual relationship between the customer and CGM LAB. This data includes:

- Information about the customer
 - Name
 - Address
 - Phone number
 - E-mail address
 - Identifier/identification number of the customer
- Information about operations manager/contact person
 - Title
 - First name/surname
 - Name suffix
 - Address
 - Phone number
 - E-mail address
 - Identifier/identification number of the person

Storing and processing personal data disclosed to CGM LAB during the business and contractual relationship serves and is limited to the purpose of fulfilling the contract, in particular order processing and customer support.

Only if permitted by means of a consent declaration may this data also be used for product related customer surveys and marketing purposes.

Data will not be transferred or sold to any third party, unless necessary for the fulfilment of the contractual obligations or if explicitly permitted by means of a consent declaration. As an example, it may be necessary for CGM LAB to transmit the address and order data to a sales and service partner when an order has been placed. We will inform you about the recipients of your data in the order confirmation.

Business agreement information is stored in the CGM Group's CRM system, the servers of which are located in the EU.

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.

3.2 Data from technical operations

Data from technical operations is needed for the provision of the contractually guaranteed services, e.g. support and system updates. CGM collects data from technical operations only for this purpose. CGM regularly examines that only data that is required to provide and enhance the technical operations of your product / services will be collected, stored and processed.

Information from the customer's business system will only be collected after the customer's confirmed consent.

When using our online services, e.g. support portal, the following data required to maintain system integrity and security is stored temporarily:

- Domain name
- IP address of the client computer
- Access date and time
- File request of the client computer (file name and URL)
- Number of bytes transferred during the connection.

Data from technical operations is stored in the CGM Group's CRM system, the servers of which are located in the EU.

3.3 Anonymized data

Anonymized data is only used when this is required for the fulfilment of CGM LAB's support commitment to the customer. In these cases the anonymization is performed by the customer; CGM LAB only handles already anonymized data provided by the customer.

4. Processing of personal data by CGM ANALYTIX on the customer's server

Personal data is used in several programs in CGM ANALYTIX.

[Click here to view list.](#)

The personal data processed in CGM ANALYTIX includes:

- Technical data about the customer, the customer's employees and business partners
- Patient data
 - Personal technical data
 - Sensitive data (health and healthcare information)

This data is stored and processed in the database on the customer's server. CGM LAB urges their clients to establish business routines that ensures that the personal data stored by the customer in CGM ANALYTIX is administered in a way that meets the demands in GDPR.

5. Data transmission / transfer

Electronic data transfer based on legal, contractual or prior consent, is carried out by CGM LAB only after user interaction or automatically - if permission has been granted.

6. Commitment to confidentiality, trainings on data protection

CGM LAB employees sign a confidentiality agreement, e.g. regulates management of patient data. The basic principle for CGM LAB in this context is that we do not access, change, delete or in any other way process information entered by our customers in our systems unless this is specifically requested by the customer or is necessary for the fulfilment of our commitments vis-à-vis the customer (e.g. providing support, migrating information or similar). CGM LAB employees commit to ensuring that all classified material and information is stored in a specified manner, and observing complete confidentiality vis-à-vis unauthorized persons. CGM LAB employees undergo data protection training.

7. Security measures / risk avoidance

CGM takes all necessary technical and organizational security measures to protect your own personal data as well as personal data of your patients 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 CGM continuously monitors developments in security technics. This includes e.g. performing consequence, risk and vulnerability analyses.

Additionally, regular and specifically developed tests are performed to assess the performance of the technical and organisational measures that ensures the security of the types of personal data processing that we perform or that our customers perform in our products.

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

8.1 Data backup

Data backups are continuously made to prevent data loss.

8.2 Privacy by design

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

Measures for achieving built-in data protection are taken into account at the beginning of the development process, e.g. secure authentication or encryption.

8.3 Privacy by default

CGM products come with factory settings that are optimized for data privacy.

8.4 Communication by e-mail (customer to/from CGM)

In case you want to contact CGM by e-mail please be aware that privacy of the transmitted information cannot be guaranteed since e-mails can not be considered as a secure form of communication. We recommend that you use different means of communication, e.g. telephone, video or regular mail if you wish to transfer confidential information.

8.5 Remote administration

Employees or subcontractors of CGM may occasionally require access to patient or customer data. This access is governed by general CGM rules.

- Remote administration access is closed by default and is granted by the customer only.
- Passwords to access customer IT systems are issued for purposes of remote administration only.
- Critical interventions are secured by a "4-eyes procedure" with at least two qualified CGM staff members.
- We are using remote administration tools requiring the customer to actively grant access and allowing the customer to track interventions.
- Remote administration access is logged in CGM's CRM system. The following data is logged: Person in charge, date and time, duration, target system, remote administration tool, brief description of the task carried out and, in the case of critical interventions, the name(s) of the additional qualified staff members consulted when applying the "4-eyes procedure".
- Recording of remote administration sessions is forbidden.

9. Rights of the data subject

GDPR establishes certain rights of the data subject vis-à-vis the data controller and data processor:

- The right to be informed about data stored about the data subject as well as the right to access said data.
- The right to rectification, to erasure, to restriction of processing, to data portability and the right to object to processing of the subject's personal data.
- The right to of the data subject withdraw consent at any time. The withdrawal has future effect.
- To lodge a complaint with the responsible supervisory authority if the subject thinks that the data controller or data processor is processing the subject's data inappropriately.

The registered shall primarily contact the data controller to exercise these rights. The relation between CGM LAB and customer regarding the position as data controller or data processor is regulated in separate agreements.

10. Enforcement

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

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

CGM LAB commits to working cooperatively with the authorised administration including the supervisory authority.

11. Amendments to this data protection statement

Please note that this data protection statement may be subject to amendments and supplements. In case of substantial amendments, we will publish a detailed notification. Each version of this data protection statement can be identified by and version number date stated in italics in brackets at the end of the text. In addition, all prior versions of this statement are archived and made available upon request by the Data Protection Officer.

12. Responsible for CGM LAB

CompuGroup Medical Lab AB
 Cirkelgatan 14
 SE-781 72 Borlänge
 Sweden

12.1 Questions regarding personal data in CGM ANALYTIX

Questions regarding the processing of personal data in CGM ANALYTIX shall be addressed to the system administrator for the current customer since the customer is data processor for information in the system. When suitable, the system administrator can forward the question to the data protection officer at CGM LAB.

Question regarding the contractual relationship between CGM LAB and customer can be sent to the data protection officer via email: dataskyddgruppen.se@cgm.com.

13. Supervisory Authority

Swedish Authority for Privacy Protection (IMY)

Telephone: +46 (0) 8-657 61 00

E-mail: imy@imy.se

(Version 4, 2021-03-31)