

Data Processing Regulations of the Sanitas Group

1. Introduction

Sanitas Health Insurance (hereinafter referred to as Sanitas) processes personal data pursuant to the Swiss Federal Data Protection Act (DSG) as a federal body within the context of the Swiss Federal Health Insurance Act (KVG) and the Swiss Federal Accident Insurance Act (UVG) and as a private legal entity within the context of the Swiss Federal Act on Insurance Policies (VVG).

Based on Art. 12 of the Swiss Federal Data Protection Act (DSG) and Art. 5 and Art. 6 of the Ordinance on Data Protection (DSV), Sanitas is required, among other things, to draw up processing regulations.

1.1 Purpose and scope

These processing regulations ensure the necessary transparency in the area of data processing.

It should also be possible for “non-experts” to understand and assess the Sanitas approach to data processing.

These processing regulations set out the principles of data processing as defined by the DSG. Sanitas notes the following principles in particular:

- Data processing by Sanitas is based on legal grounds or on the express consent of the data subject. Express consent shall be given, among other things, if high-risk profiling is carried out by a private person or if profiling is carried out by a federal body.
- Personal data shall only be processed for the purpose that is stated during the procurement of the data, that is evident from the circumstances or that is provided for by law.
The purpose of the processing of personal data and its procurement shall be expressly stated, be recognisable by the data subject or be evident from the circumstances.
- The scope of the processing shall be proportionate to the purpose and limited to what is necessary to achieve the objective.
- Personal data shall be destroyed or anonymised as soon as it is no longer required for the purpose of processing.
- The data shall be protected by technical and organisational security measures. Incorrect data shall be corrected.
- The rights of the data subject shall be safeguarded. The data subject shall receive complete information about their stored data and may request their deletion or correction.

1.2 Up-to-dateness

The data collection owner shall review the regulations and descriptions of the data collections annually to ensure that they are up-to-date and shall notify the Data Protection Officer (DPO) of any changes or confirm that they are up-to-date.

1.3 Definitions and abbreviations

The following abbreviations are used in the data processing regulations:

- DPO: Data Protection Officer of the Sanitas Group
- DSG: Swiss Federal Data Protection Act of 20 September 2020, SR 235.1

- EDO: Swiss Federal Data Protection and Information Commissioner
- DSV: Ordinance on Data Protection of August 31, 2022, SR 235.11
- KVG: Federal Law on Health Insurance of March 18, 1994, SR 832.10
- MO: Medical Officer
- MRO: Medical Review Office

2. Notification of data collection to the Swiss Federal Data Protection and Information Commissioner

Sanitas complies with the obligation to submit data to the Swiss Federal Data Protection and Information Commissioner pursuant to Art. 84b of the Swiss Federal Health Insurance Act .

3. Data protection and data security

3.1 Data protection

The Board of Directors of the Sanitas Group bears overall responsibility for compliance with data protection requirements. It delegates implementation thereof to the management of the Group companies.

The Executive Board is responsible for implementing, communicating, controlling and monitoring the specified data protection policy throughout the Sanitas Group. It ensures that Sanitas has an efficient organisation that supports compliance with data protection. The Sanitas Group has a Data Protection Officer (DPO) who, in turn, ensures the implementation of the data protection requirements and is equipped with the necessary human and financial resources.

The DPO stipulates the most important conduct regarding data protection and ensures compliance with the data protection regulations applicable to the companies of the Sanitas Group.

The DPO, in cooperation with the relevant internal units, issues appropriate guidelines for compliance with the laws and standards. The main purpose of these is to create maximum transparency in the processing of personal data in order to enable professional identification and assessment of any data protection risks.

Employees are responsible for compliance with all provisions of data protection law within their area of responsibility, in particular the duty to provide information and the duty of confidentiality. Neither supervisors nor employees may delegate this responsibility. Every Sanitas employee must sign a privacy policy upon employment. During and after termination of the employment relationship, Sanitas employees must also maintain confidentiality vis-à-vis third parties with regard to information that becomes known to them in the course of their professional activities, in particular medical data. Supervisors ensure that employees are continuously informed about applicable legal and internal regulations.

These data processing regulations also govern the access criteria and the acquisition of access rights as well as the handling of the information obtained from data collection. Access by authorised persons is limited to the personal data which they need in order to fulfil their task.

Access to premises where particularly sensitive personal data is processed is protected by access restrictions. Access is only granted to Sanitas employees or third parties who have a consulting relationship with Sanitas and have signed a data protection and confidentiality declaration. Access to the medical review office is subject to additional restrictions.

For the use of hardware and software, internet and e-mail, the directives on the safe use of hardware and software, internet and e-mail also apply.

3.2 Data security

To protect the systems, access is generally only possible if the person accessing the system can confirm their identity by means of a user name and password. Additional restrictions are also provided for clients and IT applications with access to particularly sensitive personal data.

3.2.1. General measures

Sanitas operating systems are regularly checked and protected against malware attacks. The following measures are in place to protect data collections against unauthorised or accidental destruction, accidental loss, technical failures, forgery, theft or unlawful use and unauthorised processing:

- Data backups
- Logging
- Access protection
- Secured networks
- External communication (email, internet) of particularly sensitive personal data only with sufficient encryption
- Restricted access to data centre, networks and other technical facilities for the storage and processing of data

3.2.2. Special measures

Access control

Access to Sanitas buildings is secured with a badge system. Visitors must register at the reception desk. Rooms and buildings housing technical equipment for data transmission and data storage such as servers, routers, switches, etc. are secured with locking and/or access systems and are only accessible to a restricted group of people. Rooms and buildings housing clients that provide access to data collections are secured with access systems.

Personal data carrier control

The entry and access restriction measures are also used for the purposes of personal data carrier control. Technical precautions ensure that only authorised persons are able to process data using electronic data carriers.

Transport control

Unauthorised persons shall be prevented from reading, copying (to other drives or data carriers), printing, modifying or removing data carriers.

Sensitive information shall not be sent in unencrypted form via electronic mail (email). Wherever possible, any necessary transportation of sensitive data is carried out electronically and encrypted using a recognised procedure.

The physical transportation of data is carried out by means of a secured transportation system, the data is encrypted for transportation using a recognised method, and the key is transported separately.

Announcement control and interface description

Data recipients to whom personal data is disclosed by means of data transmission equipment are identified and compliance with the legal requirements for disclosure (legal basis, declaration of consent) is ensured. Data transfers are logged and the identity of the data is checked before it is transferred.

Storage control

Unauthorised entries, changes or deletions to the memory are prevented by access and authorisation controls (e.g. user name and password) and by the IT applications. When data storage devices (hard disks) and computers (PCs and servers) are replaced, care is taken to ensure that all data is irrevocably deleted.

User control

Access to data processing systems is generally protected by technical measures and must be approved for the individual employee. The information system grants employees differentiated access rights. Access by authorised persons is limited to the data that the authorised persons actually need to perform their tasks.

Access control and permissions

Access to automated processing data is only possible for employees by means of IT applications. The necessary authorisations must be applied for. Employees only have user rights for IT applications that they need to perform their tasks and, within the IT applications, only for functional areas that correspond to their tasks. Authorisation requests must be approved by the respective supervisors and the authorisation owner. The authorisations are withdrawn from the employees when they are no longer necessary for the assigned tasks.

The internal organisation defines the access rights for each employee by means of an access concept. The more sensitive the data being processed, the higher the requirements for authorising access. A list (audit log file) is kept of the permissions granted.

Remote access to the data processing systems is only possible for specially authorised persons via encrypted access.

Input control

Entries and mutations are logged. Insofar as data is entered or mutated automatically – which mainly happens during electronic data exchange or subsequent automated processing such as payment runs, etc. – the origin of the data and the processing time are always logged.

4. Data processing procedures

4.1 Right to information

The Sanitas Data Protection Officer (DPO) is responsible for granting insured persons the right to inspect their own data. The DPO obtains the data, provides the information and, if necessary, ensures that the data is corrected in accordance with an internally defined process.

Inquiries may be made in writing to the following address:

Sanitas Health Insurance

Data Protection Officer

Jägergasse 3

8021 Zurich

4.2 Correction procedure

Once identified, data subjects may request that data collected about them that is disproportionate or not necessary for the performance of the contract be corrected or destroyed. The Sanitas Data Protection Officer decides on such requests.

4.3 Blocking of data

All persons included in a data collection may, after identification, request that data processing and, in particular, the disclosure of their data to third parties, be blocked. The Sanitas Data Protection Officer decides on such requests and on the consequences of implementing them.

4.4 Anonymisation

Tests and projects are carried out using anonymised data. Statistical data is anonymised in accordance with legal requirements. Any inferences about specific persons is not possible.

4.5 Archiving

Data is stored in accordance with legal requirements and internal company directives.

4.6. Backup and recovery

Regular data backups are performed for all relevant data defined in the contracts. The databases are regularly copied to a separate directory and a backup is made. The recovery of the data is assured by the backup system.

4.7 Logging

Defined imports (see the section "Interfaces") and user logins are logged in those systems that allow such logging. Sanitas may evaluate logs in anonymous form to monitor compliance with the usage policy. If misuse is detected or suspected, Sanitas may conduct a comprehensive usage evaluation. The log data is kept for one year for the purposes of audit compliance.

4.8 Definition of data collections

The data collections conducted by Sanitas are aligned with business processes. This results in the following data collections:

Master/contract data

- Benefits data
- Financial data
- Offer and application data
- Recourse cases
- Debt collection files
- Telephone data
- Commitments to cover costs
- Agent data

4.8.1. Interfaces

The business-relevant, external interface descriptions contain the origin of the data, the addressee, the purpose, the type of data and information regarding how frequently and in what form the data is transferred.

In the interface description, the following information on data transfer (disclosure) is recorded:

- Where does the data come from?
- Who receives the data?
- For what purpose is the data transferred?
- What data will be transferred?
- How frequently will the data be transferred?
- By whom was the transfer initiated?
- In what form is the data transferred?

4.8.2. Processes

Data is collected, processed and transferred by Sanitas in accordance with defined processes. The individual processes are recorded in process descriptions intended for internal use.

4.8.3. Responsibilities

- Data protection in general and inspection requests: Sanitas Data Protection Officer
- Technical data security: IT division
- Destruction of electronic data: IT division
- Documents for the Medical Officer: Medical Officer
- Access controls: Sanitas Security Officer

5. Closing provisions

5.1 Entry into force

These regulations replace all previously published regulations. This document comes into force on 1 September 2023*.

5.2 Supplementary documents

- Processing regulations
- List of processing activities
- Access concepts for data collections

* Decision of the management