Data Processing Regulations

Table of Contents

1. Initial position

CONCORDIA Swiss Health and Accident Insurance Ltd is responsible for implementing and processing mandatory health care insurance in accordance with the Swiss federal law on health insurance (KVG/LAMal).

The Data Processing Regulations also apply, in accordance with Art. 59a of the Health Insurance Ordinance (KVV/OAMal), to the independent data connection point, which is operated internally by CONCORDIA.

2. Documentation of the organisational units affected by the system

CONCORDIA Swiss Health and Accident Insurance Ltd is the system operator and the body that is responsible for it.

3. Interface description

3.1 Interfaces to external data users or data providers

Pursuant to Art. 84 of the KVG/LAMal, several services, which also partially include the processing of personal data, have been outsourced by CONCORDIA to external partners for document processing and postal solutions. The data-compliant processing of data, as well as data security, has been regulated in the respective cooperation agreements. Furthermore, the IT partners are partially certified in accordance with various ISO norms, such as the ISO 9001:2008 (quality management systems) and the ISO/IEC 27001 (information security management systems) in particular.

Furthermore, CONCORDIA remains responsible for the compliance with data protection for the outsourced areas.

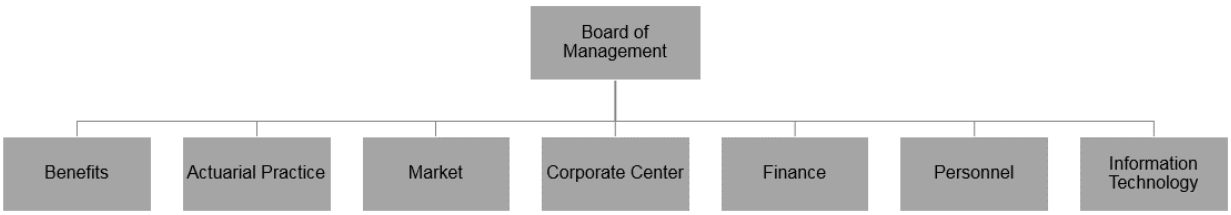
As part of the implementation and processing of health and accident insurance in the realm of mandatory health care insurance in accordance with the KVG/LAMal, CONCORDIA maintains interfaces to data users and data providers (e.g. authorities, courts, other insurers, external experts).

3.2 Data source

The data are provided by service providers, insured persons, other social insurance providers, public authorities and financial services providers.

4. Organisation chart of the responsible body

Organisation chart of CONCORDIA Swiss Health and Accident Insurance Ltd



5. Responsibilities

The Board of Management of CONCORDIA Swiss Health and Accident Insurance Ltd is responsible for complying with data protection rules and data security.

Representatives for data protection, information security and physical security are there for matters regarding data protection and data security. These representatives advise the Board of Management, establish guidelines and are also involved in the control processes.

6. Documentation on the planning, implementation and operation of the data processing

The operation of the data processing is recorded in specific operation manuals. The technical planning and implementation is documented in project documents. The technical documentation of systems components can be found in computer science operation manuals.

7. Registering the directory of processing activities with the Federal Data Protection and Information Commissioner (EDÖB/PFPDT/IFPDT/FDPIC)

The directory of CONCORDIA Swiss Health and Accident Insurance Ltd was registered in the FDPIC DataReg Portal on 28 August 2023.

8. Process documentation pertaining to the data processing

The data processing procedures for the individual processing activities are recorded in internal process documentation.

9. Data source

See chapter 3.2.

10. Purposes for which data is regularly disclosed

See chapter 3.1.

11. Control procedures and in particular the technical and organisational measures

Adequate technical and organisational measures have been implemented, which ensure the confidentiality, integrity and availability of the data.

11.1 Entrance control

To ensure that no unauthorised persons access the commercial property of CONCORDIA, entry is possible only to the employees of CONCORDIA who possess a badge or key.

Access to the commercial properties of CONCORDIA is regulated in various directives.

11.2 Data media control

By means of technical and organisational measures, CONCORDIA ensures that no unauthorised persons may read, copy, modify or delete data; that no unauthorised data is stored in the memory; and that no unauthorised personal data is inspected, modified, deleted or stored.

Certain modifications conducted by employees may be traced back in the system.

Employees are instructed in various directives and regulations on the proper handling of data.

Digital data media is disposed of by the information processing business unit by means of a regulated process.

11.3 Transport control

By means of technical and organizational measures, CONCORDIA ensures (e.g. with encryption or directives on e-mail handling) that no unauthorised persons may read, copy, modify or delete data when disclosing personal data or when transporting data media.

11.4 Disclosure control

The recipient of personal data is verified either manually or by means of technical devices.

11.5 Storage control

See 11.2

11.6 User control

CONCORDIA has at its disposal an appropriate multilevel security concept according to the level of data protection required. Users must be authenticated in order to gain access to the information systems.

11.7 Access control

Authorisation for access to data is assigned on a strictly need-to-know basis – that is, rights will only be assigned in order to exercise the function required. Assignment is based on authorisation profiles. Defined work processes are in place for user and authorisation management, and these are supported by technical devices.

The assigned authorisations are verified periodically as part of the internal control processes.

11.8 Input control (log file)

The personal data entry is stored chronologically in the central information system. In the event of abuse or the suspicion of abuse, this data may be analysed. Employees are informed accordingly in the regulations entitled “Umgang mit Hardware, Software und elektronischen Daten” (dealing with hardware, software and electronic data).

12. Type and extent of access rights

Each employee only has access to that data which he needs to fulfil his tasks.

How access takes place, which authorisation profiles (roles) can exercise which functions, and which data space may be accessed are stipulated in an authorisation concept, where likewise, who is allowed to apply for these roles and who must grant the assignment are defined and approved.

13. Data processing procedures, in particular the procedures for rectifying, blocking, anonymising (pseudonymising), storing, safeguarding, archiving or destroying data

The data processing procedures are documented in specific directives, regulations and manuals.

Employees are regularly trained on matters concerning specialist processes and data protection.

14. Configuration of information technology resources

The information technology resources deployed by CONCORDIA (hardware and software) meet standards that are both international as well as those that are customary in the sector. The information technology resources are subject to a regulated life cycle management process.

The configuration of information technology resources is documented in operating manuals and is updated as required.

15. Procedure for exercising the rights of the affected persons

To exercise their rights under the DSG/LPD/FADP, affected persons can contact the company data protection officer at:

CONCORDIA Swiss Health and Accident Insurance Ltd
Data Protection Officer
Bundesplatz 15
6002 Lucerne