Helsana

Processing Policy of the Helsana Group

1. Purpose of the Processing Policy

This Processing Policy ensures the necessary transparency in the system development and data processing environment. It been made as brief and straightforward as possible to help the layperson to understand and evaluate system development and data processing. It was drafted based on the principle of «as much as necessary, as little as possible».

This Processing Policy outlines the principles of data processing for all data collected by the insurance companies of the Helsana Group (hereinafter also referred to as «**Helsana**», «**we**» or «**us**»). The Helsana Group insurance companies comprise Helsana Insurance Company Ltd, Helsana Supplementary Insurances Ltd and Helsana Accidents Ltd.

2. Data processing and methods

2.1 Structure

Helsana's data processing can broken down into the following data activities:

- Individual business (IB) quote development
- Audit, risk, legal & compliance
- Data security management
- Facilities management
- Public health sciences
- HR management
- Collections/disbursement, finances, actuarial services
- IT management
- IB customer service
- Corporate division (CD) customer service
- IB services contracting
- IB benefits management
- CD benefits management
- IB & CD new business
- IB & CD staff insurance
- Provident fund
- Medical examination service (VAD)
- IB contract administration
- IB sales channel management
- CD sales channel management
- IB sales support

Various interfaces enable direct contact with external contractors and service providers, such as when the service provider bills Helsana directly. Furthermore, there is an interface via which certain service providers can perform an online check of an insured person's insurance cover. Data protection and the relevant data security are guaranteed by a strong authentication process and modern encryption and transmission technology.

2.2 Data processing methods

Helsana uses internal regulations to set guidelines for keeping an inventory of and checking the legality (compliance checks) of data processing operations. The methods of saving, transmitting to third parties, retaining, archiving, pseudonymising, anonymising, deleting or destroying data must also be recorded in the data protection concepts for the respective data processing operation.

2.3 Use and data access

2.3.1 Authorised users

Users authorised for Helsana IT systems include:

- Employees of Helsana, to the extent that they require such access to carry out their mandate to «manage health insurance»
- System administrators of Helsana
- Contractually mandated service providers

(collectively referred to as authorised users).

2.3.2 Authorised user management

Authorised users are managed centrally by Helsana's identity & access management. Internal and external employees are registered via HR interfaces. New identities and accounts are only entered if a valid employment contract or service contract exists and the rights have been approved accordingly by the line manager.

2.3.3 Personal access authorisation

When joining Helsana, all authorised users are granted their access rights to information as defined in the role model and on the basis of their respective function and their organisational affiliation. Any other rights required must be requested individually via the authorisation portal. In this case, each request must be confirmed by the direct superior and, depending on the authorisation role, also by the role approver.

2.3.4 Cancellation of access authorisation

Authorised users for Helsana IT systems only have access to the data for as long as they need the data to do their work. When leaving or changing tasks within Helsana, their access authorisation is cancelled and the access authorisation they need for the new area of responsibility is reassigned in accordance with the role model.

2.3.5 Training for authorised users

Authorised users attend training courses for the different applications and subsystems.

2.3.6 Manuals and processing guidelines for authorised users

Appropriate documentation is available for the subsystems. Data processing is also defined in instructions, regulations and benefits manuals as well as in lists. These are updated by the responsible organisational units on a regular basis.

The responsible organisational units use specific instructions to establish a consistent benefit assessment level in accordance with the Federal Health Insurance Act (KVG) for the entire insurance region of Switzerland.

2.3.7 IT service providers

Insofar as the operation of Helsana's IT systems are outsourced to external IT service providers, these follow comparable regulations within their purview.

3. Right of access and to rectification and release of data

Under Art. 25 of Federal Act on Data Protection (FADP), data subjects can request information from the controller as to whether their personal data is being processed and request that this data be released to them. They are also entitled to have their data held by Helsana corrected.

4. Technical and organisational measures to guarantee data integrity

4.1 Access control

All rooms at Helsana that are used to process sensitive data are protected either electronically or manually from access by unauthorised persons. The responsible persons keep a log documenting key management and electronic access control. The physical security officer may at any time request to inspect this log or have evaluations performed. The zones requiring protection determine the security measures: workplaces are protected from access by unauthorised third parties. Special rooms and sensitive rooms, such as the technical rooms and the data centres, are secured as follows:

- More stringent physical security requirements are used exclusively to restrict access to the IT systems in the data centres operated by the IT organisation of Helsana and the decentralised servers operated by the IT organisation of Helsana to specially authorised persons
- The IT systems in decentralised servers that are not operated by the IT organisation of Helsana are subject to similar security precautions as those which are operated by them

Precautions implemented in the IT systems allow only authorised persons to process data. Only authorised persons have access to Helsana's IT systems.

4.2 Authentication of authorised users

Access to the Helsana's IT systems is protected by user ID combined with a temporary individual authentication token.

4.3 Disclosure control

Data recipients to whom personal data are disclosed by means of data transmission devices are identified via the interfaces (e.g. online coverage queries by service providers in connection with the use of the insurance card).

4.4 Transmission of data

The transmission of data is protected by means of encryption.

4.5 Storage control

Authorised users receive specific authorisations to make changes to data fields as required for the purpose of carrying out their work (e.g. in accordance with the KVG or Federal Accident Insurance Act [UVG]).

4.6 Technical requirements for end devices

Access to Helsana's internal network is restricted, protected by specific control measures and monitored. External IT service providers have similar arrangements in place for their networks.

4.7 Measures to protect data (confidentiality) with respect to end devices

All clients are protected against attack by multiple technical security measures.

Printed data is stored in such a way that third parties (e.g. housekeeping staff) cannot view and/or copy it. This data is either stored in lockable containers or disposed of using shredders or Datarec in accordance with internal instructions. The clean desk and the clear screen principles apply.

4.8 Logging

In addition to controlling access to Helsana's IT systems by means of an authorisation procedure as well as the protection afforded by personal user IDs and authorisations, some individual IT systems have a log that documents all automated processing to make it possible to subsequently determine whether data was processed for the purposes for which it was collected or disclosed. Logging is conducted in accordance with Art. 4 of the Data Protection Ordinance (DPO): logs are retained for a 13-month period in compliance with audit requirements. They are only accessible to bodies and individuals responsible for reviewing the application of data protection regulations or safeguarding or restoring the confidentiality, integrity, availability and traceability of data, and may only be used for this purpose. In some cases, external IT service providers have similar in-house rules regarding auditing.

4.9 Development

Requests for the system's further development are compiled and defined, budgeted and implemented as maintenance or full-scale projects. This approach and governance are regulated within the scope of the «Helsana Project Procedure».

4.10 Support for authorised users and duty to report

The functional management of the respective divisions provides professional support to all authorised users. Technical support for the IT systems and the network is provided by the IT organisation of Helsana or outsourced.

The authorised users are informed of the IT information system's need for protection as well as the regulations on how to handle the system and its data. The regulations are outlined in directives and leaflets raising awareness of information security. The authorised users are aware of the penalties that could be imposed for intentional or negligent breaches of information security.

All violations must be reported to the line manager in line with the security incident process or the whistleblower service in line with the Code of Conduct.

4.11 Supervision and responsibility

Those responsible for the IT systems or applications are responsible for ensuring that the authorised users comply with the instructions and this Processing Policy and that the external IT service providers comply with their contractual requirements.

5. Version

This Processing Policy does not form part of any contract with the insured person or any other third party. As such, we can amend this Processing Policy at any time. The version published on this website is the up-to-date version.

Last update: **September 2023**