Privacy Policy and data processing policy
Helsana Insurance Company Ltd

Version 1.01 dated 06.06.2018

1. Brief summary

Basic insurance is compulsory for all residents of Switzerland. Helsana Insurance Company Ltd (**Helsana**) is one of the health insurance companies responsible for handling this statutory health insurance and offers all services required by law. Helsana processes personal data for the purpose of handling statutory health insurance, such as benefit payments and premium collection. Personal data is considered to be any information relating to an identified or identifiable (natural) person. This primarily concerns data regarding individuals insured by Helsana who disclose their personal data to Helsana themselves. This data includes, for example, contact information such as names, addresses and telephone numbers. In order to fulfil its legal mandate, Helsana relies on further personal data such as date of birth, AHV and insurance numbers as well as information concerning an individual's health.

Since Helsana attaches great importance to the protection of this data, some of which is particularly sensitive, this Privacy Policy will provide information regarding:

- who is responsible for data processing;
- which data is collected and processed from which persons;
- who collects and processes data and how;
- for what purpose will the data be processed and on which legal basis;
- to whom the data will be disclosed;
- how long the data will be stored;
- the specific rights of the persons concerned.

2. Applicability of the Privacy Policy

This Privacy Policy explains the collection and further processing of personal data by Helsana. At the same time, it serves as a data processing policy within the meaning of Art. 11 and Art. 21 of the Ordinance to the Federal Act on Data Protection (**VDSG**) in conjunction with Art. 84b of the Federal Health Insurance Act (**KVG**).

This is without prejudice to the right to collect and further process personal data covered by other privacy policies or terms of use, which has arisen through specific circumstances or which is governed by law.

3. Data controller, data protection officer

For the procurement and further processing of personal data in connection with the handling of statutory health insurance, Helsana is the data controller (in particular within the meaning of Art. 4 (7) of the European General Data Protection Regulation [**GDPR**] and the Federal Data Protection Act, insofar as the respective provisions apply in individual cases).

Any requests, claims or information related to data protection law as it concerns Helsana may be sent to the data protection officer of Helsana at the following contact address and must be accompanied by a copy of an official form of identification:

Helsana Insurance Company Ltd
Data Protection Officer
PO Box
CH-8081 Zurich

To the extent that Helsana falls within the scope of the GDPR, Active-Assets A^2 GmbH serves both as its data protection officer within the meaning of Art. 37 GDPR and its representative pursuant to Art. 27 GDPR. The contact details are:

Active-Assets A^2 GmbH
Gottlieb-Daimler-Str. 5
78467 Constance
Germany
privacy@helsana.ch

4. Collection, processing and use of personal data

4.1 Persons concerned

Helsana collects and processes personal data of

- individuals who are or have been insured by Helsana or another health insurance company of the Helsana Group;
- individuals designated as the head of a family, payer or authorised person (they do not necessarily have to be insured by Helsana);
- individuals assigned by the cantons to Helsana or another health insurance company of the Helsana Group to ensure compliance with the insurance obligation (cf. Art. 6 KVG);
- participants in market research, customer satisfaction and opinion surveys conducted by Helsana;
- potential customers or individuals with an interest in the products and services of Helsana

(collectively referred to as **customers**).

Furthermore, Helsana collects and processes data from service providers, medical examiners, contractors, sales partners and other business partners of Helsana as well as their employees and contacts (**partners**).

Helsana processes the following categories of personal data of customers:

- **Personal data and contact information:** this includes, but is not limited to, first name, surname, gender, date of birth, age, marital status, AHV and insurance numbers, languages, nationality, cantonal and municipal affiliation, (e-mail) address, telephone number, health data, family members, etc.
- **Data related to communications:** this includes information such as preferred communication channel, correspondence and communication with Helsana by letter, e-mail, telephone, the myHelsana online client portal or by any other means (including records of communication), customer satisfaction, etc.
- **Contract data:** type of insurance and coverage, type and scope of benefits, date of entry and withdrawal, suspension, deductibles.
- **Data related to benefit processing:** this includes, among other things, service providers, diagnoses, medical reports, information from medical examiners, benefit costs, bank and post account details, payments, data from third-party insurers, information in connection with queries, invoices from the service provider.
- **Data related to the calculation and collection of premiums:** this specifically includes insurance premiums, premium invoicing, cantonal premium reduction, collection data, etc.
- **Data related to legal disputes:** this includes, in particular, data relating to complaints and differences regarding benefits and/or the contracts concluded for this purpose, such as recourse and disputes, as well as data from the case files of public authorities and courts, etc.
- **Data related to the use of the myHelsana online client portal:** this includes in particular IP addresses and other identifiers (e.g., MAC address of the smartphone or computer, cookies), access data (including passwords), date and duration of the insurance contract relationship, date, time and number of visits to the Website, pages and content accessed, referring websites.
- **Data related to the marketing of products and services:** this includes information such as newsletter subscriptions and unsubscriptions, documents received and special activities, personal preferences and interests, etc.
- **Data related to case management:** information on health, employer and employment relationship, medical, social and job-specific conditions and corresponding need for support, etc.

(collectively referred to as **customer data**).

Furthermore, Helsana processes the following categories of personal data of partners:

- **Data of service providers, contractors and other business partners and information on their employees and contacts,** in particular contact details, information about their function, information on previous dealings with these persons, information on marketing activities (e.g. receipt of newsletters), information on business transactions, requests, quotes, offers, conditions and contracts (in particular in connection with agreed rates), information on training and professional occupation, etc. (**partner data**).

Within the framework of their business relationship, customers will have to provide any customer data necessary or legally prescribed for the establishment and processing of the contractual relationship and fulfilment of the associated contractual obligations. As a rule, Helsana will not be able to conclude or execute the contract with the respective customer without this data. The same also applies to the partner data, to the extent that business relations with service providers, suppliers and business

partners of Helsana are concerned; in principle, these cannot be concluded and processed without information on their employees and other contacts. Access to services offered on the website (in particular in connection with the myHelsana client portal) and the related collection of connection data (such as IP addresses) must also be logged; this happens automatically during use and cannot be disabled for individual visitors or customers.

4.2 Data sources

The personal data is primarily collected in direct communication with customers (letter, contact and application forms, e-mail, telephone, or by other means) and within the context of website use.

Personal data may also be collected indirectly, in particular through

- persons and bodies authorised by customers;
- other (health) insurers both within and outside the Helsana Group (Art. 84a KVG);
- service providers and medical examiners;
- the exchange of information within the scope of mutual administrative assistance (Art. 32 of the Federal Act on the General Part of Social Insurance Law [ATSG]);
- publicly accessible sources (e.g. Internet, press, media, registers);
- purchase of additional information from third-party data sources (e.g. address traders).

4.3 Data processors or agencies involved

Statutory health insurance is primarily handled by employees of regional customer services and general agencies/sales offices. For this task, they process personal data including particularly sensitive personal data from Helsana's database (cf. Section 9).

When implementing statutory health insurance, employees have access to the data required for the respective task within the scope of the data processing activities listed below (the **data activities**):

- sales channel management and sales support;
- proposal preparation
- new customer business;
- customer service;
- contract management;
- benefits management;
- services contracting;
- staff insurance;
- medical examination service;
- public health sciences;
- collection, financial and actuarial services;
- risk compensation;
- audit, risk, legal and compliance;
- IT management and data protection management;

- provident fund;
- purchasing.

Process owners ensure compliance with the provisions of the instructions and regulations on data processing in connection with data-related activities at Helsana. They are responsible for ensuring that their application data is only made available within the legally defined framework.

4.4 Automated individual decision-making

At Helsana, automated individual decisions are made during benefit processing. If customers or service providers submit an invoice to Helsana, the system checks whether the benefit claimed falls under the statutory benefits catalogue (Art. 24 ff. Federal Health Insurance Act [KVG], Art. 33 ff. Health Insurance Ordinance [KVV] and Health Care Benefits Ordinance [KLV]) and thus also automatically decides whether an entitlement exists. No profiling is performed, as only the invoices are checked against contract and tariff data (cf. Section 4.5). If debt collection proceedings have been initiated in connection with collection services, the next steps (application for continuation of liquidation, bankruptcy proceedings, application for sale, etc.) are automated such that they are filed if the deadline has been exceeded but the claim has not yet been settled.

Automated individual decisions such as these are made because they are necessary for the fulfilment of the insurance contract between the customer and Helsana and because appropriate measures exist to ensure that the rights and legitimate interests of the data subjects are safeguarded (cf. Section 11).

4.5 Profiling

At Helsana, automated processing of personal data to evaluate certain personal aspects relating to natural persons (profiling) takes place in the following areas or for the following purposes:

- sales activities and customer surveys as well as offer management;
- payment behaviour and cost analysis.

Helsana evaluates data obtained from various sources according to specific criteria. It does this in particular to determine which products might be of interest to certain people or to develop products that are tailored to the needs of certain people.

5. Purpose and legal basis of data processing

5.1 Customer data

Customer data is primarily collected for the proper implementation of statutory health insurance in accordance with the following purposes defined by law (Art. 84 KVG):

- compliance with the insurance obligation;
- premium calculation and collection;
- assessment of benefit entitlements, the calculation and granting of benefits and coordination with the benefits granted by other social insurance schemes;
- assessment of the entitlement to premium reductions in accordance with Art. 65 KVG and the calculation and granting of reductions;

- enforcement of rights of recourse against a liable third party;
- keeping statistics;
- assignment and verification of the policyholder number of the old-age and survivors' insurance;
- calculating the risk compensation.
- announcements to third parties in accordance with Art. 84a KVG.

Moreover, data processing is performed in particular and to the extent permitted by law (also) for the following purposes:

- for the protection of customers, employees and other persons, especially in the event of threats to employees and data protection, the secrets and assets entrusted to Helsana, security of the systems and buildings of Helsana;
- in connection with services offered, contract conclusion, contract handling, the cultivation and development of customer relations, communication, customer service and support, promotions, advertising and marketing (including newsletters and sending of advertising material);
- management, operation and further development of the website (including the provision of functions requiring identifying factors or other personal data) and other IT systems, ID checks;
- compliance with the legal and regulatory requirements and internal rules of Helsana, prosecution and implementation of various rights, defence of legal claims, civil proceedings, complaints, combating abuse, for the purposes of legal investigations or proceedings and to respond to requests from authorities;
- quality control, market research, product and service development, compilation of statistics, budgets, records and management information and other reports on customers, transactions and activities, offers and other business aspects of Helsana for the purposes of managing and developing the company, its offering and activities, project management;
- sale or purchase of business divisions, companies or parts of companies and other corporate transactions and the associated transfer of customer data;
- for other purposes where a legal obligation requires processing and such processing was evident from the circumstances or indicated at the time of the collection

(together the **purpose of customer data processing**).

Helsana uses customer data for the purpose of customer processing on the following legal bases:

- contract fulfilment;
- fulfilment of a legal obligation on the part of Helsana;
- customer's consent (particularly if such processing is based on specific enquiries for which consent can be withdrawn at any time, such as for the receipt of newsletters subscribed to by the customer);
- legitimate interests of Helsana, especially
    - for the efficient, effective protection of customers, employees and other persons, for the protection of the data, secrets and assets of Helsana as well as those entrusted to it, and for the security of Helsana's systems and buildings;
    - compliance with the legal and regulatory requirements and internal rules of Helsana;

- efficient and effective customer care, cultivating contacts and other communication with customers for purposes other than those of contract processing;
- maintenance and secure, efficient and effective organisation of business operations including a secure, efficient and effective operation and successful further development of the website and other IT systems;
- sale and delivery of products and services, also with reference to persons who are not direct contractual partners (e.g. beneficiaries);
- meaningful corporate management and development;
- understanding customer behaviour, requests, existing conditions and needs, market studies;
- efficient and effective improvement of existing products and services and development of new products and services;
- conducting advertising and marketing;
- operating Helsana's website and other systems;
- successful sale or purchase of business divisions, companies or parts of companies and other corporate transactions;
- concerns regarding the prevention of fraud, offences and crimes as well as investigations in connection with such offences and other inappropriate conduct, handling of legal claims and proceedings against Helsana, participation in legal proceedings and cooperation with authorities, and otherwise the establishment, exercise of or defence of legal claims.

5.2 Partner data

Helsana may process partner data to the extent permitted by applicable data protection law, in particular for the following purposes: the conclusion and execution of contracts and other business relations with partners, promotions, advertising and marketing, communication, invitations to events and participation in special offers for partners, carrying out joint activities, compliance with the legal and regulatory requirements and internal rules of Helsana, tracking and implementation of various rights, defence of legal claims, civil litigation, complaints, combating fraud and abuse, for the purposes of legal investigations or proceedings and to respond to requests from authorities, for the sale or purchase of business divisions, companies or parts of companies and other corporate transactions and the associated transfer of partner data. It does so on the same basis as described above for customer data.

6. Disclosure of data to third parties

6.1 Duty of confidentiality

All employees of Helsana are obligated to uphold the duty of confidentiality (Art. 33 Federal Act on the General Part of Social Insurance Law ATSG). If they violate this duty of confidentiality, employees are subject to special statutory penalties (Art. 54 KVAG). Employees are aware of the penalties and also sign an agreement to maintain secrecy and confidentiality when they join Helsana.

6.2 Exceptions to the duty of confidentiality

The exceptions to the duty of confidentiality are governed by law (Art. 84, Art. 84a KVG and Art. 32 Federal Act on the General Part of Social Insurance Law ATSG) and exist, unless barred by an overriding personal interest, in particular for the processing of personal data by

- third parties on behalf of Helsana;
- additional third parties in individual cases if the person concerned has granted consent in writing, it is not possible to obtain consent, or consent may be assumed to be in the interest of the insured person under the given circumstances;
- other health or social insurance companies, insofar as this is necessary for the fulfilment of their statutory duties or there is a statutory disclosure obligation;
- other authorities, courts and official bodies (e.g. in connection with withholding taxes, federal statistics, criminal charges, crime prevention and premium collection).

Non-personal data may be disclosed if it is of overriding interest. Data of general interest may be published provided that the anonymity of the persons concerned is guaranteed.

6.3 Categories of third parties

To the extent permitted by applicable (data protection) law, Helsana may pass on customer data and partner data to the following categories of third parties who process the personal data for the respective processing purpose on behalf of Helsana or for their own purposes:

- persons concerned (especially insured persons) and third parties authorised by them;
- family head indicated in the contract (if applicable) with respect to data relating to other family members who are also insured;
- other companies of the Helsana Group (for example with Helsana Supplementary Insurances Ltd when examining an insurance application for supplementary insurance policies);
- other (health) insurers outside the Helsana Group;
- industry organisations, associations, organisations and other bodies;
- service providers, medical examiners, ombudsmen;
- contractors (inside and outside the Helsana Group); including order processors;
- suppliers and other business partners;
- acquirers or parties interested in acquiring business divisions, companies or other parts of Helsana;
- media;
- the public, including visitors to the websites and social media of Helsana;
- local, national and foreign authorities and official bodies (in particular federal and cantonal bodies, invalidity insurance offices, etc.);
- other parties in possible or actual legal proceedings.

7. Transfer of data abroad

Helsana may transfer customer data and partner data within Helsana as well as to third parties in any country of the world, especially to all countries in which the service providers of Helsana process their data (e.g. the Netherlands, Ireland, Germany). If data is transferred to a country without adequate data protection, Helsana guarantees adequate protection through the use of sufficient contractual guarantees, specifically on the basis of EU standard contractual clauses, binding corporate rules or based on exceptions with respect to consent, contract execution, the determination, exercise or enforcement of legal claims, overriding public interest, the data published by customers, visitors or partners, or because it is necessary to protect the integrity of these individuals. Customers, visitors and partners may request a copy of the contractual guarantees by sending a written request along with a copy of an official form of identification to the contact address specified above (see Section 3) or find out there where a copy of this nature may be obtained. Helsana reserves the right to black out such copies for reasons of data protection or secrecy.

In particular, data is transferred abroad to the joint institution which serves as the legal liaison body between Helsana and the social insurance institutions of EU countries, namely for the purpose of coordinating benefit statements (Art. 95a KVG and Art. 19 of the Health Insurance Ordinance).

8. Data retention

As a matter of principle, Helsana stores contract-related customer data and partner data for the duration of the contractual relationship and for ten years following the termination of the contractual relationship provided that, in individual cases, no shorter or longer legal storage obligations apply, this is necessary as evidence, another exception exists that is valid under applicable law, or earlier erasure is warranted (specifically because the data is no longer required or Helsana is obliged to delete it).

In the case of operational data containing customer data or partner data (e.g. protocols, logs), shorter retention periods of no more than thirteen months generally apply.

Business documents, including communication, are kept as long as Helsana has an interest in them (in particular, as evidence in the case of claims, documentation of compliance with certain statutory and other requirements, an interest in non-personal evaluation) or is obliged to do so (contractually, legally or on the basis of other requirements). This is without prejudice to statutory obligations, such as those which relate to the anonymisation or pseudonymisation of data.

9. Helsana database

9.1 Structure

The Helsana database is broken down by data activity and comprises the following categories:

- sales channel management and sales support;
- proposal preparation;
- new customer business;
- customer service;
- contract management;
- benefits management;

- services contracting;
- staff insurance;
- medical examination service;
- public health sciences;
- collection, financial and actuarial services;
- risk compensation;
- audit, risk, legal and compliance;
- IT management and data protection management;
- provident fund;
- purchasing.

Various interfaces, such as MediData, enable direct contact with external contractors and service providers, for example 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.

9.2 Usage and data access

9.2.1 Authorised users

Individuals authorised to access the Helsana information system 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**).

9.2.2 Authorised user management

Authorised users are managed centrally by the IT organisation of Helsana. Internal employees are reported via the HR interface and external employees via the respective sourcing. 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.

9.2.3 Personal access authorisation

When joining Helsana, each authorised user is granted access rights to information as defined in the role model and on the basis of his or her function. 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.

9.2.4 Cancellation of access authorisation

Authorised users only have access to the Helsana information system 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.

9.2.5 Training for authorised users

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

9.2.6 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 KVG for the entire insurance region of Switzerland.

9.2.7 IT service providers

To the extent that the operation of the Helsana information system is outsourced to external IT service providers, such external IT service providers follow the same regulations as the division.

10. Technical and organisational measures

10.1 Access control

All rooms at Helsana that are used to process particularly sensitive personal 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 electronic data carriers 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 electronic data carriers in decentralised servers and computers which are not operated by the IT organisation of Helsana are subject to similar security precautions as those which are operated by them.

10.2 Control of personal data carriers

Precautions implemented in the IT systems allow only authorised persons to process data on the electronic data carriers. Only authorised persons have access to the Helsana information system.

10.3 Authentication of authorised users

Access to the subsystems of the Helsana information system is protected by the user ID combined with a temporary individual password.

10.4 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).

10.5 Transmission of data

Data transmission between the data terminal stations and the host computers is protected by the transmission protocol.

10.6 Storage control

The authorised users receive specific authorisations to make changes to data fields as required for the purpose of carrying out their work in accordance with KVG.

10.7 Technical requirements for end devices

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

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

The data terminals are located in protected zones. Mobile data terminals contain data storage devices that are protected by a strong, password-based encryption method.

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.

10.9 Logging

In addition to controlling access to the Helsana information system by means of an authorisation procedure as well as the protection afforded by personal user IDs and passwords, some individual subsystems 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. This log is compiled in accordance with Art. 10 VDSG: Logs are retained for a thirteen-month period in compliance with audit requirements. They are only accessible to the bodies responsible for monitoring data protection and data security regulations and may only be used for this purpose. Some external IT service providers have their own similar yet different rules regarding audit logs.

10.10 Development

Requests for the system's further development are compiled and defined, budgeted and implemented as maintenance projects, small projects or projects. This approach is regulated within the scope of the "Helsana Project Procedure".

10.11 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 data terminals and the network is provided by the IT organisation of Helsana or outsourced.

The authorised users are informed of the Helsana information system's security rating as well as the regulations on how to handle the system and its data. The provisions are described in operation manuals under the heading of Information Security. The authorised users are aware of the penalties that could be imposed for intentional or negligent breaches of information security.

All authorised users are obliged to report the following findings to the process owner or representative of the authorised users:

- observed or suspected vulnerabilities or security deficiencies in the system;
- security measures that have not been implemented or observed;
- unforeseen events that may have an impact on information security.

10.12 Supervision and responsibility

The process owners of the subsystems are responsible for ensuring that the authorised users comply with the instructions and this data processing policy and that the external IT service providers comply with their contractual requirements.

11. Rights of customers, visitors and partners

Every person concerned, customer, visitor and partner has the right of access to personal data stored by Helsana concerning them. They also have the right to request that Helsana rectify, delete or restrict the processing of their personal data and to object to such processing of their personal data. If the processing of personal data is based on consent, the person concerned may withdraw this consent at any time. In EU/EEA countries, the person concerned has the right in certain cases to receive the data generated by their use of online services in a structured, commonly used and machine-readable format that enables the further use and transmission of such data. Requests related to these rights must be sent in writing to the contact address provided (see Section 3) along with a copy of an official form of identification. Helsana reserves the right to restrict the rights of the person concerned within the scope of the applicable law and, for example, to refrain from providing complete information or deleting data.

If Helsana automatically takes a decision concerning an individual person, which has a legal impact or significantly affects the person concerned in a similar way, the person concerned may speak to a competent person at Helsana and request a reconsideration of the decision, or demand from the very start that this be assessed by a competent person, to the extent provided for by law. In this case, the person concerned might no longer be able to use certain automated services. The person will be informed of such decisions subsequently or separately in advance.

Every person concerned has the right to file a complaint with the competent data protection authority. In Switzerland, this is the Federal Data Protection and Information Commissioner (http://www.edoeb.admin.ch).

12. Changes to the Privacy Policy

Helsana may modify this Privacy Policy at any time without advance notice and without notification. The version currently published on the Website shall apply.

If the Privacy Policy forms part of an agreement reached with customers and partners, Helsana may inform them of any changes by e-mail or in another suitable way in the event of an update. If no objection is received within thirty days, the new Privacy Policy shall be deemed to have been agreed. If an objection is lodged, Helsana shall be entitled to extraordinarily terminate the agreement without notice.

* * * * *