Helsana

Privacy policy and data processing policy
for Helsana Supplementary Insurances Ltd's Health Consultation service

As at 1 January 2021

1. Brief summary

At Helsana, we have high levels of expertise in health topics as well as in customer service. By making targeted use of these strengths, we can help our customers with their health concerns. Helsana Health Consultation is a neutral point of contact and offers our customers a higher quality of care and support in special circumstances.

The Health Consultation service can be accessed by telephone. You tell us your concern and we will give you our recommendations within 24 hours. The service is available to all customers, provided they have at least one supplementary insurance product with Helsana.

Our recommendations contain evidence-based information that allows informed decisions to be made on health issues in addition to behavioural tips. Among other things, we can help you

– find your way around the healthcare system
– communicate with doctors and other professional groups
– search for service providers
– cope with illnesses and symptoms, avoid illnesses, promote and maintain health and in special life situations

Health Consultation is not a medical service provider and therefore does not compete with doctors or other service providers. We do not intervene in the treatment and do not provide any diagnostic and treatment activities. This means that we do not determine the next steps for our customers and do not recommend that they stop taking a medication or that they continue a certain treatment. For these or similar questions we refer you to your general practitioner or the responsible therapist. Our medical advice service continues to be responsible for medical questions and matters of urgent concern.

Helsana only processes the data that you, as a customer, provide in the course of the health consultation.

This service is provided by Helsana Supplementary Insurances Ltd (Helsana).

Helsana attaches great importance to the protection of your personal data and provides information about the following in this privacy policy:

– who is responsible for data processing;
– which data is collected and processed;
– 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 data subjects.

2. Applicability of the privacy policy

This privacy policy explains the collection and processing of personal data by Helsana in connection with Helsana Health Consultation. It also serves as a data processing policy as defined by Art. 11 and Art. 21 of the Ordinance to the Federal Act on Data Protection (VDSG). 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 collection and processing of personal data in connection with the provision of individual health consultations, Helsana is the data controller (in particular in the sense 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 Supplementary Insurances Ltd
Data Protection Officer
P.O. Box
8081 Zurich

4. Collection, processing and use of personal data

4.1 Data subjects

Helsana collects and processes personal data of

– people who are insured with Helsana and have a supplementary insurance product.
– people who register as an authorised person or legal representative (these do not necessarily have to have insurance with Helsana).

and would like to use Health Consultation (collectively referred to as customers).

4.2 Affected data

Helsana specifically processes the following categories of personal data of customers:

- Personal data and contact information from the insurance relationship with Helsana: in particular, this includes first name and surname, gender, date of birth, insurance number, language, address, telephone number, e-mail address, preferred method of communication, insurance coverage, bank details and IBAN of the stored payment address.
- Data related to the recommended course of action and for quality assurance/customer feedback: this includes correspondence and communication with Helsana, primarily by telephone or letter (including records of communications), as well as assessments of the discussions and the quality of the recommendation; and data related to customer feedback.
- Data that you, as a customer, disclose to Helsana voluntarily so the health consultation can be carried out: this includes, but is not limited to, data about your own health (e.g. symptoms, treatments and therapies that have been carried out, service providers that have already been consulted, etc.), data about your financial situation (e.g. income, debt level, employment, profession, etc.).

5. Purpose and legal basis

Helsana Supplementary Insurances Ltd processes the information you provide purely to provide the aforementioned consulting services, for quality assurance purposes and to enhance the offer. This also applies to all other information arising from the insurance relationship (section 6).

The data collected for individual health consultations is processed and stored by a separate department on separate systems. Health Consultation is therefore strictly separated from the insurance business. The employees who carry out the activities (health advisors) do not have access to your health data from the insurance business. At the same time, even the employees of the insurance department cannot view the data collected in the course of the health consultation. The data will therefore not be used in the context of the insurance business.

6. Access to personal data from the insurance relationship

In order to take advantage of Helsana Health Consultation, you will first be identified when you call, and only the personal data and contact information from the insurance relationship mentioned above will be used.

7. Disclosure of data to third parties

Helsana Health Consultation is operated separately from the insurance business by Helsana. As a matter of principle, data collected and processed in the course of health consultations will not be passed on to the insurance business of Helsana Supplementary Insurances Ltd or to third parties, in particular the other Helsana Group companies.

An exception is the disclosure that a health consultation has taken place, including the time at which the contact was initiated, to the Helsana insurance business. However, no information is provided on the specific matter discussed. The exclusive purpose of the disclosure of the information is to ensure seamless customer care.

During the consultation, our health advisors may ask the customer to contact our telemedicine partner directly in the event of acute medical concerns. The health advisor can, with the customer's consent for that particular case, directly connect the customer by telephone, stating the insured person's insurance number and their specific situation.

8. Transfer of data abroad

Helsana may transfer the data provided to it by the customer for the individual health consultation and any additional insurance data to any country in the world, and in particular to all countries in which Helsana's service providers process their data (i.e. the Netherlands, Ireland, Germany, etc.). 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, 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 or partners, or because it is necessary to protect the integrity of these individuals. Customers 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 redact such copies for reasons of data protection or confidentiality.

9. Data retention

As a matter of principle, Helsana stores contract-related personal data from the health consultation for the duration of the Helsana Health Consultation contractual relationship and for ten years following the termination of the contractual relationship provided that, in individual cases, no shorter or longer legal retention obligations apply; this is necessary

for evidentiary purposes; another exception exists that is valid under applicable law; or earlier deletion is warranted (specifically because the data is no longer required or Helsana is obliged to delete it). Business records, including communications, are kept for as long as Helsana has an interest in them (in particular an interest in obtaining evidence in the event of claims, documentation of compliance with certain legal and other requirements, an interest in non-personal evaluation) or is obliged to do so (by contract, law or other requirements). This is without prejudice to statutory obligations such as those which relate to the anonymisation or pseudonymisation of data.

10. Data collected from the individual health consultation

10.1 Structure

The data collected from the health consultation provided by Helsana Supplementary Insurances Ltd may include the following categories:

- Category in the registered data collection
- Master data
- Health data
- Data on the financial situation
- Data on the social situation
- Data on the professional situation
- Quality assurance

10.2 Use and data access

10.2.1 *Authorised users*

The following are authorised to access the data:

- employees of Helsana, to the extent that they require such access to carry out their mandate;
- system administrators of Helsana;
- contractually mandated service providers;

(collectively referred to as authorised users).

10.2.2 *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 there is a valid employment contract or service contract.

10.2.3 *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 their function. Any other required rights must be requested individually. In this case, each request must be confirmed by the direct superior and, depending on the authorisation role, also by the role approver.

10.2.4 *Cancellation of access authorisation*

Authorised users 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.

10.2.5 *Training for authorised users*

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

10.2.6 *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 functional management of the responsible organisational units use specific instructions to establish a consistent benefit assessment level for the entire insurance region of Switzerland.

10.2.7 *IT service providers*

Insofar as data collection services are outsourced to external IT service providers, these follow comparable regulations within their purview.

11. Technical and organisational measures

11.1 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 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.

11.2 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 data collected by Health Consultation.

11.3 Authentication of authorised users

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

11.4 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).

11.5 Transmission of data

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

11.6 Storage control

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

11.7 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.

11.8 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. office cleaning 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.

11.9 Logging

In addition to controlling access to the data 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 13-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. In some cases external IT service providers have similar in-house rules regarding auditing.

11.10 Development

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

11.11 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 persons authorised to access the system are informed about the security classification of the data collection and the regulations for handling 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.

11.12 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.

12. Rights of customers

Every data subject and every customer has the right of access to personal data stored by Helsana concerning them. They also have the right to request that Helsana rectify, erase 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 data subject may withdraw this consent at any time. In EU/EEA countries, the data subject 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 data subject 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 data subject in a similar way, the data subject 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 data subject might no longer be able to use certain automated services. The person will be informed of such decisions subsequently or separately in advance.

Every data subject 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).

13. Changes to the Privacy Policy

Helsana reserves the right to amend this privacy policy at any time without prior notice or notification. The version currently published on the website shall apply.

If the privacy policy forms part of an agreement with the customer, Helsana may inform the customer of any changes by e-mail or in another suitable way in the event of an update. If no objection is received within 30 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.