

Privacy Policy of the Helsana Group



General personal data
We process general personal data relating to you.



Financial data
We process your financial data.



Health data
We process your health data.



Biometric data
We process your biometric data.



Privacy
We process data relating to your private/personal life.



Shared data
We process personal data you have shared with us.



Collected data
We process personal data that we collect about you.



Received data
We process personal data about you that we receive from third parties.



Marketing
We use your personal data for marketing and advertising.



Product development

We use your personal data for the development and improvement of insurance products and services.



Other purposes

We use your personal data for other purposes not associated with the main service provided.



Profiling

We analyse your behaviour and make assumptions regarding your interests and preferences.



Automatic decisions

We make some decisions on a fully automated basis.



Transfer of data

We share your personal data with other companies that decide for themselves how to use the data.



Worldwide

We sometimes process your personal data outside of Switzerland and the EU.

Content

1.	What's this Privacy Policy about?	4
2.	Who is responsible for processing your data?	4
3.	What data do we process?	5
4.	Whose data do we process?	6
5.	Where do we get your data from?	7
6.	Why do we process your data?	7
6.1	Processing purposes pursued by the individual insurance companies	7
6.2	Processing purposes pursued by all insurance companies collectively	8
7.	On what basis do we process your data?	9
7.1	Data processing as a federal body	9
7.2	Data processing as a private individual	10
8.	What are the rules regarding profiling and automated individual decision making?	10
8.1	Profiling	10
8.2	Automated individual decision making	11
9.	Who do we share your data with?	11
10.	Is your personal data sent abroad?	12
11.	How long do we process your data?	13
12.	How do we protect your data?	13
13.	What are your rights?	13
14.	What data do we process on our pages on social media networks?	14
15.	Is this Privacy Policy subject to change?	15

1. What's this Privacy Policy about?

The insurance companies of the Helsana Group (hereinafter «**Helsana**», «**we**» or «**us**») obtain and process personal data relating to you or other individuals (referred to as «**third parties**»). This Privacy Policy applies exclusively to the insurance companies of the Helsana Group, i.e. exclusively Helsana Insurance Company Ltd, Helsana Supplementary Insurances Ltd and Helsana Accidents Ltd.

We use the terms «**data**» and «**personal data**» interchangeably here. «Personal data» refers to data that relates to a specific or identifiable person, i.e. which enables their identity to be inferred based on the data itself or through corresponding additional data. «**Sensitive personal data**» is a category of personal data that enjoys special protection under the applicable privacy law. Sensitive personal data might, for example, include health data. Section 3 lists all the data that we process within the context of this Privacy Policy. «**Processing**» refers to any operation involving personal data, e.g. obtaining, saving, using, altering, disclosing and deleting.

In this Privacy Policy, we describe what we do with your data if you purchase or use **insurance products** or **services**, use the customer portal **myHelsana** (incl. the app), have any **other relationship with us within the framework of a contract**, **communicate** with us or otherwise **associate with us**. We may write to notify you in advance of additional processing activities not yet mentioned in this Privacy Policy. We may also inform you of the processing of your data separately, e.g. in declarations of consent, contractual conditions, additional privacy declarations, forms and notices.

This Privacy Policy **does not apply** to our apps Helsana+, Helsana Coach and Helsana Trails or Helsana's health consultation as there are separate privacy policies for these. If you use our website, www.helsana.ch, the separate [Privacy and Cookie Policy](#) applies.

There are also separate privacy policies applicable to data handling in the recruitment process as well as to the employees of Helsana Insurance Company Ltd that **supplement** this general Privacy Policy.

This Privacy Policy is construed based on the requirements of the Federal Data Protection Act («**FADP**») including the Ordinance to the Federal Act on Data Protection («**DPO**») and the EU General Data Protection Regulation («**GDPR**»). However, if and to what extent these regulations are applicable depends on the individual case.

2. Who is responsible for processing your data?

The following companies are responsible under privacy law for the data processing operations of the Helsana Group insurance companies described in this privacy policy, unless communicated otherwise in individual cases (e.g. in other privacy policies, on forms or in contracts):

- **Helsana Insurance Company Ltd**, Dübendorf, («**HVAG**») for all data processing in the context of social health insurance under the Federal Health Insurance Act («**KVG**») and all data processing outside of insurance business (e.g. service contracts, collaboration with business partners, lease agreements, etc.)
- **Helsana Supplementary Insurances Ltd**, Dübendorf, («**HZAG**») for all data processing in the context of supplementary insurance in accordance with the Federal Insurance Contract Act («**VVG**»)
- **Helsana Accidents Ltd**, Dübendorf, («**HUAG**») for all data processing in the context of compulsory and voluntary insurance under the Federal Accident Insurance Act («**UVG**»)

HZAG and HUAG have outsourced certain activities to HVAG and their employees are employed by HVAG under employment law. HVAG employees are therefore in the employment of HVAG, HZAG and HUAG, each of which operate as insurers in their own right.

To voice your privacy concerns or exercise your rights under section 13, you can refer to our data protection advisor (Art. 10(1) and (4) FADP in conjunction with Art. 23 and Art. 25 DPO):

Helsana Group
Data Protection Advisor
PO Box
8081 Zurich
privacy@helsana.ch

Where Helsana falls within the scope of the GDPR, Active Assets A2 GmbH is both its Data Protection Officer for the purposes of Article 37 GDPR and its representative for the purposes of Article 27 GDPR. Its contact details are as follows:

Active Assets A2 GmbH
Gottlieb-Daimler-Str. 5
DE-78467 Constance
privacy@helsana.ch

3. What data do we process?

We process various different categories of data relating to you, using current and sometimes earlier information if details have changed. The most important categories are listed below:

- **Personal master data:** all contact details of customers (private and corporate customers), service providers, employees (incl. applicants and insured employees), potential customers, sales partners and other contractual as well as other individuals and legal entities.
This includes but is not limited to first name and surname, gender, date of birth, marital status, AHV and insurance numbers, languages, nationality, cantonal and municipal affiliation, (e-mail) address, telephone, biometric data, family members, PAR number, company, Cicero number and HK number.
- **Communications data (incl. legal disputes):** all data consisting of recorded communications among employees and communications between Helsana and its customers (private and corporate customers) and external partners. The content of this data is generally unstructured.
This includes but is not limited to preferred channels of communication, journal entries, e-mails, written correspondence, recorded telephone calls, customer feedback, surveys and newsletters. Litigation data relates particularly but not solely to 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.
- **Marketing data:** data that Helsana uses to acquire new customers and new business.
This includes but is not limited to details such as personal preferences and interests, leads (contact/sales opportunities), campaign data, opt-in/opt-out data, market data and sociodemographic data.
- **Compensation data:** data obtained in connection with the compensation of sales partners.
This might include new business commission or brokerage fees.
- **Application data:** data obtained in connection with the quote/application process.
This includes but is not limited to quotes, applications, quoted/requested coverage, health declarations and risk assessment data.
- **Insurance contract and premium data:** data obtained in connection with insurance contracts (in personal and corporate customer business).
This includes but is not limited to the type of insurance and coverage, the date of entry, date of withdrawal, signature and contract conclusion, premiums, deductibles.
- **Benefit data (incl. case management):** data obtained in connection with benefit processing (in personal and corporate customer business).
This includes but is not limited to data from service providers, diagnoses, medical reports, benefit costs, data from third-party insurers, data in connection with queries, invoices of service providers, etc. Furthermore, personal, job-specific, family-related and financial data are processed in Case Management.

- **Medical examination service data:** all data obtained in the context of the medical examination service (VAD) and managed there.
This includes but is not limited to benefit claims, diagnoses and expert medical opinions.
- **Collections/disbursement data:** data obtained in connection with accounting.
This includes but is not limited to open positions, invoices, payments, reimbursement claims and information related to payment history.
- **Health platform data:** data stored in the context of information within the health portal.
This includes but is not limited to bonus points or customer evidence in relation to bonus points (e.g. activities). See the separate privacy policies for Helsana+, Helsana Coach and Helsana Trails for details.
- **HR data:** data required in addition to personal master data to manage employees.
This includes but is not limited to data from the HR file, application documents, target agreements, payroll accounting, working hours and education and training. See the separate HR and Recruiting Privacy Policies for details.
- **Compliance data:** data required for assessing the compliance of Helsana business processes or privacy breaches.
This includes but is not limited to compliance assessment, compliance breaches, including supervisors or those involved in a data breach.
- **System usage data (internal, external):** data logged on the use of applications (internal) and portals (external) to guarantee user management and, where necessary, the tracking of user behaviour.
This includes but is not limited to usernames, passwords, personal settings, login/ logout times, accesses and user behaviour.

4. Whose data do we process?

We collect and process data from the following categories of individuals:

- **IB customers:** Customers in individual business (IB) are individuals with a current, future or past insurance contractual relationship with us.
- **CD customers:** Corporate division (CD) customers are legal entities that have an insurance contractual relationship with us.
- **Potentials:** Potentials are those our campaigns are aimed at. Potentials may refer to customers and partners without a previous business relationship with us.
- **App users:** We use the term app users to refer to individuals that use our apps. These may (but must not) be customers of ours.
- **Service providers:** Service providers provide a service for insured persons that can be paid for by insurance cover. Service providers for social health insurance are defined in Art. 35 of the Federal Health Insurance Act (KVG). The term also covers service providers from the field of supplementary insurance as defined by the Federal Insurance Contract Act (VVG) and recognised by HZAG and HUAG.
- **IB sales partners:** IB sales partners market HVAG and HZAG insurance products in the individual business segment and are compensated for this. Sales partners could be our internal employees (e.g. IB insurance consultants) or external parties (e.g. brokers). This also includes brokers that act as intermediaries for IB group contracts.
- **CD sales partners:** CD sales partners market HZAG and HUAG insurance products in the corporate division and are compensated for this. Sales partners could be our internal employees (e.g. CD insurance consultants) or external parties.
- **Helsana employees (incl. applicants, PVS policyholders):** Helsana employees refer to our employees, those that apply for a position with us and those included in our provident fund (PVS).
- **Other persons:** Other persons whose personal data we process and who not covered by the categories of individuals explicitly listed.

5. Where do we get your data from?

Much of the data mentioned in section 3 is **data you have shared with us** (e.g. in forms, in communication with us, in connection with contracts, when using the website, etc.). If you conclude contracts with us or want to use our services, you must also provide us with data as part of your contractual obligation under the relevant contract, specifically personal master, application and contract data. If you would like access to certain systems, you must also provide us with usage data.

Sometimes **we also collect data from third parties about you**: this primarily includes information from public registries, information we have obtained in connection with regulatory and court proceedings, information in connection with your occupational role and activities (to allow us to conclude and transact business with your employer with your help as an employee), information about you in correspondence and discussions with third parties, credit checks (where we transact personal business with you), information about you provided to us by people within your environment (family, advisors, legal representatives, etc.) so we can conclude or administer contracts with you or involving you (e.g. references, your address for deliveries, power of attorney, details of compliance with statutory requirements such as those aimed at preventing fraud), information from banks, insurance companies and sales partners and other contractual partners of ours regarding the use or provision of services (e.g. payments, purchases, etc.), information from the media and internet relating to you (where this is warranted in the specific case, e.g. in the context of an application, marketing, sales, etc.), your address from address brokers and, where applicable, interests and other sociodemographic data (specifically for marketing and research) and data in connection with the use of external website and web presences, where use of these can be attributed to you.

If you share data with us relating to others, such as family members, work colleagues, etc., we proceed on the assumption that you are authorised to do so and that this data is correct. You confirm this when you transmit third-party data to us. Please also ensure that these third parties have been informed of this privacy policy.

6. Why do we process your data?

We process your data for the purposes explained in the following. You can find further information in section 14 on how this relates to social media. You can find out more about the legal bases for our processing in section 7.

6.1 Processing purposes pursued by the individual insurance companies

HVAG processes your data primarily for the purpose of **administering social health insurance**. This includes compliance with the insurance obligation, assessing the entitlement to premium reductions and calculating and granting reductions, calculating risk compensation and sharing data with third parties in accordance with Art. 84a of the Federal Health Insurance Act (KVG). In addition, HVAG processes your data to check whether you are eligible for case management. The result of the check is checked manually by our employees and if you are effectively eligible for case management, you will be contacted.

HUAG processes your data primarily for the purpose of **administering compulsory and voluntary accident insurance**. This includes compliance with the insurance obligation and sharing data with third parties in accordance with Art. 97 f. of the Federal Accident Insurance Act (UVG). Where corporate customers are concerned, HUAG also processes data for the purposes of quality control, budgets, records and management information and other reports on customers, transactions and activities, offers and other business aspects of HUAG for the purposes of managing and developing the company, its offering and activities as well as project management.

HZAG processes your data primarily for the purpose of **administering supplementary insurance**. This includes, among other things, the risk assessment as part of the application process, the

development of underwriting regulations, any breach of the notification obligation following the conclusion of the insurance contract and maintaining and developing customer relations. Where corporate customers are concerned, HZAG also processes data for the purposes of quality control, statistics, budgets, records and management information and other reports on customers, transactions and activities, offers and other business aspects of HZAG for the purposes of managing and developing the company, its offering and activities as well as project management.

6.2 Processing purposes pursued by all insurance companies collectively

Helsana also processes data for **administering insurance contracts** for the following purposes: assessing entitlement to benefits (incl. invoice checking and checking efficacy, expediency and cost-effectiveness) as well as the benefit statement, granting of benefits and coordination with the benefits of other (social) insurance providers; enforcing rights of recourse against a liable third party (regress); statistics. We also process data for the pursuit and implementation of various rights, the defence of legal claims, conducting civil proceedings, for the purposes of legal investigations or proceedings and to respond to requests from authorities.

We primarily conclude insurance contracts with our corporate and private customers. However, we can also conclude **various types of contracts** with our corporate customers, with suppliers, sub-contractors or other contractual partners, such as partners in projects or parties in legal disputes. In the course of initiating new business, data is collected from or arises through communication with potential customers or other contractual partners (e.g. in an application or order form or contract). As part of administering contractual relationships, we process data to manage the customer relationship, to provide and claim contractual services (which also includes enlisting third parties, such as logistics companies, advertisers, banks, insurance companies or credit agencies, who then supply us with data for their part), for consultation and for customer care. The enforcement of legal claims from contracts (collection, court proceedings, etc.) also falls under this administration, as does bookkeeping, terminating contracts and public communications.

We process your data for the purposes of **communicating** with you, responding to requests and asserting your rights (section 13) and contacting you in the event of any enquiries. We retain your data in order to document our communications with you, for training purposes, for quality assurance and for queries.

We process your data for **marketing purposes and for maintaining relations**, e.g. to send our customers and other contractual partners advertisements for products and services of theirs and third parties (e.g. of contractual partners). This may, for example, take the form of newsletters and other regular contact (electronic, by post, by phone), via other channels, for which you have given us contact details, but also as part of individual marketing campaigns (e.g. events, competitions, etc.) and may include free services (e.g. vouchers). When we send mailings and newsletters, we can track whether the message and has been opened/who has opened the message and when and whether they have clicked on the links contained within it. You can reject this type of contact at any time (see the end of section 6) or deny or revoke your consent to be contacted for advertising purposes. Ultimately, we also want to enable our contractual partners to contact our customers and other contractual partners for advertising purposes (see section 9).

We also process your data for **market research**, to **improve our services and our business** and for **product development**. We are committed to improving our products and services on an ongoing basis and responding quickly to changing needs. For this reason, one of the things we analyse is why specific group categories opt for certain products and how they do so, and the form new products and services can take. This provides an indication of the market acceptance of existing insurance products and services and the market potential for new insurance products and services.

We may also process your data for **security purposes** and **access control**. We check and improve the adequate security of our IT and our other infrastructure (e.g. buildings) on an ongoing basis. Like all companies, we cannot rule out the risk of data breaches with absolute certainty, but we do our utmost to reduce the risks. As such, we process data for monitoring, checks, analyses and tests of our

networks and IT infrastructures, for system and error checks, for documentation purposes and as part of security backups. Access controls include monitoring access to electronic systems (e.g. logging into user accounts) but also physical access checks (e.g. building access). For security purposes (preventative and to investigate incidents), we also keep access logs or visitor lists and use monitoring systems (e.g. video surveillance).

We process personal data to **comply with laws, directives and recommendations by regulatory authorities and internal regulations** («**Compliance**»). For instance, we may be obliged to report to the authorities in certain cases. The fulfilment of information or reporting duties in connection with regulatory and tax law obligations may also require or entail data processing, e.g. fulfilling archiving duties and preventing, uncovering and investigating offences and other breaches (e.g. insurance misuse). This includes receiving and handling complaints and other reports, monitoring communications, internal investigations or disclosing documents to a regulatory authority if we have a reasonable reason or are legally obliged to do so. Your data may also be processed in the event of external investigations, e.g. by a law enforcement or supervisory authority or a commissioned private body. The legal obligations may be Swiss law, but also foreign regulations to which we are subject, as well as self-regulation, industry standards, our own corporate governance and regulatory orders and requests.

We also process data for the purposes of our **risk management** and in the context of prudent **corporate governance**, including business organisation and corporate development.

We may also process your data anonymously for **research purposes** (e.g. for human research in accordance with the Human Research Act). If no anonymised data is to be used, the data subjects will either be informed separately about the corresponding research project or their consent will be obtained in advance.

We can process your data **for other purposes**, e.g. as part of our internal processes and administration or for training and quality assurance purposes. These other purposes include, for example, training and education purposes, administrative purposes (such as the administration of personal master data, accounting, data archiving and the examination, administration and continuous improvement of IT infrastructure), the protection of our rights (e.g. to enforce claims in court, before or out of court and before authorities in Switzerland and abroad or to defend ourselves against claims, for example by preserving evidence, legal clarifications and participation in judicial or official proceedings) and the evaluation and improvement of internal processes. We may use recordings of (video) conferences for training and quality assurance purposes. The protection of other legitimate interests also falls under our non-exhaustive list of other purposes.

7. On what basis do we process your data?

7.1 Data processing as a federal body

HVAG acts as a federal body in its data processing as part of its activities as a social health insurer, as does HUAG as part of its activities as a compulsory accident insurance provider. As such, HVAG and HUAG process your data in these areas primarily on a **legal basis** (specifically Art. 84 KVG and Art. 96 UVG).

HVAG and HUAG may also process your data based on your **consent in the individual case** or if you have **made the data generally accessible** and have not explicitly forbidden any such processing. You can revoke consent at any time by providing HVAG and HUAG with written notice (by post) or, unless stated or agreed otherwise, by e-mail with future effect; you can find the contact details in section 2. Once they have received notice of the revocation of your consent, they will no longer process your data for the purposes to which you originally consented, unless they have other legal grounds for doing so. The withdrawal of your consent will not affect the lawfulness of processing based on said consent before its withdrawal.

Finally, HVAG and HUAG also process your data where **processing is necessary to protect the life or physical integrity** of you or a third party and you cannot provide consent within a reasonable timeframe.

7.2 Data processing as a private individual

Where we are not operating as a federal body (see above), we process your data as a private individual (e.g. all HZAG activities, HVAG activities with business partners, HUAG activity as part of voluntary accident insurance). On the one hand, your **consent** forms the basis for this data processing. In such cases, we will inform you separately about the relevant processing purposes. You can revoke consent at any time by providing us with written notice (by post) or, unless stated or agreed otherwise, by e-mail with future effect; you can find our contact details in section 2. If you have a user account (e.g. for myHelsana), you may also be able to revoke consent or contact us via the relevant website or other service. Once we have received notice of the revocation of your consent, we will no longer process your data for the purposes to which you originally consented, unless we have other legal grounds for doing so. The withdrawal of your consent will not affect the lawfulness of processing based on said consent before its withdrawal.

Where we do not ask for your consent to processing, we conduct the processing on the basis that said processing is necessary for **initiating or administering a contract** with you (or the entity represented by you) or that we or third parties have an **overriding interest** in this. Our overriding interests include the pursuit of the purposes described in section 6 above and the associated objectives and the ability to take corresponding measures. Our overriding interests also include compliance with statutory regulations, provided this is not already recognised as a legal basis by the respective applicable data protection law anyway (e.g. in the case of the GDPR, the law in the EEA and in Switzerland). But that also includes marketing our products and services, our interest in better understanding our market and our company, including securely and efficiently conducting and further developing our operational business. Furthermore, our overriding interests also include the efficient, effective protection of customers, employees and other persons, the protection of data, secrets and assets of Helsana as well as the security of Helsana's systems and buildings.

If we receive sensitive data (e.g. health data), we can also process your data based on other legal grounds, e.g. in the event of disputes based on the need for processing for any lawsuit or the enforcement or defence of **legal claims**. Other legal bases may apply in individual cases; we will inform you of this separately where necessary.

8. What are the rules regarding profiling and automated individual decision making?

8.1 Profiling

Based on your data (section 3), we may automatically evaluate some of your personal characteristics («**Profiling**») for the purposes outlined in section 6 if we want to generate preference data, but also to identify misuse and security risks, to undertake statistical analyses or for operational planning purposes. We can also generate profiles for the same purposes, i.e. we can combine behaviour and preference data, but also personal master, contract and benefit data and system usage data attributed to you, in order to better understand you as a person with your different interests and other characteristics.

If you are an HZAG customer, HZAG can use profiling based on your benefit data to determine which other products might be of interest to you. It can also process your data with the assistance of artificial intelligence (AI) to this end. It can also check the credit rating and payment history of you and other insured persons in the same contract and analyse the costs generated to conduct personalised

advertising campaigns. HZAG also uses profiling for product development and to check the costs of service providers in order to reduce benefit costs and to prevent fraud.

We monitor the proportionality and reliability of results and take measures to avoid any misuse of profiling or profiles. If these have the potential to cause legal implications or significant disadvantages for you, we generally provide for a manual review.

8.2 Automated individual decision making

In certain situations, for reasons of efficiency and uniformity of decision-making processes, it may be necessary for us to automate discretionary decisions concerning you with legal effects or potentially significant disadvantages («**automated individual decisions**»). This does not mean pure if-then decisions (e.g. if the computer allows you to access your user account after checking your password), but discretionary decisions (e.g. the decision to conclude a contract).

In this case, we will inform you accordingly and provide the measures required by applicable law. If you do not agree with the outcome of such a decision, you will be able to communicate with a person who will review the decision.

9. Who do we share your data with?

All of our employees are subject to the professional **duty of confidentiality** as defined under Art. 62 FADP. If employees work for HVAG as part of the administration of social health insurance or for HUAG as part of the administration of compulsory accident insurance, they are also subject to a duty of confidentiality in accordance with Art. 33 of the Federal Law on General Provisions concerning Legislation on Social Insurances (ATSG).

There are however **exceptions** provided for by law to the statutory duty of confidentiality: for instance, while administering social health insurance (Art. 32 ATSG in conjunction with 84a KVG), HVAG may issue data to third parties, as can HUAG while administering compulsory accident insurance (Art. 32 ATSG in conjunction with Art. 97 f. UVG). In addition, exceptions to professional secrecy also apply to us in our activities as a private individual in accordance with insurance contracts, power of attorney or in the case of an overriding private interest.

In connection with our contracts, our services and products, our legal obligations or otherwise to safeguard our overriding interests and the other purposes listed in section 6, we may also transfer your personal data to third parties, in particular to the following categories of recipients:

- **Group companies:** For instance, in the context of a risk assessment for an insurance application, HZAG may request data from HVAG in relation to you based on your consent in the insurance application.
- **Service providers and other insurers:** We share data (incl. health data) with service providers (incl. medical examiners as part of administering social health insurance and consulting physicians as part of administering voluntary supplementary insurance and accident insurance) and the ombudsman. We also share data with Medi24 Ltd (e.g. for personal medical advice). We may also share data with other insurers (health and accident insurers).
- **Service providers:** We work with service providers at home and abroad so that we can provide our products and services efficiently and concentrate on our core competencies. These services relate, for example, to IT services, sending information, marketing, sales, communication or printing services, building management and cleaning, organisation and hosting of events and receptions, some aspects of collection, credit agencies, address verifiers (e.g. for updating address lists during moves), services of consulting firms, lawyers, banks, insurers and telecommunications companies. We supply these service providers with the data they require for their services, which may also relate to you. We conclude contracts with these service providers that provide for the protection of data, insofar as such provisions are not already stipulated by law. Our service providers may also

process data on how their services are used and other data generated through the use of their services as independent controllers for their own overriding interests (e.g. for statistical evaluations or billing). Service providers provide information about their own independent data processing in their own privacy policies.

- **Contractual partners (including customers):** These are corporate customers (e.g. your employer in the case of daily sickness benefits or accident insurance) and other contractual and sales partners of ours, because this data is transmitted on the basis of these contracts. They receive data about the portfolio, registration data on issued and redeemed vouchers, invitations, etc. If you work for any such contractual partner yourself, we may also transmit data about you in this context. This may also include health data. Data recipients also include contractual partners with whom we cooperate or who advertise for us and to whom we therefore transmit data about you for analysis and marketing purposes (these may in turn be service recipients, but also sponsors and providers of online advertising for example). We require these partners to only send or serve advertising to you based on your data if you have consented to this.
- **Authorities:** We may pass on personal data to offices, courts and other authorities in Switzerland and overseas if we are legally obliged or entitled to do so or if this appears necessary to safeguard our interests. This may also include health data. The authorities process data about you that they receive from us on their own responsibility.
- Scenarios where this applies include, for example, criminal investigations, regulatory requirements and investigations, court proceedings, reporting obligations as well as legal information and cooperation obligations. Data may also be disclosed if we want to obtain information from public authorities, e.g. to justify an interest in information or because we have to indicate whose information we require (e.g. from a register).
- **Other persons:** This refers to other cases where third parties need to be enlisted for the purposes outlined in section 6. Other recipients might, for example, be different addressees specified by you or external payees, the family contact person for the contract, other third parties including in the context of representation relationships (e.g. if we send your data to your lawyer or bank) or persons involved in official or court proceedings. As part of business development, we may sell or acquire businesses, parts of businesses, assets or companies or enter into partnerships, which may also result in the disclosure of data (including yours, e.g. as a customer or supplier) to the persons involved in these transactions. Communications with our competitors, industry organisations, associations and other bodies may also involve data concerning you being exchanged.

All these categories of recipients may in turn involve third parties, meaning your data may also be accessible to them. We may restrict processing by certain third parties (e.g. IT providers), but not those of other third parties (e.g. authorities, banks, etc.).

Your data is covered by an appropriate level of data security even after disclosure in Switzerland and the rest of Europe. The provisions of section 10 apply to the disclosure of data in other countries. If you would not like certain data to be shared, please let us know so that we can check whether and to what extent we can accommodate you (section 2).

We also enable **certain third parties** to collect **personal data from you** (e.g. media photographs), such as at our events. Insofar as we are not significantly involved in the collection of this data, these third parties alone are responsible for said data collection. In the event of any concerns or to assert your privacy rights, please refer to these third parties directly.

10. Is your personal data sent abroad?

As explained in section 9, we share your data with other agencies. These are also located outside of Switzerland. Your data may therefore be processed in Europa (particularly in the Netherlands, Ireland or Germany, but also in other European states) and, in exceptional cases, any other country worldwide.

If a recipient is based in a country without adequate statutory data protection, we will impose a contractual obligation to comply with privacy guidelines on the recipient (for this, we use the new standard

contractual clauses of the European Commission, including the adaptations for Switzerland required by the Federal Data Protection and Information Commissioner [FDPIC]), where said recipient is not already subject to a recognised regulatory framework for ensuring data protection and there is no exemption clause we can use. Exemptions may apply, for instance, in the case of legal proceedings overseas, but also in cases of overriding public interest or if the execution of a contract requires that such information be shared, if you have consented to this, or if this data is data you have made generally accessible and you have not objected to its processing.

It should also be noted that data shared over the internet is frequently routed via third countries. This means your data may be transmitted abroad even if the sender and the recipient are located in the same country.

11. How long do we process your data?

We process your data as long as our processing purposes, statutory retention periods and our overriding interests in processing for documentation and evidence purposes require it or where processing takes place for technical reasons. Unless legal or contractual obligations stipulate otherwise, we will delete or anonymise your data following the expiry of the storage or processing duration associated with our standard processes.

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 or an interest in non-personal evaluation) or is obliged to do so (by contract, law or other requirements).

12. How do we protect your data?

We take appropriate security measures to protect the confidentiality, integrity and availability of your data, to protect it against unauthorised or unlawful processing and to prevent the risk of loss, unintentional alteration, unwanted disclosure or unauthorised access.

Security measures of a technical and organisational nature may, for example, include measures such as the encryption and pseudonymisation of data, logging, access restrictions, saving backup copies, instructions for our employees, confidentiality agreements, access controls, personal data carrier checks, authentication of access rights, disclosure and storage controls.

We also impose requirements on our contract processors to take appropriate security measures. However, security risks cannot be ruled out entirely; residual risks are unavoidable.

13. What are your rights?

Under certain circumstances, the applicable data protection law may grant you the right to object to the processing of your data, particularly for the purposes of direct marketing, profiling undertaken for direct marketing and other legitimate interests in processing.

To make it easier for you to control how your data is processed, you have the following rights in connection with our data processing depending on the applicable data protection law:

- The right to seek information from us as to whether and which data of yours we process
- The right to have us correct data if it is inaccurate
- The right to ask us to delete data
- The right to have us issue certain personal data in a standard electronic format or to transmit this to another controller
- The right to revoke consent insofar as our processing is based on your consent
- The right to demand further information that might be of use in exercising these rights

- Where automated individual decisions (section 8) are concerned, the right to present your view and that the decision be reviewed by an individual

If you would like to exercise one of the above-listed rights against us, please refer to us in writing or in person at one of our branches or, unless stated or agreed otherwise, via e-mail; you can find our contact details in section 2. To allow us to prevent misuse, we will require you to identify or authenticate yourself (e.g. with a copy of your ID).

You also have these rights with respect to other entities that collaborate with us on an independent basis – please refer directly to these if you want to exercise rights in connection with their processing.

Please note that these rights are subject to requirements, exceptions and restrictions in line with the applicable data protection law (e.g. to protect third parties or trade secrets). In particular, we may have to continue to process and save your data to fulfil a contract with you, to protect our own legitimate interests, i.e. asserting, exercising or defending legal claims, or to comply with statutory obligations. Insofar as legally permissible, specifically for the protection of the rights and freedoms of data subjects, we may also fully or partially reject a data subject request (e.g. by redacting certain content relating to third parties or our trade secrets). We will inform you of this where necessary.

If you do not agree with our handling of your rights or privacy, please let us know (for contact details see section 2). Particularly if you reside in the EEA, in the United Kingdom or Switzerland, you are also entitled to lodge a complaint with the privacy supervisory authority of your country.

You can contact the Swiss supervisory authority here:

<https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/adresse.html>

You can find a list of the authorities in the EEA here:

https://edpb.europa.eu/about-edpb/board/members_de

You can contact the supervisory authority of the United Kingdom here:

<https://ico.org.uk/global/contact-us/>

14. What data do we process on our pages on social media networks?

We may operate pages and other online presences on social media networks and other third party-run platforms (fan pages, channels, profiles, etc.) and collect data there in relation to you as described in section 3 and beyond. We obtain this data from you and the platforms if you contact us via our online presence (e.g. if you communicate with us, comment on our content or visit our presence). At the same time, the platforms analyse your use of our online presences and link this data to other data about you held by the platforms (e.g. in relation to your behaviour and your preferences). They also process this data for their own purposes on their own responsibility, in particular for marketing and market research purposes (e.g. personalising advertising) and to manage their platforms (e.g. what content they show you).

We process this data for the purposes described in section 6, i.e. specifically for communication, marketing purposes (including advertising on these platforms, see also the separate **Privacy and Cookie Policy**) and market research. For the corresponding legal bases, see section 7. We can process content you yourself have published (e.g. comments on a post), such as in our advertising on the platform or elsewhere. We or the platform providers may delete or restrict content from or in relation to you in line with the terms of use (e.g. inappropriate comments).

Please refer to the privacy policies of the respective platforms for further information as to what data is processed by the operators. These also indicate the countries in which your data is processed, what rights of information, erasure or other rights you have as a data subject, and how you can exercise these or obtain further information. We currently use the following platforms:

- **Facebook:** We run the page www.facebook.com/helsana. The data controller responsible for running the platform for users from Europe is Facebook Ireland Ltd., Dublin, Ireland. Its privacy policy can be viewed at www.facebook.com/policy. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: www.facebook.com/settings?tab=ads. We bear joint responsibility with Facebook Ireland Ltd., Dublin, Ireland in relation to the data collected and processed during visits to our page for generating Page Insights. Page Insights generates statistics as to what visitors do on our page (comment on posts, forward content, etc.). This is outlined at www.facebook.com/legal/terms/information_about_page_insights_data. It helps us to understand how our page is used and how we can improve it. We obtain only anonymous, aggregated data. Our responsibilities relating to privacy are in line with the information at www.facebook.com/legal/terms/page_controller_addendum.
- **Instagram:** We run the page www.instagram.com/helsana. The data controller responsible for running the platform for users from Europe is Facebook Ireland Ltd., Dublin, Ireland. Its privacy policy can be viewed at www.facebook.com/policy; the privacy policy for Instagram can be viewed at <https://help.instagram.com/519522125107875>. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: www.facebook.com/settings?tab=ads.
- **LinkedIn:** We run the page <https://www.linkedin.com/company/helsana-versicherungen-ag>. The data controller responsible for running the platform for users from Europe is LinkedIn Ireland Unlimited Company, Dublin, Ireland. Its privacy policy can be viewed at <https://de.linkedin.com/legal/privacy-policy>. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: <https://www.linkedin.com/psettings/advertising-data>.
- **Twitter:** We run the page www.twitter.com/helsana. The data controller responsible for running the platform for users from Europe is Twitter International Company, Dublin, Ireland. Its privacy policy can be viewed at www.twitter.com/de/privacy. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: www.twitter.ethicspointvp.com/custom/twitter/forms/data/form_data.asp.
- **Xing:** We run the page www.xing.com/pages/helsana. The data controller responsible for running the platform for users from Europe is New Work SE, Hamburg, Germany. Its privacy policy can be viewed at privacy.xing.com/de/datenschutzerklaerung. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: <https://www.xing.com/support/contact>.
- **YouTube:** On YouTube, we run the page <https://www.youtube.com/channel/helsana>. Google LLC is the operator of the service «YouTube». The data controller responsible for running the platform for users from Europe is Google Ltd., Dublin, Ireland. Its privacy policy can be viewed at <https://policies.google.com/privacy?hl=de#infocollect>. Using this will result in some of your data being transmitted to the USA. You can object to marketing here: <https://adssettings.google.com/authenticated?hl=de>.

15. Is this Privacy Policy subject to change?

This privacy policy does not form part of any contract with you. We can amend this privacy policy at any time. The version published on this website is the up-to-date version.

Last update: **September 2023**