

June 2026 edition

Terms of use for myHelsana

Contents

- 1 Area of application
- 2 Access authorisation
- 3 Means of access
- 4 Registration and authentication
- 5 Costs
- 6 User duty of care
- 7 Correspondence
- 8 Customers on the same insurance contract
- 9 Note on security
- 10 Liability
- 11 Marketing and information
- 12 Disabling access
- 13 Analysing User activity
- 14 Functions on myHelsana
- 15 Functions
 - 15.1 Digital insurance card
 - 15.2 Self-managed data area/data sharing
- 16 Amendments to the terms of use and changes to myHelsana
- 17 Termination of the user agreement
- 18 Applicable law and place of jurisdiction
- 19 Supplementary provisions

1 Area of application

The Helsana Group offers its insured persons and guest users (referred to collectively as “Users” in the following) various services on its myHelsana client portal and app. These terms of use set out the contractual agreements that exist between the User and Helsana when using myHelsana. By registering with myHelsana, the User recognises these terms of use.

2 Access authorisation

myHelsana is generally available to all persons insured with the Helsana Group (private customers) who are aged 18 years or over. Helsana also offers a restricted-function version of myHelsana that is available to all persons of full age, whether they are insured with Helsana or not. Helsana is at liberty, however, to decide whether or not to enter into an agreement with a User. Customers do not have any legal entitlement to access myHelsana.

3 Means of access

Users access the portal via their provider’s internet service.

To use myHelsana, the latest version of a commercially available web browser must be installed for the client portal, and Android/iOS for the app. Otherwise, myHelsana may not function properly or at all. Helsana is unable to provide support for technical problems of any kind, such as concerning the User’s end device or internet connection.

4 Registration and authentication

a) Registration for all functions

Once registered, customers will receive an activation code by post. This code is used to activate myHelsana in the first instance.

Customers who have already received the code by letter, e-mail or telephone can enter it during registration by following the instructions.

Users must then first sign in with their username, password and mTAN (security code sent by SMS) to access their data. They can then carry out the passkey registration in the mobile app in order to be able to log in with Face ID or Touch ID. If they do not carry out the passkey registration, they can continue to log in with their username, password and mTAN. If the User uses the myHelsana mobile app and has activated the “Log in with fingerprint” button for Android or the “Allow automatic passkey update” or similar button in the iOS Passwords app settings (the exact wording may differ depending on the app version), and if the device being used supports passkey and the User has recently logged in, a passkey can be automatically generated and stored by myHelsana in the background by opening the password manager API. If the User does not wish to keep the passkey, they can delete it.

Helsana deems anyone having identified themselves legitimately on the portal using their login data, as described above, as being authorised to access myHelsana and to use any of the services provided therein. In particular, the User is also entitled to amend data, submit applications, review documents uploaded to the portal and use the scanning feature to generate invoices and documents and send these to Helsana.

If there are justifiable doubts as to the identity of a registered User, Helsana may reject change requests, access to documents or any requests that have a legal impact on the User, or may check the identity of the User again. If it becomes apparent that the identity of the individual submitting the request does not correspond to that of the User, Helsana may decline to process the request without the corresponding power of attorney.

b) Registration for restricted use

To register for restricted use of myHelsana, all the User needs is an e-mail address and a password of their own choosing. Helsana policyholders have the option of switching from an account with restricted use to the full version with all functions at any time.

5 Costs

myHelsana is a free service.

6 User duty of care

It is the responsibility of each User to keep login data confidential and protect it from misuse by third parties. Users are liable for any consequences arising from the unauthorised use of their authentication details.

If a User has reason to suspect that an unauthorised third party has obtained such details, the password must be changed immediately and, if necessary, a request to disable the myHelsana account submitted to Helsana.

Users are obliged to check their myHelsana inbox regularly. It is their responsibility to ensure that invoices received via myHelsana are paid in good time using an appropriate online payment system or by CH-DD basic direct debit to a postal account or LSV+ direct debit to a bank account.

Amendments to home and/or e-mail addresses, bank details and other personal data must be entered in myHelsana by the User without delay. Correspondence from Helsana sent to the home or e-mail address stored on the system will be deemed duly served.

Once a customer has downloaded a document from myHelsana onto their own end device, they are then responsible for securing the data. Helsana cannot accept any responsibility for documents once they have left its systems.

By using the scanning feature, the User agrees to refrain from violating moral standards with their usage behaviour (e.g. photo uploads), infringing intellectual property rights or other proprietary rights, transmitting content with viruses (such as "Trojan horses" or other programs that could harm the software) or manipulating the functions or content of the scan function or entered details.

Helsana reserves the right to assert indemnity claims for all losses or damage it incurs, and to initiate criminal proceedings against insured persons if necessary.

If these terms of use are violated, or if the product is misused, Helsana is entitled to block the account of the relevant insured person at any time and without giving reasons. Helsana shall decide what constitutes misuse at its sole discretion.

If the User grants an AI agent access to their login data or, whether intentionally or unintentionally, authorises the agent to carry out actions of any kind on their behalf within myHelsana, all actions resulting therefrom shall be deemed to have been initiated by the User themselves. The User shall be solely responsible for checking, monitoring and, if necessary, restricting the scope of authorisations and the activities of any AI agent deployed by them.

7 Correspondence

By agreeing to these terms of use, i.e. by activating their myHelsana account with full functions, customers authorise Helsana to dispatch all further correspondence, including invoices and policies, electronically. The above does not, however, apply to documents that, for legal or technical reasons, require dispatch via the ordinary postal system. Customers can also ask to receive benefit statements, premium invoices, policies and tax statements by post via myHelsana.

8 Customers on the same insurance contract

Any person of full age can register for myHelsana.

If the family contact person (who may be stated in the insurance application or specified at a later date) registers for the full version of myHelsana, by entering into this user agreement, they agree to receive all correspondence from Helsana for all persons on the joint insurance contract electronically in future, i.e. including invoices and policies. The above does not, however, apply to documents that, for legal or technical reasons, require dispatch via the ordinary postal system. The family contact person has access to the data of insured persons associated with them under this insurance contract, including highly sensitive personal data.

Regardless of whether the family contact person is registered, any person of full age may register for their own access to the full-function version of myHelsana as a member of the joint insurance contract. This has no effect on the means of communication agreed between Helsana and the family contact person. This will allow the customer to access and edit their own data. The customer also has access to data they already know for all insured persons under the same insurance contract (including name, address, telephone number, insurance products, insurance card), regardless of whether or not these persons are registered for myHelsana. This does not apply to highly sensitive personal data.

Revocation is possible at any time and may be effected by writing to Customer Service. Revocation will result in contract separation into an individual contract.

9 Note on security

myHelsana is accessed via the internet.

Even if the User's end device employs state-of-the-art scientific and technical security precautions, a 100% guarantee of security cannot be given. Helsana therefore draws Users' attention to the following primary risks when using the myHelsana portal:

Inadequate security precautions on the User's end device can make it easier for a third party to gain unauthorised access to customer data. It cannot be ruled out that a third party will gain access to an end device surreptitiously while the customer is actually using myHelsana. For this reason, the Helsana Group urgently advises Users to equip their systems with a current firewall solution and to protect Wi-Fi networks with passwords. Helsana urges its customers not to access myHelsana via public Wi-Fi networks.

Information and data are exchanged between Helsana and its Users via an open network that is accessible by anyone. Although data transfers between Helsana and the User are encrypted, certain details of the connection (sender and recipient addresses) are not, and this may give rise to the inference that a business relationship exists between the User and Helsana.

Helsana has no influence over whether or how a User's internet provider will analyse data traffic. It is therefore possible for a third party to ascertain when and with whom the customer has been in contact.

For security reasons, a session time-out is installed that will automatically log the User out of myHelsana after a certain period of inactivity, whereupon they will need to sign in again to use the facility.

10 Liability

Considerable care and attention are invested in the content of the myHelsana portal. Helsana cannot, however, accept any liability for the accuracy or completeness of the data and information it provides and exchanges. Helsana offers no warranty that access to the myHelsana portal will be error-free, that defects will be corrected, or that viruses or other harmful components will not be transmitted in connection with the use of the site. Helsana accepts no liability to the extent permitted by law. In particular, Helsana accepts no liability for direct or indirect loss or damage and consequential loss or damage, such as loss of profits, loss or damage as a result of data from downloads or reputational damage.

Helsana accepts no liability whatsoever for damage, data loss, malfunctions, unwanted changes, security incidents or other adverse consequences arising from the disclosure of data, in particular login details, to AI agents or from their use within the application.

11 Marketing and information

Helsana may use myHelsana to advertise its own products or those of partners and place links to partner websites.

12 Disabling access

Helsana reserves the right to temporarily disable access to myHelsana in the interest of the User and to protect customer data if any security risk whatsoever is detected.

13 Analysing User activity

Helsana collects, processes and analyses tracking data in conjunction with the use of myHelsana for optimisation and statistical purposes. This tracking data cannot be traced to any individual User; it merely provides information on general user behaviour. In other words, these are anonymous evaluations to improve myHelsana. This data helps Helsana to optimise its website and make it more customer-friendly. Cookies (small text files containing an ID number) allow Helsana to enhance the service it provides to its customers and recognise returning website visitors.

Where Helsana falls within the scope of GDPR, it relies on its legitimate interests to operate and successfully improve myHelsana.

Most browsers have a function that allows Users to prevent cookies from being accepted automatically and to delete cookies already stored on the system. If the User does not want cookies to be stored on their device, they can change the browser settings so that cookies must either be approved before being stored or automatically refused. For ease of navigation, Helsana recommends that Users accept cookies and do not delete them. Disabling cookies can hinder the use of interactive functions on this and other websites.

A cookie banner informs Users about tracking in myHelsana when they use myHelsana via the web application. In the mobile applications (iOS and Android), tracking is based on consent; this consent is given for each device and app installation. No personalised tracking or profiling is carried out in myHelsana. Once consent has been given, events are triggered and displayed in Adobe Analytics as an anonymous user flow. This is done in order to obtain information on process interruptions by Users, i.e. which pages and bounce rates need to be improved. Adobe Analytics is a product offered by Adobe Systems Software Ireland Limited, 6 Riverwalk, Naas Road, Dublin 24, Ireland, www.adobe.com.

Users can object to tracking in the myHelsana web application at any time by rejecting the cookies.

Tracking in the mobile applications (iOS and Android) can also be objected to at any time in the operating system (iOS) or app (Android) settings.

14 Functions on myHelsana

Which functions are available on myHelsana depends on the User role and the insurance contracts concluded with Helsana. This can mean that not all functions will be available in some cases. In addition, Helsana reserves the right to modify, extend or discontinue the functions on myHelsana at any time.

15 Functions

15.1 Digital insurance card

myHelsana Users who have registered for all features can access their digital insurance card using the “Display insurance card” feature. This feature is available in the app regardless of whether or not Users are logged in and is activated by default. The identity check and, as a result, saving the card in offline mode is ensured via the device and not by Helsana. Users can deactivate the feature to display the card when they are not logged in at any time in the app settings. Deactivation deletes the version of the insurance card that is saved locally on the User’s device. You can also add your insurance card to your digital Apple or Google Wallet. The terms of use of the relevant third-party provider apply to the wallet.

15.2 Self-managed data area/data sharing

myHelsana customers who are registered for all features have the option of sharing certain pieces of myHelsana data with third parties in order to use their services.

a) One-off sharing of data with other people – via SMS, e-mail, social media and other apps

Data displayed in myHelsana can be shared if myHelsana makes this feature visibly available. This applies to PDF documents that are made available to you in myHelsana or generated using lists.

Example: medication data is accessed by the customer in the app and displayed as a list. Clicking the share symbol creates a PDF file, showing the displayed list. The customer can share this via e-mail, WhatsApp, or similar programs, using the iOS or Android tools.

b) Voluntary creation of the self-managed data area for the purpose of sharing data with a partner service

Some third parties offer appealing digital services. Connecting to these offers significant added value for myHelsana customers. These services rely on customers voluntarily providing them with some of their personal data.

myHelsana provides customers with the self-managed data area for the use of these third-party digital services. Customers can request their own data – in terms of a request for information – in this data area, and independently decide with which third parties the data should be shared until they object to such sharing. Helsana cannot see the data in the self-managed data area. Helsana merely provides the interface to the third-party services. Customers must activate the sharing of data with the service partner in order to use the services in question. If our policyholders do not activate the sharing of data, no data will be shared with the partner services.

Once myHelsana customers have set up their self-managed data area, they can also put a stop to the transmission of data at any time in the myHelsana settings.

If they need support, explicit permission is requested for Helsana employees, to allow them to temporarily access the data in the self-managed area exclusively for the purpose of resolving a technical issue.

16 Amendments to the terms of use and changes to myHelsana

Helsana is entitled to amend these terms of use at any time. Advance notice of any such changes will be communicated in an appropriate manner. The latest version always applies. The User must agree to this version to continue using myHelsana.

17 Termination of the user agreement

Either party has the right to withdraw from the user agreement at any time without citing reasons and without observing a notice period. Cancelling the user agreement will result in access to myHelsana being disabled immediately.

In any case, the user agreement for the full version of myHelsana is terminated automatically twelve months after the end of the contractual relationship with Helsana. In the interim, customers will receive all documents by post.

18 Applicable law and place of jurisdiction

These provisions or the contractual relationship between Helsana and the Users of myHelsana are subject to Swiss law. The place of jurisdiction is the registered office of Helsana Insurance Company Ltd.

19 Supplementary provisions

In addition to these terms of use, the use of myHelsana is subject to the Privacy Policy and the legal information on the Helsana website.

myHelsana data protection

Contents

- 1 What this Privacy Policy is about
- 2 Responsibility of myHelsana
- 3 Where do we get your data from?
- 4 For what purpose is personal data processed?
- 5 Who do we share your data with?
- 6 Is your personal data sent abroad?
- 7 Rights of data subjects
- 8 Technical and organisational measures to protect user data
- 9 Deletion of data
- 10 Changes to the myHelsana Privacy Policy

1 What this Privacy Policy is about

In the Privacy Policy at helsana.ch/data-protection, Helsana Insurance Company Ltd and Helsana Supplementary Insurances Ltd (hereinafter referred to as “Helsana”, “we” or “us”) provide information on how personal data is obtained and processed in the context of myHelsana. This abridged version of the Privacy Policy should be read alongside the full version.

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 in conjunction with 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. “Processing” refers to any operation involving personal data, e.g. obtaining, saving, using, altering, disclosing and deleting.

2 Responsibility of myHelsana

Both Helsana Insurance Company Ltd and Helsana Supplementary Insurances Ltd are responsible for data processing in connection with the use of myHelsana.

- Helsana Insurance Company Ltd, Dübendorf (“HVAG”), is responsible for all data processing related to social health insurance under the Federal Health Insurance Act (“KVG”)
- Helsana Supplementary Insurances Ltd, Dübendorf (“HZAG”), is responsible for all data processing related to supplementary insurance under the Federal Insurance Contract Act (“VVG”)

You can contact our Data Protection Advisor (Art. 10(1) and (4) DSG in conjunction with Art. 23 and Art. 25 DSG) about your data protection concerns and to exercise your rights under section 7 of this Privacy Policy:

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 Where do we get your data from?

In general, you provide us with the data processed in myHelsana yourself (e.g. via forms, when communicating with us, in connection with contracts, 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.

The data and documents displayed on myHelsana are drawn from the relevant Helsana departments and systems, and remain visible to the User for the duration of their online session. 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.

4 For what purpose is personal data processed?

The aforementioned data is used by Helsana primarily for the purpose of providing insurance services (processing benefit statements, communicating and offsetting insurance premiums, updating master data, etc.), contract changes (modifying deductibles, handling changes of address, etc.) and communication with our policyholders (answering queries and concerns when contact is made by either policyholders or Helsana, maintaining customer or contractual relationships).

In addition, the data collected and processed is used anonymously to improve myHelsana, for security purposes and for access control. This is done, for example, by analysing which features are used and how often and how Users navigate through myHelsana, via system and error checks, and as part of creating back-ups.

If you use the myHelsana client portal, the website may temporarily store your data to ensure it is not lost during the session, e.g. if you reload the website. No cookies are used for this process. When the browser is closed, the temporarily stored content is deleted.

5 Who do we share your data with?

As a matter of principle, all our employees are subject to a professional duty of confidentiality in accordance with Art. 62 DSG. If employees work for HVAG as part of the administration of social health insurance, they are also subject to the duty of confidentiality in accordance with Art. 33 of the Federal Act on the General Part of Social Insurance Law ("ATSG").

There are, however, exceptions provided for by law to the statutory duty of confidentiality: for example, HVAG may disclose data to third parties in the course of administering social health insurance (Art. 32 ATSG in conjunction with 84a KVG). 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 4, 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 recruiters, 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): this refers to corporate customers 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 4. 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 6 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 your request.

Behavioural data is passed on in pseudonymised form to Adobe Analytics for the purpose of analysing and improving the user experience in myHelsana.

For the independent disclosure of data via the self-administered data area, please refer to the terms of use (part A), section 15.2.

6 Is your personal data sent abroad?

As explained in section 5, we share your data with other agencies. These are also located outside of Switzerland. Your data may therefore be processed in Europe (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 data protection regulations on the recipient (for this purpose, we use the new standard contractual clauses of the European Commission, including the modifications requested by the Federal Data Protection and Information Commissioner [FDPIC] for Switzerland), 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.

7 Rights of data subjects

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

If you would like to exercise any of the above-listed rights against us, please contact 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).

8 Technical and organisational measures to protect user 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.

9 Deletion of 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).

10 Changes to the myHelsana Privacy Policy

As a general rule, the use of myHelsana is governed by the full Privacy Policy of Helsana, which can be viewed at helsana.ch/data-protection. The full Privacy Policy and this abridged version may be amended at any time. The published version is the applicable version.

Last updated: June 2026