Privacy policy for the use of the Hallesche4u mobile app

Hallesche Krankenversicherung a. G.
70166 Stuttgart

Privacy policy

Data security and data protection are top priorities at Hallesche4u. We are therefore providing some comprehensive information about the processing of your personal data. Your data remains your property. Our systems are subject to regular security audits and we are constantly upgrading them. Our Hallesche4u app is a mobile app for Android and iOS that you can download and install on your mobile device. This privacy policy describes which personal data is processed by us when you use the Hallesche4u app and what rights you have with respect to such data.

1. Definitions

The legislator requires that personal data is processed lawfully, fairly and in a manner that is comprehensible to the data subject ("lawfulness, fairness and transparency"). To ensure this, we will inform you about the individual legal terms of the European Data Protection Regulation (GDPR) and the new Federal Data Protection Act (BDSG-neu), which are also implemented in these privacy policy stipulations:

1.1 Personal data

"Personal data" denotes any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.2. Processing

"Processing" denotes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.3. Restriction of processing

"Restriction of processing" denotes the marking of stored personal data with the aim of limiting their processing in the future;

1.4. Profiling

"Profiling" denotes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

1.5. Pseudonymisation

"Pseudonymisation" denotes the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational

measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

1.6. Filing system

"Filing system" denotes any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

1.7. Controller

"Controller" denotes the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

1.8. Processor

"Processor" denotes a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

1.9. Recipient

"Recipient" denotes a natural or legal person, public authority, agency or another body, to which the personal data is disclosed, regardless of whether they are a third party. However, public authorities which may receive personal data within the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of the data by such public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

1.10. Third party

"Third party' denotes a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

1.11. Consent

"Consent" of the data subject denotes any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

2. Who is responsible for the Hallesche4u app?

The entity responsible for data protection issues:

Hallesche Krankenversicherung a.G.
Reinsburgstr. 10
70178 Stuttgart Germany

Telephone: +49 711 - 6603 – 0
Fax: +49 711 - 6603 - 333
Email: service@hallesche.de

3. To whom can I address questions regarding data protection?

If you have any questions about data protection, please contact our data protection officer.

You can reach the DPO by post at the address of the data controller indicated above with the header "data protection officer" or by email: datenschutz@hallesche.de.

4. General information on data processing

The data you submit is hosted on ALH Gruppe servers. The data centre used for this purpose is located in Germany.

There is no legal obligation to submit personal data to us. However, by their very nature, we cannot offer you the majority of the functions of the Hallesche4u app without processing personal data.

In addition, we do not use automated decision-making within the meaning of Art. 22 GDPR, in particular profiling.

5. What data is processed, for what purposes and on what legal basis?

In this section we inform you about what data we collect from you and then process, for what purposes we require the data and the legal basis for such processing.

5.1 Data collection by the app stores

When downloading the mobile app, the information required is transferred to the respective app store, in particular username, email address and customer number of your account, time of download, payment information and the individual device identification number. We have no influence on this data collection and are not responsible for the collection. We only process the data insofar as it is necessary to download the mobile app to your mobile device.

5.2 Log files

When you use the mobile app, we collect data on the servers of the ALH Gruppe in log files, which are technically necessary to enable us to offer you the functions of our mobile app and to ensure the stability and security of the app.
The data collected in this way, including the time stamp or function used, does not allow any conclusions to be drawn about your person. This data is not merged with other data sources.
Please note that server log files may contain the IP address you are using to surf the Internet. Server log files are stored for three months and then automatically deleted. The legal basis for the processing of the IP address is Art. 6 para 1 sentence 1 lit. f) GDPR. We have a legitimate interest in ensuring the functionality, stability and security of our app when we store log files.

5.3 ALH Gruppe insurance data

The Hallesche4u app serves as a customer portal for people insured with us. You can, among others, manage the insurance policies you hold with us via the Hallesche4u app. When you enter your contact details and contract number in the Hallesche4u app, information about your contract(s) is automatically displayed in the app. The data processed is, in particular: Your contact details, policy number(s), type of insurance(s), amount of premium and payment interval of the insurance(s), the term of the insurance(s)

and the insurance premiums. ALH Group is entitled to process this data for the purpose of implementing the insurance contract concluded with you in accordance with *Art. 6 para 1 sentence 1 lit. b) GDPR*.

5.4 Additional data you provide to us

Once you have installed our app, we will request your express consent to process and, in particular, store all the information you provide to us via the app. It is your sole decision to submit this data to us. We are then entitled to process your personal data based on your consent pursuant to *Art. 6 para 1 sentence 1 lit. a) GDPR*. Your data will, of course, be processed strictly for the intended purpose. The following describes what personal data we use which you have submitted, and for what purposes.

5.4.1 Registration details

When you register for the Hallesche4u service, we will ask you for your name, date of birth, email address, telephone number and contract number. We require this data to assign you to existing insurance contracts and to provide you with the Hallesche4u customer account.

5.4.2 Identification

A comparison of your data is required as part of the registration process for security reasons and for more precise identification. You can choose whether you would like to receive the activation data to use the Hallesche4u app by post to the address stored in the system or directly online. If you choose the latter option, we will first ask you to identify yourself to us using a Video-Ident procedure.

We use the "NECT IDENT" service of Nect GmbH, Großer Burstah 21, 20457 Hamburg ("NECT") for this purpose. NECT will ask you for your consent to the collection and forwarding of your personal data before carrying out the identification procedure. This generally includes a video or photo recording of you or your face, along with the data on your identity card. The legal basis for the processing of this data is therefore your consent pursuant to *Art. 6 para 1 sentence 1 lit. a) GDPR*. The respective rights can be asserted with NECT.

NECT only receives a pseudonymous ID number from us, which enables us to assign the data transmitted to us by NECT to your person.

5.4.3 Biometric data (TouchID/FaceID)

You can unlock the Hallesche4u app using the device authentication (e.g. fingerprint or facial recognition) of your end device to secure your Hallesche4u account against unauthorised access. No biometric data collected in this process or characteristics derived therefrom will be transferred to Hallesche4u. The app only uses the service provided by your device for verification. We only receive information via the operating system of your mobile end device to confirm if the scanned data corresponds to the data registered in the operating system and, if successful, we then log in automatically using the stored login data.

You can disable this function in the app settings at any time.

5.4.4 Invoices

The Hallesche4u app will continue to offer you the option of transmitting reimbursable bills to us quickly and easily via your smartphone. The invoices you submit via the app are stored by us in encrypted form for secure protection. We will use the invoices for verification and reimbursement purposes only and will not disclose it to third parties. The legal basis for this is *Art. 6 para 1 lit. a)* and *lit. b) GDPR*.
Invoices may in some cases contain special categories of personal data within the meaning of *Art. 9 para 1 GDPR*. If this is the case, the legal basis of the processing is your consent in accordance with *Art. 9 para 2 lit.a) GDPR*.

5.4.5 Other requests

If you get in touch via our contact form, email or telephone, your enquiry or request and all the personal data arising from such contact, will be stored and processed by us to process your request. We do not disclose this data to third parties without your consent. This data is processed on the basis *of Art. 6 para 1 sentence 1 lit. b) GDPR*, insofar as your request relates to the performance of a contract concluded with us or is required to execute pre-contractual measures. Furthermore, the processing is based on *Art. 6 para 1 sentence 1 lit. f) GDPR*, as we have a legitimate interest in the effective processing of the requests addressed to us. In addition, we are also entitled to process the aforementioned data pursuant to *Art. 6 para 1 sentence 1 lit. c) GDPR*, as we are legally obliged to enable fast electronic contact and direct communication to or with us.
Please be reassured that your data will be used strictly for the purpose of processing and responding to your enquiry and will be deleted again after processing has been completed, provided we are under no legal obligation to retain the data.

When contacting us, you can also voluntarily share your local log file with us. This will help us to process your request more efficiently. Your local log file contains information about requests to our backend systems but no personal data. You are under no obligation to share your local log file with us.

6. How long will my data be stored?

We store the personal data that is required to execute contracts concluded with you for the duration of the contractual relationship. In addition, we only store this data if the relevant statutory retention obligations require us to do so.

We will delete any other data you provide to us voluntarily when you delete your Hallesche4u user account or withdraw your consent to processing.

7. Is any personal data disclosed to third parties?

As a matter of principle, we do not disclose your data to third parties outside ALH Gruppe without your express consent.
However, similar to any modern business, we work with external processors to provide you with an uninterrupted and optimum service. In the following, we inform you regarding when and how we disclose your personal data to our external partner service providers.

When we work with external service providers, we regularly commission order data processing on the basis of *Art. 28 GDPR*. For this purpose, we conclude the corresponding agreements with our partners to ensure the protection of your data. We only commission carefully selected processors to process your data. They are bound by our instructions and are regularly inspected by us. We only commission external service providers who can guarantee that all data processing operations are carried out in accordance with data protection legislation.

We work with the following service providers:

7.1 Use of DOCYET (symptom checker)

A symptom checker is provided within the app via a separate interface. The entity responsible for this in accordance with data protection law is:

DOCYET GmbH
Floßplatz 6
04107 Leipzig

When you use the symptom checker, a direct connection is established to the operator's servers. No data will be transferred to us. In particular, health data is transferred in accordance with *Art. 9 para 1 GDPR*. If you provide the data to DOCYET, this is expressly based on your consent pursuant to *Art. 9 para 2 lit. a) GDPR*. For more information on privacy, please visit https://www.docyet.com/product/datenschutz/.

7.2 Firebase Crashlytics

We use anonymised crash reports to improve the stability and reliability of our apps. We use "Firebase Crashlytics", a service provided by Google Ireland Ltd, Google Building Gordon House, Barrow Street, Dublin 4, Ireland.

In the event of a crash, anonymous information is transmitted to Google's servers in the USA (state of the app at the time of the crash, installation UUID, crash trace, manufacturer and operating system of the mobile phone, last log messages). This information does not contain personal data.

Crash reports will only be sent with your express consent. When using iOS apps, you can grant consent in the app settings or after a crash. For Android apps, when configuring the mobile device, you have the option to generally agree to the transmission of crash notifications to Google and app developers.

The legal basis for the transfer of data is *Art. 6 para 1 lit. a GDPR*.

You can revoke your consent at any time by disabling the "Crash reports" function in the iOS apps settings (in the magazine apps, the entry is in the menu item "Communication").

For Android apps, the disabling of the app is essentially carried out in the Android settings. To do this, open the app settings, select the item "Google", and in the three-point menu at the top right, select the menu item "Use and diagnosis". Here you can disable the sending of the corresponding data. For more information, please consult the Help section in your Google account.

For more information on data protection, please visit the Firebase Crashlytics privacy policy: https://firebase.google.com/support/privacy and https://docs.fabric.io/apple/fabric/data-privacy.html#data-collection-policies.

8. What rights exist with respect to personal data?

This section explains the rights you have regarding your personal data.

8.1 Revocation of consent

If the processing of personal data is based on consent which has been granted, you have the right to revoke your consent at any time. The revocation of the consent shall not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.
You can contact us at any time to exercise your right of revocation.

8.2 Right to confirmation

You have the right to request confirmation from the controller as to whether we are processing your personal data. You can request confirmation using the contact details above at any time.

8.3 Right to information

If personal data is processed, you can request information about such personal data and about the following information at any time:

- the purposes of processing;
- the categories of personal data that is processed;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular in the case of recipients in third countries or international organisations;
- if possible, the anticipated duration for which the personal data will be stored or, if this is not possible, the criteria for determining such period of storage;
- the existence of a right to rectification or erasure of your personal data or to a restriction of processing by the controller or a right to object to such processing;
- the existence of a right of appeal to a supervisory authority;
- if the personal data is not collected from the data subject, any available information on the origin of the data;
- the existence of automated decision-making, including profiling, pursuant to *Art. 22 para 1 and 4 GDPR* and, at least in such cases, useful information about the logic involved and the scope and intended effects of such processing for the data subject.

If personal data is transferred to a third country or to an international organisation, you have the right to be informed about the appropriate safeguards in accordance with *Art. 46 GDPR* in connection with the transfer. We will provide a copy of the personal data that is the subject of processing. We may charge a reasonable fee based on administrative costs for any additional copies requested by you. If you make the application electronically, the information will be provided in a commonly used electronic format, unless indicated otherwise. The right to receive a copy under *para 3* shall not prejudice the rights and freedoms of other persons.

8.4 Right to rectification

You have the right to request us to rectify any inaccurate personal data relating to you without delay. Taking into account the purposes of the processing, you may request the completion of incomplete personal data, including via a supplementary declaration.

8.5 Right to erasure (“right to be forgotten”)

You have the right to request the controller to delete your personal data immediately and we are obliged to delete personal data without delay if one of the following reasons applies:

- The personal data is no longer required for the purposes for which it was collected or otherwise processed.

- The data subject revokes the consent on which the processing was based pursuant to *Art. 6 para 1 sentence 1 lit. a) or Art. 9 para 2 lit. a) GDPR*, and there is no other legal basis for the processing.
- The data subject objects to the processing in accordance with *Art. 21 para 1 GDPR* and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to *Art. 21 para 2 GDPR*.
- The personal data has been processed unlawfully.
- The deletion of the personal data is necessary to comply with a legal obligation under Union or Member State law to which the controller is subject.
- The personal data was collected in relation to information society services provided in accordance with *Art. 8 para 1 GDPR*.

Where the controller has made the personal data public and is under an obligation to delete it pursuant to paragraph 1, the controller shall take reasonable steps, including technical measures, in view of the available technology and the cost of implementation, to inform data controllers who are processing the personal data that a data subject has requested that the controllers erase all links to, or copies or duplications of, such personal data.
The right to erasure ("right to be forgotten") shall not apply insofar as the processing is necessary:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation which requires processing by Union or Member State law to which the controller is subject or to perform a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with *Art. 9 para 2 lit. h) and i)* and *Art. 9 para 3 GDPR*;
- or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to *Art. 89 para 1 GDPR*, insofar as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of such processing; or
- to establish, exercise or defend legal claims.

8.6 Right to restriction of processing

You have the right to request us to restrict the processing of your personal data in one of the following conditions:

- the accuracy of the personal data is contested by the data subject, for a period that would enable the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of the use of the personal data instead;
- the controller no longer requires the personal data for the purposes of the processing, but the data is required by the data subject to establish, exercise or defend legal claims;
- the data subject has objected to processing pursuant to *Art. 21 para 1 GDPR* pending verification of whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted in accordance with the above conditions, such personal data shall be processed, besides being stored, only with the consent of the data subject or to establish, exercise or defend legal claims or to protect the rights of another natural or legal person or for reasons of substantial public interest of the Union or of a Member State.
The data subject may contact us at any time using the contact details provided above to exercise the right to the restriction of processing.

8.7 Right to data portability

You have the right to receive the personal data relating to you that you have provided to us in a structured, commonly used and machine-readable format. You also have the right to disclose the data to

another controller without hindrance from the controller to whom the personal data was provided, where:

- the processing is based on consent pursuant to *Art. 6 para 1 sentence 1 lit. a)* or *Art. 9 para 2 lit. a)* or on a contract in accordance with *Art. 6 para 1 sentence 1 lit. b) GDPR*, and
- the processing is carried out by automated means.

In exercising your right to data portability pursuant to paragraph 1, you reserve the right to request the personal data to be transmitted directly from one controller to another, where technically feasible. The exercise of the right to data portability does not affect the right to erasure ("right to be forgotten"). This right shall not apply to processing that is required to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.

8.8 Right to object

You have the right to object, on grounds relating to your particular situation, to processing of your personal data at any time which is based on *Art. 6 para 1 lit. e)* or *f) GDPR*; this also applies to profiling based on these provisions. The controller shall cease processing personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or to establish, exercise or defend legal claims.

Where personal data is processed for direct marketing purposes, you shall have the right to object to the processing of your personal data for such marketing purposes at any time, which includes profiling to the extent that it is related to such direct marketing. If you object to processing for direct marketing purposes, the personal data will cease to be processed for such purposes.

In the context of the use of information society services, and notwithstanding *Directive 2002/58/EC*, you may exercise your right to object by automated means using technical specifications.

You have the right to object, on grounds relating to your particular situation, to the processing of your personal data which is carried out for scientific or historical research purposes or for statistical purposes pursuant to Article 89 para 1, unless such processing is necessary to perform a task carried out in the public interest.

You may exercise the right to object at any time by contacting the respective controller.

Please note that you will cease to be able to use our app if you object.

8.9 Automated individual decision-making, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on you or which may similarly affect you in a significant way. This shall not apply if the decision:

- is necessary to enter into or perform a contract between the data subject and the data controller;
- is authorised by Union or Member State law to which the controller is subject and which also specifies appropriate measures to safeguard the rights, freedoms and legitimate interests of the data subject; or
- takes place with the express consent of the data subject.

The controller shall take reasonable steps to safeguard the rights, freedoms and legitimate interests of the data subject, which include at least the right to obtain human intervention on the part of the controller, to express the data subject's point of view and to contest the decision.

The data subject may exercise this right at any time by contacting the respective data controller.

8.10 Right to complain to a supervisory authority

Without prejudice to any other administrative or judicial remedy, data subjects may lodge a complaint with a supervisory authority, in particular in the Member State of the data subject's residence, place of work or the place of the alleged infringement, if the data subject considers that the processing of their personal data infringes this regulation.

8.11 Right to an effective legal remedy

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Art. 77 GDPR, you are entitled to seek an effective legal remedy if you consider that your rights under this regulation have been infringed owing to the processing of your personal data that does not comply with this regulation.

9. Children and young persons

Our offer essentially targets adults. Children and young persons under the age of 16 are not permitted to transmit personal data to us without the consent of their legal guardians.

10. Amendments

We expressly reserve the right to amend this privacy policy due to the rapid development of the Internet and data protection legislation.

Date: March 8, 2022