Privacy Policy Mobile App

Table of Contents

1. Introduction

In the following, we provide information about the collection of personal data when using our mobile app (hereinafter only "App").

Personal data is any data that can be related to a specific natural person, such as their name or IP address.

1.1 Contact details

The controller within the meaning of Art. 4 (7) EU General Data Protection Regulation (GDPR) is FoodQuest GbR, Rheinsberger Straße 76/77, Berlin, Germany, email: support@foodquest.com. We are legally represented by Daniel Bischoff, Teresa Sommer.

Our data protection officer can be reached via heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu , E-Mail: datenschutz@heydata.eu.

1.2 Scope of data processing, processing purposes and legal bases

We detail the scope of data processing, processing purposes and legal bases below. In principle, the following come into consideration as the legal basis for data processing:

- Art. 6 para. 1 s. 1 it. a GDPR serves as our legal basis for processing operations for which we obtain consent.
- Art. 6 para. 1 s. 1 lit. b GDPR is the legal basis insofar as the processing of personal data is necessary for the performance of a contract, e.g. if a user purchases a product from us or we perform a service for him. This legal basis also applies to processing that is necessary for pre-contractual measures, such as in the case of inquiries about our products or services.
- Art. 6 para. 1 s. 1 lit. c GDPR applies if we fulfill a legal obligation by processing personal data, as may be the case, for example, in tax law.
- Art. 6 para. 1 s. 1 lit. f GDPR serves as the legal basis when we can rely on legitimate interests to process personal data, e.g. for cookies that are necessary for the technical operation of our website.

1.3 Data processing outside the EEA

Insofar as we transfer data to service providers or other third parties outside the EEA, the security of the data during the transfer is guaranteed by adequacy decisions of the EU Commission, insofar as they exist (e.g. for Great Britain, Canada and Israel) (Art. 45 para. 3 GDPR).

In the case of data transfer to service providers in the USA, the legal basis for the data transfer is an adequacy decision of the EU Commission if the service provider has also certified itself under the EU US Data Privacy Framework.

In other cases (e.g. if no adequacy decision exists), the legal basis for the data transfer are usually, i.e. unless we indicate otherwise, standard contractual clauses. These are a set of rules adopted by the EU Commission and are part of the contract with the respective third party. According to Art. 46 para. 2 lit. b GDPR, they ensure the security of the data transfer. Many of the providers have given contractual guarantees that go beyond the standard contractual clauses to protect the data. These include, for example, guarantees regarding the encryption of data or regarding an obligation on the part of the third party to notify data subjects if law enforcement agencies wish to access the respective data.

1.4 Storage duration

Unless expressly stated in this privacy policy, the data stored by us will be deleted as soon as they are no longer required for their intended purpose and no legal obligations to retain data conflict with the deletion. If the data are not deleted because they are required for other and legally permissible purposes, their processing is restricted, i.e. the data are blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons.

1.5 Rights of data subjects

Data subjects have the following rights against us with regard to their personal data:

- Right of access,
- Right to correction or deletion,
- Right to limit processing,
- Right to object to the processing,
- Right to data transferability,
- Right to revoke a given consent at any time.

Data subjects also have the right to complain to a data protection supervisory authority about the processing of their personal data. Contact details of the data

protection supervisory authorities are available at https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html.

1.6 Obligation to provide data

Within the scope of the business or other relationship, customers, prospective customers or third parties need to provide us with personal data that is necessary for the establishment, execution and termination of a business or other relationship or that we are legally obliged to collect. Without this data, we will generally have to refuse to conclude the contract or to provide a service or will no longer be able to perform an existing contract or other relationship.

Mandatory data are marked as such.

1.7 No automatic decision making in individual cases

As a matter of principle, we do not use a fully automated decision-making process in accordance with article 22 GDPR to establish and implement the business or other relationship. Should we use these procedures in individual cases, we will inform of this separately if this is required by law.

1.8 Making contact

When contacting us, e.g. by e-mail or telephone, the data provided to us (e.g. names and e-mail addresses) will be stored by us in order to answer questions. The legal basis for the processing is our legitimate interest (Art. 6 para. 1 s. 1 lit. f GDPR) to answer inquiries directed to us. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are legal retention obligations.

2. Data processing in the app

2.1 Downloading the app

Our app is ready for download at Apple's App Store, Google's Play Store (hereinafter "Stores"). When users download the app, the necessary information is transmitted to the stores, i.e. in particular user name, e-mail address and customer number of the 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 it. We process the data only insofar as it is necessary for downloading the mobile app to the user's mobile device.

2.2 Hosting

Our app is hosted by Backend: Cloudflare, Datenbank: Supabase, Bilder: Uploadcare. The provider thereby processes the personal data transmitted via the app, e.g. on content, usage, meta/communication data or contact data. It is our legitimate interest to provide an app, so that the legal basis of the data processing is Art. 6 para. 1 s. 1 lit. f GDPR.

The provider hosts the app on servers in Cloudflare verteilt seiner Server weltweit (Edge Hosting); bei Supabase steht die Datenbank in Deutschland; Uploadcare ist in den USA.

2.3 Informative use of our app

When users use our app, we collect the data that is technically necessary for us to offer users the functions of our app and to ensure stability and security. This is our legitimate interest, so that the legal basis is Art. 6 para. 1 s. 1 lit. f GDPR.

The data processed to this extent are:

- IP address
- Date and time of the request
- Time zone difference from Greenwich Mean Time (GMT)
- Content of the request (concrete interface)
- Access status/HTTP status code
- Amount of data transferred in each case
- Operating system and its interface
- Language and version of the operating system

2.4 Access to functions or data

The app requests the user's access to functions of the end device or to data of the device in order to be able to execute functions of the app. By allowing access, the user gives consent to the associated data processing, so that the legal basis is Art. 6 para. 1 s. 1 lit. a GDPR. Users can revoke their consent at any time by terminating access in the settings of their end device. The revocation does not affect the lawfulness of the processing until the revocation.

The data processed or access functions used in this respect are

- bestehende Fotoaufnahmen, Kamera, Standort

2.5 Data processing for the provision of functions

In the app, we process data in order to provide the user with functions of the app. The legal basis for the processing is the usage agreement concluded with the user via the app.

The data processed to this extent are:

- Data entered into the app by the user themselves
- Dietary preferences (e.g., intolerances, allergies)
- Compliance and symptoms related to dietary preferences (e.g., allergies or other diet-related conditions; posts and comments written by the user (mostly related to diet/health)

2.6 Proof of consent without a user account (Anonymous user account)

When users use the app without registering regularly, we create an anonymous user account in the background. In doing so, we store a unique user ID as well as the timestamp of creation and the last login. This serves exclusively the purpose of legally storing and being able to prove the data protection consents granted by the user in the app (in particular the explicit consent to the processing of health data and dietary preferences) as well as their version in our database. The legal basis for this storage is the fulfillment of our legal obligation to provide proof in accordance with Art. 6 para. 1 sentence 1 lit. c GDPR in conjunction with Art. 7 para. 1 GDPR. The anonymous user account and the associated consent data will be automatically deleted if the user has not used the app for a period of 24 months.

2.7 Single sign-on

Users can log in to our app using one or more single sign-on methods. In doing so, they use the login data already created for a provider. The prerequisite is that the user is already registered with the respective provider. When a user logs in using a single sign-on procedure, we receive information from the provider that the user is logged in to the provider and the provider receives information that the user is using the single sign-on procedure in our app. Depending on the user's settings in his account on the provider's site, additional information may be provided to us by

the provider. The legal basis for this processing is Art. 6 para. 1 sentence 1 lit. f GDPR. We have a legitimate interest in providing users with a simple log-in option. At the same time, the interests of the users are safeguarded, as use is only voluntary.

Providers of the offered method(s) are:

- Apple Inc., Infinite Loop, Cupertino, CA 95014, USA (Privacy policy: https://www.apple.com/legal/privacy/de-ww/).
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (Privacy policy: https://policies.google.com/privacy).

2.8 In-App Purchases and Subscriptions

We offer paid subscriptions and in-app purchases in our app. The payment processing is carried out entirely via the platforms of the respective app stores (Apple App Store for iOS or Google Play Store for Android). We do not collect or process sensitive payment data (such as credit card information) ourselves. To verify the purchase and unlock the corresponding premium features in the app for you, we only receive anonymized transaction confirmations (so-called tokens/receipts) from Apple or Google about the successful completion of the subscription. The legal basis for this processing is the fulfillment of the contract concluded with you for the use of the paid features in accordance with Art. 6 para. 1 sentence 1 lit. b GDPR. Further information on data processing by the app stores during in-app purchases can be found in the privacy policies of the respective providers:

- **Apple** (Apple Inc., Infinite Loop, Cupertino, CA 95014, USA): https://www.apple.com/legal/privacy/en-ww/
- **Google** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland): https://policies.google.com/privacy

2.9 Third-party tools

2.9.1 PostHog

We use PostHog for A/B testing, for product analytics. The provider is PostHog, Inc., San Francisco, 2261 Market St #4008, San Francisco, CA, USA. The provider processes contact data (e.g. e-mail addresses, telephone numbers), meta/communication data (e.g. device information, IP addresses), usage data (e.g. web pages visited, interest in content, access times) in the EU.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. f GDPR. We have a legitimate interest in further developing our product based on feedback from users.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://posthog.com/privacy.

2.9.2 Sentry

We use Sentry to track errors in applications or on websites, to monitor applications. The provider is Functional Software, Inc., 132 Hawthorne Street San Francisco, CA 94107, USA. The provider processes usage data (e.g. web pages visited, interest in content, access times), meta/communication data (e.g. device information, IP addresses), content data (e.g. entries in online forms) in the USA.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. f GDPR. We have a legitimate interest in adequately monitoring the functionality of our applications.

The legal basis for the transfer to a country outside the EEA are adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://sentry.io/privacy/.

2.9.3 Cloudflare

We use Cloudflare as a fundamental component of our backend infrastructure to provide our services securely and reliably. The provider is Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA. Cloudflare processes all data required for the transmission and operation of our platform (e.g., IP address, first name, username, email, dietary preferences, user posts, user images, search queries, and search filters). The legal basis is Art. 6 para. 1 sentence 1 lit. f GDPR. We have a legitimate interest in the stability, security, and functionality of our app.

The legal basis for the transfer to a country outside the EEA are adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://www.cloudflare.com/en-gb/privacypolicy/.

2.9.4 OpenAI API

We use the OpenAI API for the moderation, translation, and categorization of text content and images. The provider is OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland. The only personal data transmitted in this context is the content created by users (posts, comments, images). The legal basis for the processing is Art. 6 para. 1 sentence 1 lit. f GDPR.

The legal basis for the transfer to a country outside the EEA are standard contractual clauses. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed by standard data protection clauses (Art. 46 para. 2 lit. c GDPR) adopted by the EU Commission in accordance with the examination procedure under Art. 93 para. 2 of the GDPR, which we have agreed to with the provider.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://openai.com/policies/privacy-policy.

2.9.5 Supabase

Supabase enables fundamental functions of our application, including the storage, processing, and analysis of data in the database. The provider is Supabase, Inc., 970 Toa Payoh North #07-04, Singapore 318992, Singapore. Supabase may process personal data, such as first name, username, email address, IP addresses, uploaded images, messages sent within the application, as well as the set dietary preferences and other voluntary information. The legal basis is Art. 6 para. 1 sentence 1 lit. b GDPR.

The legal basis for the transfer to a country outside the EEA are standard contractual clauses. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed by standard data protection clauses (Art. 46 para. 2 lit. c GDPR) adopted by the EU Commission in accordance with the examination procedure under Art. 93 para. 2 of the GDPR, which we have agreed to with the provider.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://supabase.com/docs/company/privacy.

2.9.6 heyData

We have integrated a data protection seal on our website. The provider is heyData GmbH, Schützenstraße 5, 10117 Berlin, Germany. The provider processes meta/communication data (e.g. IP addresses) in the EU.

The legal basis of the processing is Art. 6 para. 1 s. 1 lit. f GDPR. We have a legitimate interest in providing website visitors with confirmation of our data privacy compliance. At the same time, the provider has a legitimate interest in ensuring that only customers with existing contracts use its seals, which is why a mere image copy of the certificate is not a viable alternative as confirmation.

As the data is masked after collection, there is no possibility to identify website visitors. Further information is available in the privacy policy of the provider at https://heydata.eu/en/privacy-policy .

3. Changes to this privacy policy

We reserve the right to change this privacy policy with effect for the future. A current version is always available here.

4. Questions and comments

If you have any questions or comments regarding this privacy policy, please feel free to contact us using the contact information provided above.