



Homebrewed - Privacy and Data Protection Policy on Google platforms

Published date: 16 September 2026

Effective date: 16 September 2026

Version: 1.2

This Privacy Policy explains how the Homebrewed Android application handles information. Homebrewed is a software product of baseworks.tech.

baseworks.tech is the controller of personal data processed for our own purposes as described in this Policy. Certain providers, including Google, Open Food Facts and payment providers, may act as separate controllers where they independently determine the purposes and means of particular processing. Their processing is governed by their own privacy notices.

The current version of this policy and other company policies will be available from the baseworks.tech policies page: <https://www.baseworks.tech/policies/>.

Table of contents:

Section 1: Identity and contact details of the data controller	2
Section 2: Scope	2
Section 3: Summary	2
Section 4: Information stored on your device	3
Section 5: Information Homebrewed does not collect	3
Section 6: Open Food Facts	4
Section 7: Camera and Google ML Kit barcode scanning	4
Section 8: Nearby devices, Bluetooth and legacy location permission	5
Section 9: Household sharing	6
Section 10: Google Play and Google services	6
Section 11: On-device diagnostics	6
Section 12: Backups, device transfer, imports and exports	7
Section 13: Retention and deletion	7
Section 14: Children	8
Section 15: Your data-protection rights	8
Section 16: Security	8



Section 17: Changes to this policy	9
Section 18: Governing language	9
Section 19: Contact	9

Section 1: Identity and contact details of the data controller

The data controller for Homebrewed (also referred to as the “company”) responsible for the processing of your personal data for its own purposes is:

baseworks.tech, registered in the Netherlands under Chamber of Commerce number (KvK nummer) 98170643, VAT number NL005312934B1, postal address Box E1586, Oder 20, 2491 DC Den Haag, Netherlands.

Questions, requests or complaints about this policy or our data practices may be sent to privacy@baseworks.tech.

Section 2: Scope

This policy applies only to the Homebrewed Android application with application ID app.homebrewed, including a build distributed through Google Play.

It does not govern the baseworks.tech website, online shop, other baseworks.tech software, the Homebrewed iOS application or any Docker/self-hosted version of Homebrewed. Those products and services have separate policies appropriate to how they operate.

Google Play, Google Play services, Android system services, a device manufacturer's services and Open Food Facts operate under their own privacy terms, as explained below.

Section 3: Summary

Homebrewed is designed to keep your personal food and household information on the Android device on which it is installed. There is no Homebrewed account, sign-in or baseworks.tech server for the Android application. baseworks.tech does not receive your meals, recipes, ingredients, products, profiles, goals or household content through the app.

Homebrewed contains no advertising, advertising SDK, general-purpose analytics, usage profiling or third-party crash-reporting service. It does not build an advertising or behavioural profile about you.

The app communicates with:



- Open Food Facts when it needs product information or an Open Food Facts product image;
- Google ML Kit components used for barcode recognition, which process camera input on the device but may send limited app, device and performance metrics to Google;
- Google Play Billing when the app requests localized product information, opens a purchase, acknowledges a completed purchase, or checks whether the permanent unlock is currently owned;
- Android, Google Play and device services involved in installation, updates, security scanning and any system backup or device transfer you enable; and
- devices you deliberately pair for direct household sharing.

Section 4: Information stored on your device

Homebrewed stores the following information in the application's private storage area on your device:

- daily meal entries and burned-calorie entries;
- recipes, ingredients, products entries;
- nutrition targets, macro-nutrient goals and meal proportions;
- local profiles, including a name and an optional avatar image, used to separate entries within a household;
- product information and image references obtained from Open Food Facts;
- app preferences, such as appearance settings;
- the timestamp at which the app-managed trial first started;
- a record containing whether a verified permanent unlock was last known to be owned and its purchase timestamp;
- display information for the permanent unlock, such as product identifier, display name, description and localized price.
- user-initiated backup archives (ZIP files) generated when you export your local data;
- data transferred or received when joining a household, accepting a new household member;
- household membership, synchronization state and device-generated cryptographic material used to authenticate paired devices;
- a small local technical diagnostic log described in Section 11.

Homebrewed does not persist Google Play purchase tokens, raw signed purchase records, purchase signatures, ProductDetails objects or billing-flow offer tokens.

This information is processed by the app on your device. Except for the specific external processing described in this policy, baseworks.tech does not receive it, cannot inspect it remotely and cannot recover it for you.

Meal and nutrition information may reveal something about a person's health, diet or routines. The app treats it as local user content: it remains under the control of the device owner and any household members with whom the owner deliberately shares it. Whether Android system backup copies some app files is controlled by Android, the device and the user's backup settings, as described in Section 12.



Section 5: Information Homebrewed does not collect

Homebrewed does not collect, transmit to or store on behalf of baseworks.tech:

- account registration information; the Android app has no Homebrewed account system;
- passwords or authentication tokens for a Homebrewed service;
- advertising identifiers or information for advertising or cross-app tracking;
- precise or approximate location data;
- Health Connect, Google Fit or other connected health-platform data; the current app does not read from or write to those services;
- your contact list, messages, microphone recordings or call information;
- payment-card details, billing addresses or Google Account credentials; Google collects these directly through Google Play and Homebrewed does not access them;
- analytics, usage statistics or behavioural telemetry for baseworks.tech.

The Homebrewed app does receive limited purchase and product information from Google Play on the device, as described in Section 10. That information is processed locally. It is not transmitted to or stored by a baseworks.tech server.

The limited metrics automatically processed by Google ML Kit are described separately in Section 7. Ordinary connection information processed independently by external services is described in Sections 6 and 10.

If you choose to email baseworks.tech for support or privacy assistance, the message and contact details you provide are handled outside the app so the company can respond. The general [baseworks.tech Privacy and Data Protection Policy](#) applies to that correspondence.

Section 6: Open Food Facts

Homebrewed uses the public [Open Food Facts](#) service to look up food products. The following information may be sent to Open Food Facts when you use the corresponding feature:

Feature	Information intentionally included in the request
Barcode lookup	The scanned or entered barcode
Product search	The search words you enter
Product image display	The search words you enter

The requests identify the application as Homebrewed Android but do not deliberately include a Homebrewed profile identifier, advertising identifier, your local database, your location or other meal and recipe content.



Like any internet service, Open Food Facts and the infrastructure serving its API or product images receive ordinary connection information needed to answer the request, such as the requesting IP address, time, requested address and user-agent information. Open Food Facts determines how it logs, retains and otherwise handles that information under its own privacy terms. baseworks.tech does not receive those server logs.

Product results that you keep are stored on your device. Open Food Facts data is contributed by its community and can be incomplete, outdated or incorrect. Its database, contents and images are subject to the licences identified in the Homebrewed Licenses and Acknowledgements document.

Section 7: Camera and Google ML Kit barcode scanning

Homebrewed uses the camera only when you choose a feature that scans a product barcode or a household invitation QR code. Camera frames and detected barcode or QR-code contents are processed on the device. Homebrewed does not deliberately store camera frames or send them to baseworks.tech or Google.

The Android build uses Google's ML Kit barcode-scanning software. Google states that ML Kit input data and results are processed on-device and are not sent to Google servers. Google also states that ML Kit may contact Google servers for matters such as bug fixes, updated models and hardware-accelerator compatibility information, and may collect limited information for diagnostics and usage analytics, including:

- device information such as manufacturer, model, Android version, build and available machine-learning hardware;
- application information such as the package name and app version;
- a per-installation identifier not intended by Google to uniquely identify a user or physical device; and
- performance and utilization metrics for the ML Kit APIs.

Google says this metrics information is encrypted in transit and is not transferred by ML Kit to third parties. Google controls its processing under its own terms and [Privacy Policy](#). See [ML Kit Terms and Privacy](#) and [ML Kit's Google Play data-disclosure guidance](#).

Android asks for camera permission when a scanning feature needs it. You can deny or withdraw camera access in Android Settings. Doing so prevents camera-based scanning but does not remove information already stored in Homebrewed. A barcode may still be entered by another method where the app offers one.

Section 8: Nearby devices, Bluetooth and legacy location permission

Homebrewed uses Bluetooth Low Energy for direct household sharing between deliberately paired Android devices. It does not use Bluetooth for advertising, analytics, location tracking or general presence detection.

On Android 12 and later, Android may request Nearby devices permissions so Homebrewed can scan for, connect to and advertise to nearby household devices. Homebrewed declares that Bluetooth scanning is not used to derive physical location.

On Android 11 and earlier, the Android platform classified Bluetooth discovery behind location permission. The app therefore declares fine-location permission only for those older Android versions so that nearby-device discovery can function. Homebrewed does not request location coordinates, record location history or transmit location to baseworks.tech.

You can deny or withdraw the relevant permission in Android Settings. Doing so prevents the affected household-sharing feature from working but does not remove information already stored in the app or already copied to another household device.

Section 9: Household sharing

Homebrewed allows a small group of deliberately paired devices to keep household entries in sync.

Synchronization occurs directly between those devices over Bluetooth. There is no Homebrewed cloud account, baseworks.tech server or internet relay for household data.

Pairing requires a deliberate exchange between devices. Each device generates cryptographic material used to authenticate household communication, and the direct connection is encrypted and authenticated. Android Keystore facilities protect device-generated identity material where the implementation supports them. When you join an existing household, your current local entries and information are permanently removed and replaced by the household owner's data.

Every member of a household can see and edit the information shared within that household. Only join or invite people whom you intend to give that access. A person with physical or system-level access to an unlocked device may also be able to view information stored there.

You can leave a household using the app's household controls. Leaving stops future synchronization with that household. Information already copied to another member's device remains on that device; baseworks.tech has no remote copy and no technical means to erase another member's local copy.

Section 10: Google Play and Google services

When Homebrewed is obtained through Google Play, Google independently processes information needed to provide Google Play, including installation, update, security, device, account, storefront and payment activity. Google Play Protect or similar Android security services may inspect installed applications for harmful behaviour.

Homebrewed uses the Google Play Billing Library to display and sell the permanent adding and editing unlock. The app requests localized product information from Google Play, including the product identifier, display name, description and localized price.

The app also queries Google Play for currently owned one-time products. Google Play can return information including the product identifier, purchase state, purchase time, acknowledgement status, signed purchase data, purchase signature and purchase token. Homebrewed uses this information on the device to:

- determine whether the permanent unlock is in a purchased or pending state;
- verify that signed purchase data belongs to the Homebrewed package and permanent-unlock product;
- grant permanent access only for a verified purchased record;
- acknowledge a verified purchase through Google Play
- detect a refund or revocation when a later successful ownership query no longer reports the purchase.

The purchase token is used transiently when Homebrewed asks Google Play to acknowledge a purchase. Homebrewed does not persist the token and does not transmit it, the purchase signature, raw signed purchase data, an order identifier or payment credentials to baseworks.tech. There is no baseworks.tech purchase-verification backend and no baseworks.tech receiver of the associated payment event.

Google independently controls the purchase interface, payment processing, Google Account association, transaction records and refund handling. Homebrewed does not receive your Google Account password, full payment-card number or billing credentials.

Google's processing is governed by the [Google Privacy Policy](#) and the [Google Play Terms of Service](#). A device manufacturer or Android distribution may provide additional system services under its own terms.

Section 11: On-device diagnostics

Homebrewed keeps a small local technical log on the device to help diagnose application failures and memory use. The web layer keeps up to 25 recent entries. Records can contain timestamps, error descriptions, stack information and memory measurements. They are designed not to record the contents of meals, recipes or profiles, although an error description may repeat a technical value involved in the error.

Homebrewed and its Bluetooth component can also write technical messages to the Android system log. Android, the device manufacturer, a connected developer tool or a person with sufficient device access controls whether those system logs are retained or extracted.

These diagnostic records are not automatically transmitted to baseworks.tech or to a third-party crash-reporting provider. Removing Homebrewed removes diagnostic files and application storage in its active local container, subject to Android backup, forensic, system-log and deletion behaviour outside that container.

The separate, limited diagnostics and utilization metrics processed by ML Kit are described in Section 7.

Section 12: Backups, device transfer, imports and exports

Homebrewed currently permits Android's backup and device-transfer mechanisms. Depending on the Android version, device manufacturer, Google Account and backup settings, Android may copy eligible app files to a private backup associated with the user's Google Account or transfer them directly to another device. Google or a device manufacturer controls that service, including what is eligible, whether a backup occurs and how long it is retained. Review the device's backup settings and the provider's privacy and security practices.

You can export Homebrewed data as a ZIP archive from Settings. Export preparation takes place on your device. The Android system share interface or document interface then lets you choose where to send or save the archive.

Once you choose another application, person, storage location or cloud provider, that recipient controls the copy you send. An archive can contain the personal and household information described in Section 4. Review the recipient's privacy and security practices and protect exported files against unauthorized access.

Importing an archive replaces the current contents of the app's local database. This also applies when joining a household and importing the transferred data received from the household owner. You are responsible for keeping any export that you need and for understanding the destination or source selected in the Android interface.

Section 13: Retention and deletion

Homebrewed retains local information until you delete the relevant entry, reset the relevant data, delete the app, or replace the database by importing an archive.

You can:

- delete individual meals, recipes, ingredients and products using their in-app controls;
- delete a local profile and its associated entries using the profile controls;

- leave a household to stop future synchronization;
- clear cached Open Food Facts information from Settings;
- reset the local Homebrewed database from Settings; and
- uninstall the app to remove its active local container from the device.

Deleting local information does not delete an export you previously shared, a copy already synchronized to another household member, a system backup or device-transfer copy controlled by Google or a device manufacturer, or connection and metrics records independently held by Open Food Facts or Google. Use the controls of the relevant recipient or service for those copies.

baseworks.tech holds no Homebrewed server copy that it can delete or restore on your behalf. Because the Android app has no Homebrewed account, there is no remote Homebrewed account to delete.

Section 14: Children

Homebrewed is a general-wellness application and is not directed at children. The app has no account or age-verification system and baseworks.tech does not knowingly collect children's personal data through it. A parent or guardian should supervise a child's use where required by applicable law.

Section 15: Your data-protection rights

Where baseworks.tech acts as a controller of personal data, applicable data-protection law may give you rights of information, access, rectification, erasure, restriction, portability and objection, and rights concerning consent and automated decision-making.

In practice, the personal food and household information described in Section 4 stays in your possession. You can inspect, correct, export and delete it using the app without asking baseworks.tech. The app does not make decisions about you that produce legal or similarly significant effects.

For information that you separately provide when contacting baseworks.tech, send a request to privacy@baseworks.tech. We may need information sufficient to understand the request and verify that we are responding to the correct person. We will handle the request within the period required by applicable law.

You may complain to the supervisory authority in the country where you live or work or where you believe an infringement occurred. In the Netherlands, the authority is the [Autoriteit Persoonsgegevens](https://autoriteit.persoonsgegevens.nl).

Questions about information independently handled by Google, Open Food Facts, a device manufacturer, a backup provider or a sharing recipient should normally be directed to that organization using its privacy controls.

Section 16: Security

Homebrewed uses the private application storage and security protections supplied by Android. Household connections are authenticated and encrypted, and household identity material is generated on the device and protected using Android security facilities. Internet requests use encrypted HTTPS connections.

The local Homebrewed SQLite database is not presently protected by a separate app-level database-encryption passphrase. Its protection depends on Android's application sandbox, device encryption, lock-screen security and the user's control of the device. Exported archives must be protected separately by the user.

The app does not provide a company-operated remote backup or recovery service. You remain responsible for securing your device, screen lock, Google Account, shared exports and access by other household members. No storage or transmission method can be guaranteed completely secure.

Section 17: Changes to this policy

We may update this policy when Homebrewed's features, legal obligations, Android behaviour or third-party services change.

The latest version will be published on the [baseworks.tech policies page](#) with a version number and effective date. Material changes affecting how the app handles information will also be identified through an appropriate in-app notice, Google Play release communication or another method where required.

Section 18: Governing language

The authoritative version of this policy is English. A translation may be supplied for convenience. If a translation differs from the English version, the English version prevails to the extent permitted by applicable law. Mandatory language requirements remain unaffected.

Section 19: Contact

Privacy questions, requests or complaints:

privacy@baseworks.tech

General Homebrewed support:

support@baseworks.tech

Postal correspondence:

baseworks.tech, Box E1586, Oder 20, 2491 DC Den Haag, Netherlands

 baseworks.tech