



Privacy Policy – Papybara Application Manager

Version 2.3 · As of October 22, 2026

This English version is a courtesy translation. Only the German version is legally binding; in case of any discrepancy the German version prevails.

1. Summary

The Papybara Application Manager is a desktop application that runs locally. All data stays on your device and is stored encrypted. There is no user account, no provider cloud, no telemetry, no advertising, no tracking and no cookies. The Provider receives no data and has no access to it.

Data leaves your device only if you explicitly switch on or use an optional feature (Section 5). There is neither a license key nor a trial period; the Software therefore also stores no start date and no key and writes nothing to the Windows registry.

2. Provider and Responsibility

Provider of the Software: Christian Molter, München, contact: c.molter.m@gmail.com.

Because the Provider neither collects, stores nor can view any personal data, the Provider is not the controller within the meaning of the GDPR for the data stored in the Software. You yourself are responsible for the data you enter in the Software. For purely private use (managing your own job applications) the exemption for personal and household activities applies (Art. 2(2)(c) GDPR).

The Provider merely processes the local record of consent to the Terms of Use on your device (Section 3); this too is not transmitted to the Provider.

3. Which Data the Software Processes Locally

Everything you enter or import: applications (company, position, status, dates, salary and note fields, job links and descriptions, cover letter drafts), interview appointments, tasks, journal entries, the job board list, uploaded documents (e.g. résumé, references, cover letters as PDF), banner images and settings. This may include personal data of third parties, such as names, email addresses and phone numbers of contact persons.

To document your consent to the Terms of Use the Software stores locally: time, version and checksum of the text, software version, Windows user name and computer name (legal basis Art. 6(1)(f) GDPR, legitimate interest in documentation).

The sole purpose of the processing is to manage and evaluate your job applications. For private use the legal basis is your own decision; where the GDPR applies, Art. 6(1)(b) or (f) GDPR.

4. Storage Location and Data Flow

The data is located in the data folder "Bewerbungsmanager-Daten" in your user directory (or at the location you set for it). There is no automatic transmission to the Provider or to third parties. The Software contains no analytics, crash reporting or advertising components.

5. Optional Features with Data Transmission

These features are off by default or require your explicit action. Without them no data is transmitted.

a) Google Calendar (switch under Settings → Security → Google): the Software creates and updates

calendar events for interviews, follow-ups and employment contracts. Transmitted are the event time, title (company, position, type) and, if applicable, location/link/notes. The sync runs in the background as long as the connection exists. Permission: "calendar.events".

b) Reading Gmail (separate switch): at your request the Software searches the mailbox for rejection wording and reads matching messages for that purpose. The evaluation takes place locally on your device; message contents are not stored permanently. Status changes happen only after your confirmation. Permission: "gmail.readonly".

c) Gmail draft (separate switch): at the press of a button the Software creates a draft in your Gmail account (recipient, subject, text and the PDF attachments you choose). It never sends emails; sending is done exclusively by you in Gmail. Permission: "gmail.compose".

For a) to c) you use your own Google Cloud project. There is a direct connection between your device and Google (Google Ireland Limited / Google LLC, USA); processing there is governed by Google's privacy terms. The provider of this Software is not involved. The credentials (client ID, client secret, access token) are stored only locally in the encrypted database. You can disconnect at any time in the Software and revoke access in your Google account (Security → Third-party access).

d) Retrieving a job link (match assessment): the Software retrieves the job page you stored. For technical reasons the target page receives your IP address and a standard browser identifier. The assessment itself takes place locally; retrieval and evaluation trigger no further transmission.

e) Claude AI / other AI (switch under Settings → Claude AI): the Software creates a text (prompt) locally that may contain the job posting and excerpts of your profile documents. It is not transmitted automatically: you copy it yourself into Claude or a privacy-compliant AI of your choice. From then on the terms and privacy notices of that provider apply. Before pasting, check whether it contains personal data of third parties and pay attention to the settings for training and processing (e.g. data processing agreement, turning off training).

f) Opening links (job boards, job links, vendor sites, the website www.papybara.de with the current version and information, and the "Community Support" button in the sidebar, which opens the community forum on [papybara.de](https://www.papybara.de/de/community-forum): <https://www.papybara.de/de/community-forum> with the German interface, <https://www.papybara.de/en/forum> with the English one): the Software hands the link to your default browser only when you click. From the moment of the call there is a connection between you and the respective website, whose privacy notices apply.

The community forum is an offering of the Provider on the website [papybara.de](https://www.papybara.de). The Software transmits no data to it. The privacy policy of the website [papybara.de](https://www.papybara.de) applies to visiting, registering and posting in the forum. Do not post credentials, passwords, recovery codes or confidential application data in the forum.

g) Checking for a new version (switch in Settings → Automation; you are asked once at the first start): the Software retrieves the small version information from www.papybara.de at most once every 24 hours. It contains only the current version number, a download link, a checksum and notes on the new version; the Software only evaluates it if it contains these details and an https address on [papybara.de](https://www.papybara.de). None of your data and no version number are sent. For technical reasons the web server sees your IP address and the time of the request (usual server logs of the web host); the Provider does not evaluate them. The legal basis is your consent (Art. 6(1)(a) GDPR), which you can withdraw at any time by turning the switch off. A download of the new version only happens after your confirmation, from www.papybara.de, and is verified against the checksum; nothing is installed without your action. Only the time of the last check, the skipped version and the date of the reminder pause are stored locally in the encrypted database.

6. Technical and Organizational Measures (Art. 32 GDPR)

Encryption: the database, documents and banners are stored with AES-256-GCM (authenticated encryption, which also protects against unnoticed modification). The database runs in main memory and is written to disk only in encrypted form; no unencrypted database file is created.

Key management: a random 256-bit master key encrypts the data. It exists only in wrapped (encrypted)

form. In password mode the wrapping key is derived solely from your password (scrypt, $N = 2^{15}$, $r = 8$, $p = 1$); the password itself is not stored. In two-factor mode (password + authenticator code) the same applies, and in addition the authenticator secret is stored wrapped with the master key; the code is an additional sign-in barrier of the app. In pure authenticator mode the master key is wrapped with a device key from the operating system vault (Windows: Credential Manager/DPAPI); protection there depends on the Windows user account (password mode is stronger and is recommended). In addition there is a recovery code that is shown once.

Access protection: password policy (at least 12 characters with at least 3 of 4 character types, or a passphrase of 25 characters or more; trivial passwords are rejected; no forced changes) and increasing lockout times after failed attempts.

Backups: automatic backup copies (daily, weekly, monthly) and a copy before every program update. They contain only the encrypted files. Rotation limits the number of copies kept. An additional manual backup to a location of your choice is possible.

Data minimization and transparency: no telemetry, no accounts, connections to third parties only through explicit features that can be switched off (Section 5); Gmail access separated into reading and drafts, each with the least permission required; the Software does not send emails.

Limits for which you are responsible: while the Software is running, the data is held decrypted in main memory. Export files (e.g. PDF/CSV for the employment agency, the complete export of all data, .ics calendar file, backup copies that you place elsewhere) are created by you and are not encrypted by the Software unless you protect them yourself. Protect your device (disk encryption such as BitLocker, screen lock, updates, antivirus) and keep your password, recovery code and backups safe. Without the password or recovery code nobody – not even the Provider – can restore the data.

7. Recipients and Transfers to Third Countries

The Provider receives no data. Recipients arise only through your use of optional services (Google, websites, the AI of your choice). Google may process data in the USA; safeguards exist under the EU-US Data Privacy Framework or standard contractual clauses. For other services their own statements apply.

8. Retention and Deletion

The data remains stored until you delete it. You delete individual entries in the Software; deleted applications, interviews, to-dos, journal entries and job boards then stay in the trash for 30 days (still encrypted) and are deleted automatically afterwards; in the trash you can delete them permanently right away. A local error log (file "fehlerprotokoll.log" in the data folder) contains only technical error messages without application data and is never transmitted automatically; you can pass it on yourself as an error report. You achieve complete deletion by uninstalling and deleting the data folder including the backup folder and, if used, by disconnecting from Google and deleting the calendar events and drafts created there. Further copies you have made (exports, backups, AI chats) you delete at the respective location.

9. Data of Third Parties (Contact Persons, HR Departments)

Record only data that is necessary for your application (data minimization). Do not pass data of third parties on to external services (in particular AI providers) without need. If you use the Software commercially or for other people, you are yourself responsible for GDPR compliance (e.g. information duties, data processing agreements); the Terms of Use permit private use only.

10. Your Rights

Under the GDPR you have rights to access, rectification, erasure, restriction of processing, data portability and objection (Arts. 15–21) as well as the right to lodge a complaint with a data protection supervisory authority (e.g. the Bavarian State Office for Data Protection Supervision). Because the Provider holds no data of yours, you can exercise them directly yourself: viewing, changing and deleting in the Software, export through the export functions, safekeeping through the backup. If you have questions, contact

c.molter.m@gmail.com. For data held by Google or AI providers, contact the respective provider.

11. Changes

This policy will be adjusted when features or data flows change. The version shown in the Software under Settings is authoritative (currently version 2.3, as of October 22, 2026, for software version 2.26).

Note: this policy is a carefully prepared draft and not legal advice.