Privacy Policy (App)

As of: 17.11.2026

1. Service provider and responsible person in terms of the GDPR

Responsible provider of the BillMore application in terms of data protection law is:

BillMore GmbH
Kolpingstraße 14
73433 Aalen
Register Court: HRB 735402, Ulm
VAT ID: DE313425388
CEO: Steffen Keller

Phone: +49 7361 9992490

The provider is currently not obliged to appoint a data protection officer. You can reach our contact person for data protection matters at privacy@billmore.de, or by mail to the above address with the address suffix "Data Protection".

2. General

Your personal data (hereinafter referred to as "data") will be processed by the operator (hereinafter also referred to as "BillMore", "we" or "us") only to the extent necessary and for the purpose of providing functional and user-friendly products, including the content contained therein and the services offered therein. The following products are offered by BillMore:

- **Web App** (app.billmore.com)
- **Mobile App for iOS** (apps.apple.com/app/id1155855485)
- **API** (api.billmore.com)

With the following privacy policy, we inform you in particular about the type, scope, purpose, duration and legal basis of the processing of personal data, insofar as we decide either alone or together with others on the purposes and means of processing. In addition, we inform you below about the third-party components we use for optimization purposes and to increase the quality of use, insofar as other providers process data on their own responsibility.

3. Information on the collection of personal data

(1) We provide you with a web app that you can access via your browser, a mobile app that you can download to your (mobile) device (iOS, Android), and an application programming interface (API) that you can access programmatically (hereinafter collectively referred to as "Products"). In the following, we provide information about the collection of personal data when using our products. Personal data is any information relating to an identified or identifiable person (Art. 4 No. 1 GDPR).

(2) When you contact us by email or via a contact form, we will store your email address and, if provided by you, your name and telephone number in order to answer your questions. We delete the data arising in this context after storage is no longer necessary or - in the case of statutory retention obligations - restrict processing.

(3) If we use contracted service providers for individual functions of our products or wish to use your data for advertising purposes, we will inform you in detail below about the respective processes. We will also state the specified criteria for the storage period.

(4) In addition to the purely informational use of our products, we offer various services that you can use if you are interested. To do so, you must generally provide additional personal data that we use to provide the respective service and to which the aforementioned data processing principles apply.

(5) In some cases, we use external service providers to process your data. These have been carefully selected and commissioned by us and are regularly monitored.

4. Your rights

(1) You have the following rights with respect to the personal data concerning you:

- Right of information,
- Right of correction or deletion,
- Right to limit processing,
- Right to object to the processing,
- Right of data transferability.

(2) You also have the right to complain to a data protection supervisory authority about the processing of your personal data in our company.

5. Use of cookies

(1) When using our products, cookies are stored on your device. Cookies are small text files saved in your device's memory. Through cookies, the entity that places the cookie (in this case, us) can receive certain information. Cookies cannot run programs or transmit viruses to your device. They are intended to make our products more user-friendly and efficient overall. This particularly includes session cookies. These store a so-

called session ID, which can be used to assign multiple requests from you. This way, your device can be recognized if you use our products again. Session cookies are deleted when you log out.

(2) You can configure your operating system and the mobile app settings according to your preferences, for example, to refuse third-party cookies or all cookies. Please note that you may not be able to use all the functions of our products if you do so.

(3) When using our mobile app, instead of cookies, we use a technology with a comparable function. A randomly generated ID is assigned to the user and stored. The legal basis for using technically necessary cookies is Art. 6(1) sentence 1(f) GDPR. The legal basis for using cookies that are not technically necessary is Art. 6(1) sentence 1(a) GDPR.

6. Creation of Log Files

(1) When you use our products, we automatically collect certain technical data in so-called log files. This data is necessary to ensure the security and stability of our systems and to optimize our services. In particular, the information collected includes:

- IP address of the accessing device
- Date and time of access
- Name and URL of the requested file
- Browser and operating system used
- Amount of data transferred
- Access status/HTTP status code

(2) The processing of this data takes place in accordance with Art. 6(1) sentence 1 lit. f) GDPR to protect our legitimate interest in ensuring technical security and optimizing our services. The stored log data is automatically deleted after no more than 30 days unless a longer retention period is required for error analysis or security reasons.

(3) When you use our application programming interface (API), we process the corresponding server and access logs (specifically, the time, the endpoint accessed, the amount of data transferred, and the status code). In addition, for certain processes, such as the deletion of documents, contacts, or products, we create audit log entries with a snapshot of the relevant data record to ensure the proper processing is traceable. The legal basis is Art. 6(1)(f) of the GDPR; in the context of data processing on behalf of a client, the provisions of the data processing agreement apply. These entries are deleted as soon as they are no longer necessary for the stated purposes and no statutory retention obligations preclude their deletion.

7. Collection of Personal Data When Using Our Mobile App

(1) When you download our mobile app, the respective app store of your device's operating system processes certain data, such as your username, email address, or payment information. We have no influence over and are not responsible for this data processing. We only receive the information that is necessary for providing and managing the app.

(2) Within the mobile app, we also process the device identifier as well as a randomly generated ID to enable the use of the app and to provide certain features.

(3) When you use certain features of our mobile app for the first time, we will ask for your permission in a pop-up to access your camera (e.g., for scanning receipts), your photos (e.g., for uploading your logo), or your address book (e.g., for adding customers). If you do not grant permission, we will not use this data. In that case, you may not be able to use all functions of our app. You can later grant or revoke this permission in the app settings or in your device's operating system settings. If you allow access to this data, the app will only access and transfer it to our server to the extent necessary to provide the functionality. Your data will be treated confidentially and deleted if you revoke usage rights or if it is no longer required for service provision, provided no legal retention obligations exist. The legal basis for this processing is Art. 6(1) sentence 1 lit. f) GDPR.

8. Storage of data and documents

(1) When you use our application (mobile app or web app), all data you enter, especially third-party address data (e.g., address, telephone number, fax number, company-related data, order data, contract data, etc. of your customer), is stored in encrypted form in a database controlled by us at the provider MongoDB (see Section 13). Documents created with the application (e.g., invoices, estimates, delivery dockets, etc.) as well as uploaded documents (e.g., recorded expense receipts, etc.) and images (e.g., your company logo) are encrypted and stored on servers of the Google Cloud Platform (see Section 15). The data and documents mentioned above can also be created, retrieved, and managed via our application programming interface (API); they are stored within the same infrastructure.

(2) Insofar as we act as a processor within the meaning of commissioned data processing pursuant to Article 28 of the GDPR in connection with our services, i.e., if we process personal data on your behalf and in accordance with your instructions, for which you are responsible under data protection law, the statutory provisions on commissioned data processing shall apply between BillMore and you. For this purpose, the data processing agreement (DPA) concluded with you applies, available at https://billmore.com/legal/dpa (currently available in German). The sub-processors we engage are listed at https://billmore.com/legal/subprocessor.

9. Sending of emails

(1) For sending emails, we use the services of Amazon Web Services (see Section 14). This includes the dispatch of automatically generated information emails, such as for account confirmation or password resets, the

distribution of our newsletter, as well as emails you send to your own customers through our email services (e.g., to send generated documents).

(2) As part of the email dispatch, the data required for delivery is transmitted to the provider by way of commissioned data processing. This includes in particular the sender information (the email address provided during user account management and, if applicable, your name), the recipient address, the subject and content of the message including any attachments (e.g., documents such as invoices sent by you), as well as technical dispatch and delivery information (e.g., time, delivery status). Insofar as you send messages to your own customers via our email services, personal data of these recipients may also be processed, for which you are responsible under data protection law.

10. User account

(1) If you wish to use our application (mobile app or web app), it is necessary for concluding the contract that you provide your personal data, which we require to process your order and to assign your stored data. For this purpose, we may transmit your payment data to our bank or to the respective payment service provider. The legal basis for this is Art. 6(1) sentence 1 lit. b) GDPR. Information about your user account (email address, first name, last name, company name, address, telephone number, IP address, date of registration) is stored in a database controlled by us at the provider MongoDB (see Section 13).

(2) Due to commercial and tax law requirements, we are obligated to store your address, payment, and order data for a period of up to eight years (Section 257 HGB, Section 147 AO); the period begins at the end of the calendar year in which the respective document was created. However, after two years, we restrict the processing, meaning your data is only used to fulfill legal obligations.

(3) To prevent unauthorized third-party access to your personal data, especially financial data, the ordering process is encrypted using TLS technology.

(4) We log your acceptance of the Terms of Use and the data processing agreement upon registration, as well as your acceptance of amended versions, with the time, user, text version and IP address; we retain the accepted text versions. The log serves as proof of the conclusion of the contract and of the terms agreed in each case. The legal basis is Art. 6(1) sentence 1 lit. f) GDPR and, insofar as commercial and tax retention obligations apply, Art. 6(1) sentence 1 lit. c) GDPR. We delete the log at the end of the sixth calendar year after the end of the contract.

11. Payment processing

(1) In our web app, we use Mollie B.V. as a payment processor to ensure your payments can be handled securely and smoothly. As part of the payment process, we transmit to Mollie the information necessary for completing the transaction, such as first and last name, company name, street, postal code, city, country, credit card details, bank account details, and the payment method used. Only the data actually required to carry out the payment is shared. The legal basis for this processing is Art. 6(1) sentence 1 lit. b) GDPR.

(2) Third-Party Provider Information: Mollie B.V., Keizersgracht 126, 1015 CW Amsterdam, Netherlands, Tel.: +498920194095; Terms of Use: https://www.mollie.com/user-agreement, Privacy Policy: https://www.mollie.com/privacy.

(3) In addition, in our mobile app, we offer the option to process payments directly through the Apple App Store. In this case, the payment method stored in your Apple account is used. If you submit a refund request to Apple, we receive what is known as a "Consumption Request," which is used to determine whether you have utilized the paid services or not. As part of this process, the necessary usage data is transmitted to Apple to support the refund process. The legal basis for this processing is also Art. 6(1) sentence 1 lit. b) GDPR. You can find more information on payments via the App Store in Apple's relevant terms and conditions and privacy notices: https://www.apple.com/legal/internet-services/itunes/.

12. AI-supported features

(1) We offer AI-supported features in our products. These are provided using AI services that our processor Amazon Web Services (see Section 14) operates exclusively in data centers within the European Union. The content is not transferred to third parties – in particular not to the providers of the underlying AI models – and is not used to train AI models. AI-supported features are labeled as such in our products.

(2) Receipt recognition and booking suggestions: At your request, we analyze receipts you upload and generate suggestions (e.g., booking suggestions). For this purpose, the content of the respective receipt as well as – to identify recurring booking patterns – key data of previous bookings with the same business partner (date, amounts, tax rates, accounts, line item descriptions; no names or contact details) are processed. This feature is only used after the owner of the company has activated it in the settings; the activation can be ended there at any time with effect for the future. The time and user of the activation or deactivation are logged; we delete the log at the end of the third calendar year after the deactivation. The legal basis for this processing is Art. 6(1) sentence 1 lit. b) GDPR and, for the logging, Art. 6(1) sentence 1 lit. f) GDPR; insofar as you process personal data of your own customers in this context, the data processing agreement concluded between you and us applies.

(3) To manage the monthly usage quotas and to control costs, we store technical usage data for each receipt analysis pursuant to paragraph 2 (company, triggering user, time, model used, volume of processed data in tokens, processing duration and status). The content of the receipts or of the suggestions is not included. The legal basis is Art. 6(1) sentence 1 lit. b) and lit. f) GDPR (billing, prevention of misuse).

(4) AI assistant: Our products provide an AI assistant that answers your questions about using the software on the basis of our documentation. It does not require activation. Only the question text you enter is transmitted to the AI service; no data from your user account or your company is transmitted. Please do not enter any access credentials or any personal data that is not required to answer your question. Questions and answers are stored together with the time and the associated user account and are reviewed by our employees on a random basis

in order to improve the quality of the answers and of our documentation, to identify incorrect answers, and to prevent misuse. To prevent misuse, the number of requests per period is technically limited. The legal basis is Art. 6(1) sentence 1 lit. b) GDPR (support in using the software) and, for the storage and evaluation, Art. 6(1) sentence 1 lit. f) GDPR; our legitimate interest lies in improving our support and preventing misuse.

13. Use of MongoDB

We use the services of MongoDB Ltd. as our central database. This is necessary to ensure technically error-free and highly available services. The data is stored on Amazon Web Services servers in the Frankfurt data center operated by MongoDB, while MongoDB Inc. provides the technical management of the database.

Third-Party Provider Information: MongoDB Ltd., 3 Shelbourne Building, Crampton Avenue Ballsbridge, Dublin 4, Irland. Phone. +35319014654; Terms of Use: https://www.mongodb.com/cloud-terms-and-conditions , Privacy Policy: https://www.mongodb.com/legal/privacy-policy.

In exceptional cases where personal data may be transferred by MongoDB to third countries and authorities could potentially access the data stored by the provider, we have concluded a data processing agreement with the provider to ensure an appropriate level of protection. The provider also assures that it has concluded contracts with its subcontractors in non-European countries based on the EU Standard Contractual Clauses in accordance with Art. 46(2)(c) GDPR, in order to maintain the same level of protection.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Based on this adequacy decision, data transfers to companies certified under the DPF may be carried out pursuant to Art. 44 and Art. 45 GDPR. MongoDB is one of those certified companies.

The legal basis for processing is Art. 6(1) sentence 1 lit. b) GDPR. For the use of MongoDB, including the involvement of MongoDB's subcontractors, Art. 49(1) sentence 1 lit. b) GDPR also applies. The use of MongoDB is necessary for contract performance to reliably provide the online services.

14. Use of Amazon Web Services (AWS)

We use the services of Amazon Web Services EMEA SARL to ensure technically error-free and highly available services. This particularly includes a central server for communication between our products and the databases. The data is processed on Amazon Web Services servers located in the Frankfurt data center, while the server itself is managed by us. We also use AWS services for sending emails (see Section 9).

Third-Party Provider Information: Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg, Fax: + 352 2789 0057; Terms of Use: https://aws.amazon.com/agreement/, Privacy Policy: https://aws.amazon.com/privacy/, Further Information on GDPR Compliance: https://aws.amazon.com/compliance/gdpr-center/.

In exceptional cases where personal data may be transferred by AWS to third countries and authorities could potentially access the data stored by the provider, we have concluded a data processing agreement with the provider to ensure an appropriate level of protection. The provider also assures that it has concluded contracts with its subcontractors in non-European countries based on the EU Standard Contractual Clauses in accordance with Art. 46(2)(c) GDPR, in order to maintain the same level of protection.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Based on this adequacy decision, data transfers to companies certified under the DPF may be carried out pursuant to Art. 44 and Art. 45 GDPR. AWS is one of those certified companies.

The legal basis for processing is Art. 6(1) sentence 1 lit. b) GDPR, as well as Art. 49(1) sentence 1 lit. b) GDPR for the use of Amazon AWS, including the involvement of subcontractors by Amazon. The use of AWS is necessary for fulfilling the contract to provide a secure and highly available online service.

15. Use of Google Cloud Platform (GCP)

In order to provide technically error-free and highly available services, we use services from Google Cloud EMEA Limited. This includes, in particular, the Firebase service, which we use to reliably store your documents and data (see Section 8) in a data center in Frankfurt.

Third-Party Provider Information: Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland, Fax: +353 (1) 436 1001. Firebase Terms of Service: https://firebase.google.com/terms, GCP Terms of Service: https://cloud.google.com/terms, Firebase Data Processing Terms: https://firebase.google.com/terms/data-processing-terms, GCP Privacy Notice: https://cloud.google.com/terms/cloud-privacy-notice, Google Privacy Policy: : https://policies.google.com/privacy, Additional information about GCP data processing: https://cloud.google.com/terms/data-processing-addendum.

In exceptional cases where personal data is transferred to Google LLC in California, USA, and U.S. authorities may access data stored by Google, the level of protection can be safeguarded by entering into data processing agreements with standard contractual clauses pursuant to Art. 46(2)(c) GDPR. We have concluded the corresponding data processing agreement with Google.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Under this adequacy decision, data can be transferred pursuant to Art. 44 and Art. 45 GDPR to companies certified under the DPF. Google is one of those certified companies.

The legal basis for processing is Art. 6(1) sentence 1 lit. b) GDPR, and for the use of the Google Cloud Platform including Google's subcontractors, Art. 49(1) sentence 1 lit. b) GDPR. The use of Google Cloud Platform is necessary for contract fulfillment to reliably provide our online services.

16. Use of Google Analytics

(1) Provided you have given us your consent, we use Google Analytics in our products, a web analytics service offered by Google Ireland Ltd. ("Google"). Google Analytics uses what are known as "cookies," text files that are stored on your computer and enable an analysis of your use of the products. The information generated by the cookie about your use of our products is typically transmitted to a Google server in the U.S. and stored there. If IP anonymization is enabled, however, Google will truncate your IP address within Member States of the European Union or in other contracting states of the Agreement on the European Economic Area. Only in exceptional cases will the full IP address be transmitted to a Google server in the U.S. and truncated there. Acting on behalf of the operator of these products, Google will use this information to evaluate your use of our products, to compile reports on activities, and to provide the operator with other services related to product usage and internet usage.

(2) The IP address transmitted from our products through Google Analytics is not combined with other Google data.

(3) The legal basis for data processing is Art. 6 lit. a) GDPR. The use of Google Analytics is voluntary and is intended to help us improve our services. You can enable or disable this feature via an opt-in switch in the settings of the mobile app under "Settings – Usage Data." In our web app, you can disable the feature in the cookie settings at the bottom of the page. Alternatively, you can also prevent the transmission of cookies via your internet browser settings and delete already stored cookies.

(4) We use Google Analytics with the extension "_anonymizeIp()." This means IP addresses are processed only in truncated form, making any direct personal reference impossible. If any data collected about you can be linked to you personally, it will be immediately excluded and the personal data promptly deleted.

(5) We use Google Analytics to analyze the use of our products and to make regular improvements. The collected statistics enable us to enhance our services and make them more interesting for you as a user. In exceptional cases where personal data may be transferred to Google LLC in the U.S., based in California, and where U.S. authorities might be able to access the data stored by Google, the level of protection can be assured by entering into data processing agreements with Standard Contractual Clauses in accordance with Art. 46(2)(c) GDPR. We have concluded a corresponding data processing agreement with Google. The legal basis for using Google Analytics is your explicit consent pursuant to Art. 6(1) sentence 1 lit. a) GDPR.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Under this adequacy decision, data can be transferred pursuant to Art. 44 and Art. 45 GDPR to companies certified under the DPF. Google is one of those certified companies.

(6) Third-Party Provider Information: Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland, Fax: +353 (1) 436 1001. Terms of Use: https://marketingplatform.google.com/about/analytics/terms/us/, Privacy Policy: https://policies.google.com/privacy

(7) The usage data that is stored will be deleted by Google after no more than 12 months.

17. Use of Vercel

We use the services of Vercel Inc. for hosting our web app. All data is forwarded by Vercel to our servers. Vercel does not use or store your data. Hosting with Vercel is required to ensure the reliable provision of products and to provide technically error-free and highly available services as part of fulfilling our contractual obligations to you.

Third-Party Provider Information: Vercel Inc.,440 N Barranca Avenue #4133, Covina, CA 91723, United States; Terms of Use: https://vercel.com/legal/terms, Privacy Policy: https://vercel.com/legal/privacy-policy, Additional Information on Data Processing Agreements: https://vercel.com/legal/dpa.

If data is processed via "Vercel Functions," the Frankfurt region is used. In exceptional cases where personal data may be transferred to Vercel in the USA and U.S. authorities could potentially access the data stored by the provider, we have concluded a data processing agreement with the provider based on the EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR, to ensure an adequate level of protection.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Under this adequacy decision, data can be transferred pursuant to Art. 44 and Art. 45 GDPR to companies certified under the DPF. Vercel is one of those certified companies.

The legal basis for processing is Art. 6(1) sentence 1 lit. b) GDPR, as well as for the use of Vercel—along with its subcontractors—pursuant to Art. 49(1) sentence 1 lit. b) GDPR. The use of Vercel is necessary for contract performance to reliably provide our online services. Vercel is required for operating the web app, enabling the software to be used via a browser in addition to the mobile app.

18. Use of Zendesk

We use the Zendesk ticketing system for the efficient handling of customer inquiries. When you use this system, incoming emails, their content, and any additional data you voluntarily provide will be forwarded to Zendesk in order to record, process, and respond to your inquiry promptly. The data is processed in a data center in Ireland.

Third-Party Provider Information: Zendesk, Inc.,1019 Market Street, Suite 600, San Francisco, CA 94103 United States; Terms of Use: https://www.zendesk.com/company/agreements-and-terms/main-services-agreement/, Privacy Policy: https://www.zendesk.com/company/agreements-and-terms/privacy-notice/.

In exceptional cases where personal data may be transferred by Zendesk to third countries and authorities could potentially access the data stored by the provider, we have concluded a data processing agreement with the provider to ensure an appropriate level of protection. The provider also assures that it has concluded contracts

with its subcontractors in non-European countries based on the EU Standard Contractual Clauses in accordance with Art. 46(2)(c) GDPR, in order to maintain the same level of protection.

Furthermore, on July 10, 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework (DPF). Under this adequacy decision, data can be transferred pursuant to Art. 44 and Art. 45 GDPR to companies certified under the DPF. Zendesk is one of those certified companies.

The legal basis for this processing is the performance of a contractual relationship pursuant to Art. 6(1) sentence 1 lit. b) GDPR, as well as our legitimate interests in optimizing our customer service pursuant to Art. 6(1) sentence 1 lit. f) GDPR.

19. Use of finAPI (bank connection)

(1) In our web app, you can connect your company's bank accounts in order to retrieve account transactions and match them with your invoices and receipts. Access is read-only; no payments are initiated. This feature is only used after the owner of the company has expressly activated it (agreement to the bank connection); only the owner can set up and disconnect bank connections. The bank connection can be ended in the settings at any time with effect for the future. The activation is logged with the time, user, text version and IP address; we delete the log at the end of the third calendar year after the bank connection ends.

(2) The account information is retrieved from your bank by finAPI GmbH, a payment institution supervised by the German Federal Financial Supervisory Authority (BaFin), with which you conclude a separate user agreement for this purpose. In this respect, finAPI processes your data as an independent controller. You log in to your bank on a page operated by finAPI; we never receive or store your bank credentials. Whether finAPI stores your credentials for automatic retrievals is decided by you in finAPI's form. We transmit to finAPI a pseudonymous user identifier and the information required for the retrieval (start date, account types, language); your name and email address are not transmitted. If you trigger a refresh manually, your IP address and information about your browser and operating system are additionally transmitted to finAPI and from there to your bank. In addition, finAPI retrieves the transactions automatically once a day, unless the owner disables this in the settings. According to finAPI, the data is processed in data centers in Germany or the EU.

(3) finAPI initially retrieves all accounts of your bank login, including privately used accounts. To enable the owner to select the accounts, we store their account data (IBAN, account name, account holder, account type, currency, balance) until the selection is made. We only retrieve transactions for the selected accounts. We delete the account data of accounts that are not selected after the selection and have these accounts deleted at finAPI. The same applies to accounts removed later; para. 5 applies accordingly to transactions already retrieved. For the selected accounts, account data (IBAN, account name, account holder, account type, currency, balance), transactions (booking and value date, amount, currency, payment reference, name and IBAN of the counterparty, references) and connection details (name of the bank, status, expiry of the authorization) are stored

in encrypted form in our database (see Section 13). The transactions are visible to the owner and the administrators of the company.

(4) The legal basis for this processing is Art. 6(1) sentence 1 lit. b) GDPR and, for logging the activation, Art. 6(1) sentence 1 lit. f) GDPR. Insofar as the transactions contain personal data of third parties (e.g., payers or payees), the data processing agreement concluded between you and us applies.

(5) If you disconnect a bank connection, we have it deleted at finAPI. When doing so, you decide whether the transactions and matches already retrieved are deleted or remain stored as your company's accounting data. Stored transactions remain until you delete them; after the end of the contract, § 8 (9) of the Terms of Use applies. When the last bank connection is disconnected, or 14 days after your subscription ends or you switch to a plan without bank connection, we also have your user deleted at finAPI. finAPI's statutory retention obligations remain unaffected.

(6) Third-Party Provider Information: finAPI GmbH, Adams-Lehmann-Straße 44, 80797 Munich, Germany; Privacy Policy: https://finapi.io/datenschutz. finAPI's terms of use and privacy notice for the account information service are displayed to you on finAPI's page when you connect.

20. Data Exchange via Interfaces to Third-Party Services

(1) If you activate an interface to a third-party service, we will, at your request, transmit the data required for the respective function to that service or receive data from it in order to provide the respective function (e.g., transmission of invoice and receipt data to an accounting or tax consulting system, generation of payment links and processing of payments, or transfer of order data for automatic document creation). For the bank connection, Section 19 applies in addition.

(2) Only the data required for the activated function is exchanged. Depending on the arrangement, the operator of the connected service processes the data either as an independent controller or as your processor; in this respect, its privacy policy applies. The legal basis is Art. 6(1)(b) or (f) of the GDPR; in the context of commissioned data processing, the data processing agreement concluded between you and us applies.

(3) If a service connected by you processes data in a third country, the transfer takes place at your instigation; you are responsible for ensuring an adequate level of protection vis-à-vis the recipient, unless the recipient is our subcontractor.

21. Objection or Withdrawal of Consent to the Processing of Your Data

(1) If you have given consent to the processing of your data, you may withdraw this consent at any time with effect for the future. Such a withdrawal will affect the lawfulness of the processing of your personal data after you have notified us of your withdrawal. You can manage and revoke your consent in the settings of the application at any time with effect for the future.

(2) Insofar as we base the processing of your personal data on legitimate interests (Art. 6(1) lit. f) GDPR), you have the right to object to such processing. This particularly applies if the processing is not necessary for the performance of a contract with you, as described in the following explanation of each function. When exercising such an objection, please explain the reasons why you believe we should not process your personal data in the manner we do. In the event of a justified objection, we will review the matter and either cease or adjust the data processing, or demonstrate to you our compelling legitimate grounds for continuing the processing.

(3) Of course, you may object at any time to the processing of your personal data for advertising and data analysis purposes. You can inform us of your objection to advertising by using the settings function within our web app or mobile app.