Data Privacy Statement Finanzcockpit

We thank you for your interest in our products, our company and how we handle the data you have entrusted to us.

1. Responsible Authorities and Contact

Star Finanz-Software Entwicklung und Vertriebs GmbH, Grüner Deich 15, 20097 Hamburg, is the party responsible for matters related to data privacy laws.

If you have any questions related to data privacy law, you can contact our data privacy officer at: Star Finanz-Software Entwicklung und Vertriebs GmbH, Data Privacy Officer, Grüner Deich 15, 20097 Hamburg, fax +49 40 23728-350

E-mail: datenschutz@starfinanz.de

2. Data Privacy Principles

We assure you of the lawful and responsible handling of all data that you transmit to us as a user of our products. In the following, we would like to show you in a transparent manner which data we process in detail, what we use it for and whether—and, if so, to what extent—it is stored by us and/or disclosed to third parties.

2.1 What sources and data we use

We process personal data only to the extent that has been personally authorized by you. As part of that, we only collect and process the data that is absolutely necessary to maintain and use the services that are made available to you. All services that transmit personal data inform you of the exact scope of the data prior to using and transmitting your data and request your acknowledgement of the transmission. All of your data belongs to you; therefore we do not convey any of the data transmitted to us to third parties without your consent unless we are legally obliged to do so (e.g., if there is an applicable court order).

By way of example, personal data can be understood as: personal details (name, address and other contact information, date and place of birth and nationality), identification data (e.g., ID card information) and authentication data (e.g., signature sample). Furthermore, this can also include order data (e.g., payment order, securities order), data from the fulfillment of our contractual obligations [e.g., sales data in payment transactions, credit lines, product information (e.g., deposit, credit and portfolio transactions)], information about your financial situation (e.g., creditworthiness, scoring/rating data, origin of assets), advertising and sales data (including advertising scores), documentation data (e.g., consultation records), registry data, data on your use of the telemedia we offer (e.g., timestamp when accessing our website, apps or newsletter; clicks or information entered on our pages as well as other similar data).

2.2 Principles of data processing to fulfill contractual obligations

We process the personal data you transmit to us in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (Bundesdatenschutzgesetz; BDSG) in order to provide our services within the framework of the contractual relationship.

2.3 Processing based on your consent

To the extent that you have given us your consent to the processing of personal data for specific purposes (e.g., circulation of data within a network/group, evaluation of payment transaction data for marketing purposes), the legality of this processing exists on the basis of your consent. Consent that has been granted can be revoked at any time.

Please note that the revocation will only take place with future effect. Any processing that took place before the revocation is not affected.

2.4 Data privacy rights

According to the GDPR, you have the right to information about your stored data free of charge (Art. 15 GDPR), the right to rectification (Art. 16 GDPR), the right to delete your data (Art. 17 GDPR), the right to limit processing (Art. 18 DS-GVO) and the right to data portability (Art. 20 GDPR).

Should you have any questions that this data privacy statement has been unable to answer, or if you would like information about the data stored about you, please contact us by e-mail at the address provided under the Contact section.

In addition, there is a right of appeal to a data protection authority (Art. 77 GDPR).

3. Data Collection, Storage and Use of Personal Data

3.1 Feedback and support requests

If you send us feedback or a support request, or use the support form on our website, your e-mail address will only be used for correspondence with you and only to resolve your support case. It is not disclosed to third parties.

As part of the support you have requested, it may happen that you transmit or have to transmit some of your personal data to us so that we can fulfill our contractual obligation. In these cases, your prior consent is not required in accordance with Art. 6 GDPR.

3.2 Licensing

When the list of orders is retrieved, the routing numbers used in the app are sent to us. The data is processed immediately in order to determine the possible licensing financial institutions and likewise to create/verify your app license. The data is not saved or transmitted to third parties. The stored data does not allow any conclusions to be drawn about specific users. The data is used to create anonymous usage statistics for our apps.

3.3 Setting up new EBICS bank accounts

When a new bank account is set up, the routing number that is entered in the app is sent to us. The data is processed immediately in order to obtain the corresponding EBICS access data such as the URL and host name of the banking system as well as the EBICS version used. The data is not saved or disclosed to third parties.

3.4 Setting up bank accounts from the corporate customer portal

When a bank account is set up from the corporate customer portal of the Sparkassen-Finanzgruppe, information about the user that is stored in the app settings (username, password and a routing number) is transmitted to the Finanz Informatik systems. The data is processed immediately in order to authorize and authenticate the user vis-á-vis the corporate customer portal and to retrieve order data.

3.5 Setting up connections to SFirm/StarMoney Business

In the app, it is possible to set up 1:1 connections between your SFirm/StarMoney Business installations and your mobile device (known as "linking"). This linking ensures that all encrypted data sent by SFirm/StarMoney Business can only be received and decrypted again by the correct receiving instance of Finanzcockpit 2. Even Star Finanz and its employees are unable to decrypt these data packets. After the linking and configuration of the desired accounts in SFirm/StarMoney Business, the data required for display in the app is provided by SFirm/StarMoney Business via a server-based service (data-exchange server) from Star Finanz, from which it is retrieved by the Finanzcockpit 2 app and then deleted from the server.

The data traffic between the SFirm/StarMoney Business installation and the Finanzcockpit 2 app is unidirectional and encrypted. It is based on the linking of these two clients and their configuration (set data and time periods for each Finanzcockpit 2 instance) in your installation of the 'SFirm' or 'StarMoney Business' electronic banking software.

3.6 Branding

The Sparkasse branding of the app includes the logo of your primary Sparkasse and your personal financial advisor. The branding is based on the routing number of the EBICS bank account or your primary savings bank in SFirm/StarMoney Business. The data is processed immediately in order to determine the possible financial institutions and to display the corresponding logo of the financial institution and the individual financial advisor. The data is not saved or disclosed to third parties. The stored data does not allow any conclusions to be drawn about specific users. The data is used to create anonymous usage statistics for our apps.

3.7 App launch and updating

Each time app is launched as well as each time the user initiates a manual update of the app, the following information that is stored in the app is sent to the Star Finanz data-exchange server:

- routing number,

- company name,
- username

This process involves some personal as well as some non-personal data.

3.8 Use of web views

The app offers various information in so-called "web views". These are web pages that are displayed within the app. This involves, for example, the licensing terms, data privacy statements and version history that can be viewed in the app. When using these pages, the data that are sent by the browser when visiting a website and that are required for using the page are automatically recorded. These are the web request, the user IP address, the browser type, the browser language, the date and time of the visit to the website. After usage ends, the data is only saved anonymously in order to improve the quality of the services.

4. Collection, Storage and Use of Non-personal Data

4.1 App launch and updating

See section 3.7.

4.2 Storage of data to improve app quality

We store anonymized information on the servers we use about which features are utilized by our users. Neither IP addresses, login information nor other data that would allow conclusions to be drawn about an individual are saved. This anonymized data is used to compile usage statistics. You can disable the transfer of this information in the app settings.

5. Permissions Requested by the App and Their Use

5.1 Camera & photos

Scanning QR codes to transfer EBICS bank access data, keys, accounts, transactions and balances from SFirm and/or StarMoney Business.

5.2 Mobile data

If there is no Wi-Fi connection, the app uses the mobile data connection, for example, when retrieving open orders, sending electronic signatures and/or when retrieving the most recent data from SFirm/StarMoney Business.

5.3 Push notifications

Push notifications for the Finanzcockpit 2 app can optionally be enabled by using the operating system manufacturer's push services. Delivery of push notifications to the user's device only takes place if the user has agreed to the sending of push notifications in general. If the user turns

off the push notifications again in the app settings, they will no longer receive any push notifications.

To be able to send push notifications to your device, it is necessary for the Finanzcockpit 2 app to send your device token—a unique, encrypted and anonymized device ID generated from your device ID—to Microsoft or the Finanz Informatik systems and the operating system manufacturer. It is not possible for Star Finanz, Finanz Informatik, the operating system manufacturer or Microsoft to draw conclusions about individual users.

5.4 Other applications

We use Microsoft Azure Notification Hubs as well as the Apple Push Notification Service (APNs) or Google Cloud Messaging to display push messages to users of the Finanzcockpit app.

We use the Matomo analysis software for so-called user tracking (Matomo is an open source solution hosted on Star Finanz servers). Anonymous information is collected in the app about which functions are used by the users. This information is transmitted to our servers and stored there. Neither IP addresses, account data nor other data that would allow conclusions to be drawn about a specific person are stored. The information stored in Matomo will not be passed on to third parties. Matomo is used on the basis of Art. 6 Para. 1 lit. f GDPR. As the operator of the Finanzcockpit app, we have a legitimate interest in the anonymous analysis of user behavior in order to further optimize the application for the benefit of our users. This anonymized data is used exclusively to generate usage statistics. The prerequisite for the transfer of usage data is that you have consented to the transfer. You can revoke your consent at any time in the app settings ("More > Settings > Help improve the app").

We use the error diagnosis service Microsoft Visual Studio App Center to be able to send us an anonymous crash/error report in the event of a crash or error, which supports us in error analysis and improvement of the app. There is neither tracking nor a transfer of personal data. The prerequisite for the transmission of crash/bug reports is that you have consented to the transmission. You can revoke your consent at any time in the app settings ("More > Settings > Help improve the app").

6. Data Security

6.1 Technological protective measures

6.1.1 Star Finanz servers

All of the servers we use are configured and installed in-house and operated in high-security data centers in Germany. The hardware used is supplied by certified well-known manufacturers and is failsafe and redundant. The servers are transported and installed in the data centers by our own employees, not by subcontractors, logistics companies or other third parties. As a matter of principle, we do not save any data on other servers, especially not abroad.

We ensure that all security technologies we use are technologically state-of-the-art and are constantly updated. Our security policies are continuously adapted and revised to reflect new findings in order to protect your data from theft and misuse. All of the data you transmit to us is handled responsibly and processed in accordance with all statutory data protection regulations, in particular the European General Data Protection Regulation (GDPR) and the German Federal

Data Protection Act (Bundesdatenschutzgesetz; BDSG), and in accordance with the highest security standards for data processing and storage.

6.1.2 Data transfer

Your data is transmitted exclusively via SSL-encrypted connections from your device to our servers operated in high-security data centers in Germany. The certificates are checked for validity and—where technologically possible on a given platform—the fingerprints of the certificate are also verified in order to prevent misuse and man-in-the-middle attacks to the greatest possible extent.

Transfer of data to third countries (i.e., countries outside the European Economic Area; EEA) only takes place if it is necessary/required by law to carry out your orders or if you have given us your consent. If required by law, we will inform you separately about details.

6.1.3 Data processing, duration of storage and deletion

Your data is processed and if necessary saved on servers that belong to Star Finanz-Software Entwicklung und Vertriebs GmbH in Germany and protected by us against access by third parties through comprehensive technological and organizational precautions.

If necessary, we process and store your personal data for the duration of our business relationship, which also includes, for example, the initiation and execution of a contract. Afterwards the data is deleted.

In addition, we are subject to various retention and documentation obligations, which result from the German Commercial Code (Handelsgesetzbuch; HGB) and the tax code (Abgabenordnung; AO), among other things. Their specified periods for storage and documentation are two to ten years.

Finally, the storage period is also subject to the statutory limitation periods, which, for example, can be up to thirty years according to §§ 195 et seqq. of the German Civil Code (Bürgerlichen Gesetzbuch; BGB), whereas the regular limitation period is three years. After the retention period has expired, the data is routinely deleted.

6.2 Organizational protective measures

Within Star Finanz, only internal employees who are involved in the execution and fulfillment of the respective information processes have access to data. Owing to encryption and anonymization, the data cannot be read or associated with specific users via different systems, even with physical access to those systems.

6.3 Use of third-party services

The respective third party's own data privacy policies apply to the use of third-party backup services, and we have no influence over their content or compliance.

6.4 No disclosure to third parties

Data is only passed on to third parties without your consent if we are legally obliged to do so, for example, if there is an applicable court order.

Updated: June 2023.
Version: 1.3