

Data Privacy Policy

Status: January 2023

We appreciate your interest in our products, our company and our handling of the information you have entrusted to us.

1. Contact

For questions related to data protection, please contact our data protection officer at:
Star Finanz-Software Entwicklung und Vertriebs GmbH, Data Protection Officer, Grüner Deich 15,
20097 Hamburg, Germany; fax +49 40 23728-350

E-mail: datenschutz@starfinanz.de

2. Data Privacy Policies

We assure you of the lawful and responsible handling of all data that you transmit to us as the user of our products and would like to provide you hereinafter with a transparent description of what data we process in detail, what we use it for, and whether and to what extent it is stored by us and/or transmitted to third parties.

2.1 Which sources and information we use

We process personal data only within the scope authorized by you personally. In doing so, we only collect and process the data that is absolutely necessary for the maintenance and use of the services provided to you. Prior to use and transmission of your data, all services that transmit personal information indicate the precise scope of the data and require your confirmation of transmission. All of your data belongs to you, therefore we do not pass along any of the data transmitted to us to third parties without your consent unless we are legally obliged to do so, such as when presented with a corresponding court order.

We understand personal data to include: name, address, telephone number, e-mail address, IP address and IBAN.

2.2 Rules for data processing for the fulfillment of 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 (BDSG) for the provision of our services within the framework of the contractual relationship.

2.3 Processing based on your consent

Insofar as you have given us your consent to the processing of personal data for specific purposes (e.g., transfer of data within the network/group, analysis of payment transaction data for marketing purposes), the legality of this processing is based on your consent. The consent you have given can be revoked at any time.

Please note that the revocation only works with future effect. Any processing that occurred before the revocation is not affected.

The following specifies in detail how we handle your personal data in the different program features:

2.3.1 Merge assistant

To merge financial institutions and make the associated change to the account number, SFirm provides an assistant to help you in changing the bank information. If you make use of this feature, we transfer your old account numbers along with the routing number of the issuing bank to our servers for the purpose of determining and returning the new account numbers. The data is neither stored nor disclosed to third parties.

We will only use the consent you have granted one time; you do not have to revoke it.

2.3.2 Pairing with the Finanzcockpit app

SFirm supports the transmission of selected financial data to a dedicated app on smartphones and tablets. The financial data is end-to-end encrypted and is not readable by us or by third parties. When setting up the end-to-end encryption (pairing) between the device and the SFirm installation, a unique pairing ID is generated and sent to our servers along with a unique ID for your SFirm installation in order to link it there with your SFirm license. The unique pairing ID will also be sent to our servers periodically when financial data is transmitted. We use these IDs to provide secure data transmission and to ensure compliance with the license terms (number of allowed pairings). The data can be viewed by the licensor (e.g., your financial institution). The data is not disclosed to third parties.

2.4 Processing for the fulfillment of contractual obligations

As part of any support you have requested, you may need to provide us with some of your personal information so that we can fulfill our contractual obligation. In these cases, prior consent from you in accordance with Article 6 of the GDPR is not required.

2.5 Processing on the basis of safeguarding the legitimate interests of the responsible party

To be able to ensure compliance with the terms and conditions of the license and to identify license misuse, we create a unique ID for each SFirm installation and transmit it along with your SFirm license key to our servers, where it is stored and processed to determine the number of installations per license. The ID is visible to the licensor (e.g., your financial institution). The data is not disclosed to third parties.

Prior consent from you in accordance with Article 6 of the GDPR is not required for this.

2.6 Data protection rights

Per the EU GDPR, you have the right to information about your stored data free of charge (Article 15 GDPR), the right of rectification (Art. 16 GDPR), the right to delete your data (Art. 17 GDPR), the right to restrict processing (Art. 18 GDPR), and the right to data portability (Art. 20 GDPR).

Should you have any questions that this data privacy policy has not been able to answer, or if you would like information about the data that is stored about you, please contact us by e-mail at the address provided under the Contact section.

In addition, you have the right of appeal to a data protection authority (Art. 77 GDPR).

3. Data Privacy by Default

The protection of personal and non-personal data that is processed in the software is a central component of the conception, development and quality assurance of our software products. Our software products are continually reviewed, improved and adapted to changing circumstances with regard to the availability, integrity and confidentiality of personal data and processing systems.

Star Finanz software products are designed to favor data privacy by default. This means, for example, that only those personal data required for the product to function are collected (per a policy of data minimization). Furthermore, access to the data is secured through password protection. The user has the ability to delete the data in the software.

4. Collection, storage and use of personal data

4.1 Use of webviews

In SFirm, various information may be displayed in so-called "webviews". These are HTML documents that are displayed using a web browser embedded in SFirm. This concerns on the one hand locally available or dynamically generated HTML documents such as the license terms displayed in SFirm or the SFirm start page, and on the other hand external websites that are displayed e.g. within the service center.

We use the external component "Microsoft Edge WebView2 Runtime" from Microsoft Corporation to display web views within SFirm. It is required for the correct functioning of SFirm.

When displaying HTML documents via WebView2, diagnostic data may be sent to Microsoft. You can find more information about this on the following Microsoft websites:

- Explanations about diagnostic data: <https://support.microsoft.com/de-de/windows/diagnose-feedback-und-datenschutz-in-windows-28808a2b-a31b-dd73-dcd3-4559a5199319>
- Microsoft's privacy policy, which describes how Microsoft handles personal data: <https://privacy.microsoft.com/de-de/privacystatement>

When using external websites using "Microsoft Edge WebView2 Runtime", data may also be recorded by the respective website (as is the case with every other website call). Which data is recorded and how it is stored lies solely in the sphere of influence of the website operator and cannot be influenced by SFirm.

5. Collection, storage and use of non-personal data

5.1 Collection of data to improve software quality

In SFirm, anonymized information is collected about which functions are used by users. This information is transmitted to our server and stored there once per session. Neither IP addresses, account details nor other data are stored that would allow conclusions to be drawn about a specific person.

We use the Matomo analysis software for this so-called tracking of the data. Matomo is an open source solution that is hosted on Star Finanz servers. 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 SFirm, we have a legitimate interest in the anonymized analysis of user behavior in order to further optimize the application for the benefit of our users. This anonymized data is used exclusively for the creation of usage statistics.

6. Data Security

If we process personal data you have transmitted to us, the following data security provisions apply.

6.1 Technical safeguards

6.1.1 Star Finanz Servers

All the server systems we use are operated in high-security datacenters in Germany. The hardware used is supplied by certified well-known manufacturers and is designed to be failsafe and redundant. Our employees are bound to secrecy. As a rule we do not store any data on other servers, especially not abroad.

We affirm that all security technologies we use are state-of-the-art and are continuously updated. Our security concepts are constantly being adapted to new findings and renewed to protect your data from theft and misuse. We handle all data that is transmitted to us responsibly and process said data according to all legal provisions on data protection, in particular the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG), and using the highest security standards for data processing and storage.

6.1.2 Data transfer

Your data is transferred exclusively via SSL-encrypted connections from your terminal device to our servers operated in high-security datacenters in Germany. During this process, the certificates are checked for validity and, if technically possible, the transmissions are also signed in order to prevent misuse and man-in-the-middle attacks to the greatest possible extent.

Data transfer to third countries (countries outside the European Economic Area, or EEA) only takes place if it is required for the execution of your orders or by law, or if you have given us your consent. Insofar as it required by law, we will inform you of details separately.

6.1.3 Data processing, length of storage and deletion

Your data is processed and stored on servers that belong to Star Finanz-Software Entwicklung und Vertriebs GmbH in Germany and protected by us through comprehensive technical and organizational safeguards against access by third parties.

Where necessary, we process and store your personal data for the duration of our business relationship, which includes, for example, the initiation and execution of a contract. The data is then deleted afterwards.

In addition, we are subject to various filing and documentation obligations, which result, inter alia, from the German Commercial Code (HGB) and the German Tax Code (AO). The periods stated therein for storage or documentation are two to ten years, respectively.

Finally, the storage period is also assessed according to the statutory limitation periods, which can be up to thirty years, for example, according to §§ 195 et seqq. of the German Civil Code (Bürgerliches Gesetzbuch, BGB), for which the regular period of limitation is three years.

After the storage period expires, the data is routinely deleted.

Additionally, the data is then promptly deleted when the purpose associated with processing no longer applies.

6.2 Organizational safeguards

Within Star Finanz, only internal employees who are involved in the execution and fulfillment of the respective information processes have access to data.

7. Changes to the Data Privacy Policy

Star Finanz reserves the right to change these guidelines at any time in accordance with data protection laws.