



Customer Information on Data Processing

1. General Information

With the following information we would like to inform you about the processing of your personal data by Solarisbank AG. Which data are processed in detail and how they are used depends largely on the services requested or agreed in each case.

Responsible for data processing is Solarisbank AG, Anna-Louisa-Karsch-Straße 2, 10178 Berlin. You can reach our data protection officer at this address or at privacy@solarisbank.de. If we process the data in joint responsibility with a cooperation partner, you can find the contact point in the cooperation partner's data protection information.

2. Information on Data Processing

We process personal data, which are necessary in the context of a contractual or pre-contractual business relationship for the provision of our service or for the initiation of a contract, on the basis of Art. 6 (1) lit. b GDPR. We, our cooperation partners or our service providers have received this information from you, for example when opening and maintaining an account or applying for a loan. In addition, to the extent necessary for the provision of our services or the preparation of an offer, we process personal data that we have received from third parties (e.g. Schufa), e.g. for the execution of orders, for the fulfilment of contracts or on the basis of a consent given by you. Furthermore, we process personal data which we have obtained and may process from publicly accessible sources (e.g. debtor registers, land registers, commercial and association registers, press, media, internet). The following personal data are regularly processed by us in the interested party process, at the opening of the master data or in the course of an authorization:

Name, address, contact data (telephone, e-mail address), birth date/place, gender, nationality, marital status, identification data (e.g. ID data), authentication data, tax ID, FATCA status, Schufa score.

In the context of the use of products/services from the product categories listed below, further personal data may be processed in addition to the above-mentioned

data.

- **Bank account (digital banking)**

Order data and transaction data (e.g. transfer orders), data from the fulfilment of our contractual obligations (e.g. account statements), data for the fulfilment of legal and regulatory obligations – in particular to prevent financial crime

- **Debit cards, Tokenized cards, Virtual cards, Pre-paid cards, Mobile Payment Systems** (e.g. Apple Pay, Google Pay, Samsung Pay)

Transaction data (currency, total, country, time, merchant, type of transaction, credit)

- **Financing**

Creditworthiness documents (income, expenses, external account statements), employer, type and duration of employment, pay slips, scoring/rating data

Insofar as this is necessary, Solarisbank AG processes your data beyond the actual fulfilment of the contract to safeguard legitimate interests in accordance with Art. 6 (1) lit. f GDPR. These include consulting and exchanging data with credit agencies to determine creditworthiness, default risks and to verify your stated address; asserting legal claims and defending against legal disputes; ensuring the bank's IT security; preventing criminal offences; measures to manage business and further develop services and products; and risk management in the bank.

If you have given us your consent to process personal data for specific purposes (e.g. passing on data to cooperation partners, account snapshot), your consent constitutes the legal basis for this processing. A given consent can be revoked at any time. Please note that the revocation will only take effect in the future.

As a bank, we are subject to various legal and regulatory obligations, i.e. statutory requirements (e.g. German Banking Act, Money Laundering Act, tax laws) and regulatory requirements (e.g. of the European Central Bank, the European Banking Supervisory Authority and the Federal Financial Supervisory Authority). We must also process your personal data in accordance with Art. 6 (1)



lit. c GDPR and Art. 6 (1) lit. e GDPR in order to fulfil these obligations and requirements. The purposes of processing include, among other things, creditworthiness checks, identity and age checks, fraud and money laundering prevention, the fulfilment of tax control and reporting obligations as well as the assessment and management of risks in the Bank.

In the context of our business relationship you must provide those personal data which are necessary for the establishment, execution and termination of a business relationship and the fulfilment of the associated contractual obligations or which we are legally obliged to collect. Without these data we will usually have to refuse the conclusion of the contract or the execution of the order or we will no longer be able to execute an existing contract and may have to terminate it.

3. Recipients of Data

Within the bank, those persons who need your data to fulfil our contractual and legal obligations have access to it. We will only transfer your data to third parties (e.g. to cooperation partners) if we are authorised to do so under data protection law (e.g. in accordance with the above-mentioned legal provisions). Your data may also be passed on by us to external service providers (e.g. IT service providers), who support us in data processing within the framework of order processing in accordance with strict instructions.

Under these conditions, recipients of personal data may be: public authorities and institutions (e.g. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Finanzbehörden, Bundeszentralamt für Steuern) in case of a legal or official obligation as well as other credit and financial service institutions, comparable institutions and contract processors to which we transfer personal data for the execution of the business relationship with you and cooperation partners with whom we cooperate in order to offer you digital banking products.

4. Data Transmission to Third Countries

We only transfer your data to countries outside the EU or

the EEA (so-called third countries) if this is necessary for the execution of your orders (e.g. payment and securities orders) or if there is a legal obligation (e.g. tax reporting obligations), you have given us your consent, in the context of commissioned data processing, or if the level of data protection is sufficient to protect your data. As an appropriate guarantee for the legality of data transmission, we have, among other things, safeguard in place, such as EU standard contract clauses in accordance with Art. 46 (2) lit. c GDPR or a Privacy Shield certification of the company receiving the data.

5. Storage Time

We store your personal data as long as it is necessary for the fulfilment of our contractual and legal obligations. If the data are no longer required for the fulfilment of these purposes, they are regularly deleted. This does not apply if the deletion conflicts with retention periods arising from laws and regulations: these include inter alia the Commercial Code, the Tax Code, the Banking Act, the Money Laundering Act and the Securities Trading Act. The periods for storage and documentation specified there range from two to ten years. In addition, we also store data to preserve evidence under the statute of limitations. According to §§ 195 ff. of the German Civil Code (BGB), these limitation periods can be up to 30 years, whereby the regular limitation period is three years.

6. Your Rights in Connection With Data Processing

You have the right to request information about what data about you is stored by us and for what purpose it is stored. In addition, you may have incorrect data corrected or data deleted that is inadmissible or no longer necessary to be stored. You have the right to data transferability. You also have the right to complain to a supervisory authority about the data processing taking place.

You have the right to object at any time to the processing of personal data concerning you on the basis of Art. 6 (1) lit. e GDPR and Art. 6 (1) lit. f GDPR for reasons arising from your particular situation; this also applies to profiling within the meaning of Art. 4 (4) GDPR.

If you object, we will no longer process your personal data, unless we can prove compelling reasons worthy of



protection for the processing, which outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

7. Automated Decision-Making and Profiling

In individual cases, we use automated decision making according to Art. 22 GDPR to bring about a decision on the establishment and implementation of the business relationship. Should this result in a negative legal consequence, we will inform you of the automated decision-making process and allow you to express your point of view separately and to obtain a decision by a qualified employee.

We process your data partially automatically with the aim of evaluating certain personal aspects (profiling). For example, we use profiling in the following cases: Due to legal and regulatory requirements, we are obliged to combat money laundering, terrorist financing and asset-polluting crimes. Data is also evaluated (for example, in payment transactions). These measures also serve to protect you. We use scoring and rating to assess your creditworthiness. The probability with which a customer will meet his payment obligations in accordance with the contract is calculated. The calculation can include, for example, income, expenses, existing liabilities, occupation, employer, length of employment, payment duration (e.g. account transactions, balances), experience from the previous business relationship, contractual repayment of earlier loans and information from credit bureaus. For corporate customers, additional data such as industry, annual results and financial circumstances are also included. Both scoring and rating are based on mathematically and statistically recognised and proven methods. The calculated score values and credit ratings support us in our decision-making and are included in our ongoing risk management.