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, Cuvrystraße 53, 10997 Berlin. You can reach our data protection officer at this address or at privacy@solarisgroup.com. 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. 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 portability. 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.

3. Digital Banking and Cards

3.1. 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. In addition, to the extent necessary for the provision of our services, we process personal data that we have received from third parties, 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 (for corporate accounts e.g.: debtor registers, land registers, commercial and association registers; all accounts e.g.: 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, contact data (address, telephone, e-mail address), birth date/place, gender, nationality, marital status, identification data (e.g. ID data), authentication data (e.g. signature), tax ID, FATCA status, employment status.

In addition, the following product specific data is processed:

For the **bank account**, 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.

For **Debit cards, Tokenized cards, Virtual cards, Prepaid cards, Credit cards and Mobile Payment Systems** (e.g. Apple Pay, Google Pay, Samsung Pay) transaction data (currency, total, country, time, merchant, type of transaction, credit) is processed.

Insofar as this is necessary, we, Solarisbank AG, process 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.

In case your identification before entering into a contractual relationship with us is carried out by means of a qualified electronic signature (“QES-Identification”), we will transmit personal data needed for the identification to SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden („SCHUFA“). The data exchange with SCHUFA shall also verify your own data input. Additional information regarding SCHUFA’s business may be found in the SCHUFA Information Sheet pursuant to Art. 14 GDPR or online at **www.schufa.de/datenschutz**.

In order to create a qualified electronic signature for QES-Identification, we transmit personal data to Swisscom IT Serivce S.E Mariahilfer Straße 123, 1060 Vienna, Austria (“Swisscom”).

When performing **QES-Identification**, you have to make a reference transaction to us from your bank account. In case of “QES-Identification” as **Identification method**, the IBAN of the account used for the reference transaction is processed. we transfer personal data to Tink Germany GmbH, Gottfried-Keller-Str. 33, 81245 Munich and to finleap connect GmbH, Hardenbergstr. 32, 10623 Berlin to facilitate the reference transaction.

If you have given us your consent to process personal data for specific purposes (e.g. passing on data to cooperation partners), 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, 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.

3.2. Fraud prevention and anti-money laundering checks

When you register via our cooperation partners' website or app and consent to the use of our fraud prevention tool and respective cookies via our cooperation partners' frontend, we will perform a risk assessment for fraud prevention and anti-money laundering purposes. For such purposes, we use SEON Technologies Kft., Rákóczi út 42. 7. em., Budapest 1072, Hungary ("**SEON**") as a service provider under a data processing agreement according to Art. 28 GDPR. For the processing activities described in this section, we have entered into a joint controllership agreement with each of our cooperation partners (Art. 26 GDPR). We will provide you with further information at any time upon request.

In order to perform the risk assessment, our cooperation partners collect and transfer to us the following browser data, device data, traffic data and location data from your device: IP address including type (e.g. commercial, mobile line, university) and whether it is listed as harmful, TOR value, VPN, proxy, number of accessories attached to your device, whether your phone is muted or not, device system's volume, country code and name of carrier (a) associated with the SIM card and (b) the device is currently using, device model type and unique identifier, system uptime, iCloud token, version and name of device given by the user in iOS settings, when the device last booted in UNIX time format and UTC time zone, country code and ID associated with device, cookie session ID, and browser details / settings including scrolling behaviour. We may add additional information and will then transfer such data to SEON along with your email address, name and phone number for performance of a risk analysis regarding potential fraudulent or other illicit activities.

SEON analyses this personal data based on a mathematically-statistically recognised and proven procedure and will provide us with a fraud risk score. As part of the analysis, SEON may perform email analysis, social media lookup or address profiling.

Based on the analysis and risk score, you will be able to complete your registration, be rejected as a customer, or may be guided through an extended registration process, with the aim to complete your onboarding process. The decision-making process is fully automated. You can contact us at privacy@solarisgroup.com (i) if you want to receive more information regarding the logic involved in the decision-making process and/or about the consequences of the execution of the automated decision-making process, (ii) if you need to receive additional explanations regarding the decision adopted following the above mentioned analysis, (iii) if you want to challenge the automated decision and/ or (iv) if you want to request a human review of this automated decision. Once you are onboarded, we will continue to collect the above data and perform additional risk analysis via SEON for ongoing fraud risk assessment.

The legal basis of the processing is your consent (Art. 25 TTDSG, Art. 6 (1) lit. a GDPR) and the implementation of necessary steps for entering into a contract requested by you (Art. 22 (2) lit. a GDPR). You cannot register to use our banking service without consenting, because the fraud prevention and anti-money laundering check is necessary for a secure provision of our services. As a licensed bank, we have a statutory obligation to fight money laundering by setting up a functioning risk management system and internal security measures as well as an ongoing screening of customers' activities (sections 4, 6 and 10 of the German Anti-Money-Laundering Act). You can withdraw your consent at any time by email to privacy@solarisgroup.com, but without consent you will not be able to continue using our services.

Your personal data will be stored until the purposes of processing these data as set forth above have been achieved, and be deleted within 12 months after performance of the risk assessment at the latest, unless statutory retention obligations apply (e.g. under anti-money laundering, commercial or tax law).

3.3. 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, German Federal Financial Supervisory Authority, European Banking Authority, European Central Bank, Tax Authorities, German Federal Central Tax Office) in case of a legal or official obligation as well

as other credit and financial service institutions, comparable institutions, collection agencies 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.

For the purpose of checking and verifying the address you have provided, we will transmit it to Deutsche Post Direkt GmbH, Junkersring 57, 53844 Troisdorf ("Deutsche Post"). If the address you have provided is not known to Deutsche Post or does not match the information you have provided, we will transmit the address you have provided to SCHUFA for checking and verification purposes.

For the identification purposes in order to check and verify the information provided by you, we transfer your personal data to one of the following identification service providers: (i) WebID Solutions GmbH, Friedrichstraße 88, 10117 Berlin, Germany (ii) IDnow GmbH, Auenstr. 100, 80469 Munich, Germany and (iii) Fourthline B.V., Keizersgracht 452, 1016 GD Amsterdam, the Netherlands.

Additionally, we transfer personal data to other obliged entities under the German Money Laundering Act, if this data processing is necessary for the fulfilment of their customer due diligence obligations.

3.4. 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, safeguards in place, such as EU standard contract clauses in accordance with Art. 46 (2) lit. c GDPR which you can obtain from us on request. In addition to the agreement of standard contract clauses, in the event of data transfer to a third country without an appropriate level of data protection we examine which further measures we can take to protect personal data, for example whether we can encrypt data or use pseudonyms.

3.5. 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.

In case of a QES-Identification in cooperation with Swisscom, the documentation of the qualified electronic certificate will be stored for 35 years, beginning with the time of creation of the qualified electronic certificate.

The main retention periods concern the documents relating to the opening of the account (5 years; the retention period begins at the end of the calendar year in which the business relationship ends) and the transaction data occurs (10 years; the retention period begins on the day on which the data is created).

3.6. 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 case: Due to legal and regulatory requirements, we are obliged to combat money laundering, terrorist financing and other criminal actions. Data is also evaluated (for example, in payment transactions). These measures also serve to protect you.

4. Financing

4.1. 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 when applying for a loan or a credit line. 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 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 application process, at the opening of the master data or in the course of an authorization:

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

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.

In addition, the following product specific data is processed:

For **Financing and Credit cards**, Creditworthiness documents (income, expenses, external account statements), employer, type and duration of employment, pay slips, scoring/rating data is processed.

Insofar as this is necessary, we process 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. Furthermore, we process personal data to credit brokers if they have a legitimate interest in doing so, e.g. if this data processing is necessary to validate bonuses or to adjust the risk assessment.

SCHUFA processes data and also uses such data for purposes of profile creation (Scoring) in order to provide its contractual partners domiciled in the European Economic Area and Switzerland as well third countries as applicable (to the extent an adequacy decision from the European Commission is available for such countries) information to be used to evaluate the creditworthiness of natural persons amongst other things. Additional information regarding SCHUFA's business may be found in the SCHUFA Information Sheet pursuant to Art. 14 GDPR or online at www.schufa.de/datenschutz.

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.

4.2. 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, collection agencies, identification service providers and contract processors to which we trans-fer personal data for the execution of the business relationship with you and cooperation partners with whom we cooperate in order to offer you financing products.

For the purpose of checking and verifying the address you have provided, we will transmit it to Deutsche Post. If the address you have provided is not known to Deutsche Post or does not match the information you have provided, we will transmit the address you have provided to SCHUFA for checking and verification purposes.

Additionally, we transfer personal data to other obliged entities under the German Money Laundering Act, if this data processing is necessary for the fulfilment of their customer due diligence obligations.

4.3. 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 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, safeguards in place, such as EU standard contract clauses in accordance with Art. 46 (2) lit. c GDPR which you can obtain from us on request. In addition to the agreement of standard contract clauses, in the event of data transfer to a third country without an appropriate level of data protection we examine which further measures we can take to protect personal data, for example whether we can encrypt data or use pseudonyms.

4.4. 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.

4.5. 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 other criminal actions. 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.