Conditions for Online Banking
Using the App or Browser-Based User Interfaces of the Partner of solarisBank

In addition to the General Terms & Conditions of the Bank, the following special conditions apply to the use of the online banking service made available by solarisBank AG (hereinafter: the "Bank") using the app or browser-based user interface of the partner of solarisBank (hereinafter the "User Interface").

1. Range of services

(1) The ~~account holder/depositor~~customer or its authorised representative may carry out banking transactions by means of online banking to the extent offered by the Bank. They may also access information from the Bank by means of online banking. Furthermore, pursuant to Section 675f paragraph 3 German Civil Code (*Bürgerliches Gesetzbuch*), they are entitled to use payment initiation services and account information services pursuant to Section 1 paragraphs 33 and 34 German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*). In addition, they may use other third-party services selected by them.~~Additionally, they are authorised to use a payment initiation service provider according to Section 1 para. 33 German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*) to initiate payments.~~

(2) ~~Account holders/depositors~~ Clients and authorised representatives shall be referred to uniformly as "Participants", accounts and deposits uniformly as "Account", unless explicitly stated otherwise.

(3) The transaction limits agreed separately with the Bank apply to the use of the online banking.

2. Requirements for the use of online banking

(1) The Participant can use online banking if the bank has authenticated him or her.

(2) Authentication is the procedure agreed separately with the Bank whereby the Bank can verify the identity of the Participant or the authorised use of an agreed payment instrument, including the use of the personalised security feature of the Participant. Using the authentication elements agreed for this purpose, the Participant may identify himself or herself to the Bank as an authorised Participant, access information (see number 3 of these Conditions) and place orders (see number 4 of these Terms and Conditions).

(3) Authentication elements are

- knowledge elements, i.e. something that only the Participant knows (e.g. personal identification number (PIN)),
- possession elements, i.e. something that only the Participant has (e.g. device for generating or receiving one-time transaction numbers (TANs) that prove the subscriber's ownership, such as the girocard with TAN generator or the mobile terminal), or
- being elements, i.e. something that the Participant is (inherence, e.g. fingerprint as a biometric feature of the Participant).

(4) The Bank authenticates the Participant based on him or her transmitting the knowledge element, proof of the possession element and/or proof of the existence element to the Bank in accordance with the Bank's request.

~~The Participant requires the personalised security features and authentication instruments agreed with the Bank for using the online banking in order to confirm his identity to the bank as an authorised participant (see 3) and authorise orders (see 4). Instead of a personalised security feature, a biometric feature of the Participant can be agreed upon for the authentication or authorisation.~~

~~**2.1 Personalised security features**~~

~~Personalised security features are features, that are provided to the Participant by the Bank for authentication. The personalised security features, which may also be alphanumerical, are for example:~~

- ~~the personal identification number (PIN),~~
- ~~transaction numbers (TANs) that can be used once.~~

~~**2.2 Authentication instruments**~~

~~Authentication instruments are personalised features or procedures that the Participant and the Bank agreed upon and are used by the Participant for placing online banking orders. The personalised security feature can be provided to the Participant by the following authentication instruments:~~

- ~~online banking app for the reception or generation of TANs on a mobile end device (e.g. mobile phone)~~
- ~~iOS or Android application using so-called device binding~~
- ~~mobile end device (a mobile phone, for example) to receive TANs by text message (mobile TAN),~~
- ~~chip card with signature function~~
- ~~another authentication instrument on which there are signature keys.~~

~~For a chip card, the Participant also requires an appropriate card reader.~~

~~The Bank may extend or restrict the list of permitted authentication instruments and shall notify the Participant of this at least two months before the exclusion of existing authentication instruments from the list or inclusion of new instruments on the list.~~

3. Access to online banking

The Participant shall have access to online banking when

- he/she enters his individual customer ID (e.g. account number, login name) and
- he/she identifies himself/herself using the authentication element(s) requested by the Bank, and
- the access is not blocked (see numbers 8.1 and 9 of these Terms and Conditions).

Once access to online banking has been granted, information may be accessed or orders may be placed in accordance with number

4 of these Terms and Conditions.

~~–~~ (2) For access to sensitive payment data within the meaning of Section 1 paragraph 26 sentence 1 German Payment Services Supervision Act (e.g. for the purpose of changing the customer's address), the Bank requests the participant to identify himself/herself by using an additional authentication element if only one authentication element was requested for access to online banking. The name of the account holder and the account number do not qualify as sensitive payment data for payment initiation services and account information services used by the participant (Section 1 paragraph 26 sentence 2 German Payment Services Supervision Act).~~he has provided his account number or individual customer ID and his PIN or electronic signature,~~

~~– verification of this data by the Bank has resulted in authorisation of access for the Participant and~~

~~– there is no block on access (see 8.1 and 9).~~

~~Once access has been given to online banking, the Participant is able to call up information and place orders. The sentences 1 and 2 are also applicable when the Participant initiates payment orders by a payment initiation service provider and requests information via an account information service provider (see No. 1 para. 1 sentence 3).~~

4. ~~Online banking o~~Orders

4.1 Placing orders~~ and authorisation~~

The Participant must agree to an order (e.g. bank transfer) for its effectiveness (authorisation). On request, the Participant must use authentication elements (e.g. entering a TAN as proof of ownership).

The Bank confirms receipt of the order via online banking.~~In order to take effect, online banking orders (transfers, for example) shall be placed by the Participant authorised with the personalised security feature provided by the Bank (e.g. TAN) or the agreed biometric security feature and communicated to the Bank by online banking. The Bank shall confirm receipt of the order by online banking. The sentences 1 and 2 are also applicable when the Participant initiates payment orders by a payment initiation service provider and requests information via an account information service provider (see No. 1 para. 1 sentence 3).~~

4.2 Cancellation of orders

The extent to which an online banking order may be cancelled is governed by the special conditions that apply to the respective order type (conditions for transfers, for example). Instructions may only be cancelled outside online banking unless the Bank has expressly provided a cancellation option in its online banking.

5. Processing of ~~online banking~~ orders by the Bank

(1) ~~Online banking o~~Orders are processed on the business days specified for processing the type of order in question (a transfer, for example) on the online banking page of the Bank or in the Schedule of Prices and Services, in the course of normal workflow. If the order is received after the time specified on the online banking page of the Bank or in the "Schedule of Prices and Services" (acceptance period) or if the time of receipt does not fall on a bank working day as defined by the "Schedule of Prices and Services" of the Bank, the order is deemed to have been received on the following bank working day. Processing shall begin only on that day.

(2) The Bank shall carry out the order if the following completion conditions are met:

- The Participant has authorised the order (cf. number 4.1 of these Terms and Conditions).
- The Participant is authorised to carry out the transaction type concerned (a securities transaction, for example).
- The online banking data format is observed.
- The online banking transaction limit agreed separately is not exceeded.
- The additional requirements for completion of the respective order type are in place in accordance with the relevant special conditions (sufficient funds in the account for the transfer, for example).

If the completion conditions specified in sentence 1 are in place, the Bank shall complete the ~~online banking~~ orders in accordance with the provisions of the special conditions that apply to the respective order type (conditions for the transfer, for example, or conditions for the security transaction).

(3) If the completion conditions specified in paragraph 2 sentence 1 ~~Clauses 1-5~~ are not in place, the Bank shall not complete the ~~online banking~~ order. The Bank shall notify the Participant via online banking and thereby, as far as possible, explain the reasons for this and the ways in which errors that have led to the order being declined can be corrected via online banking. This does not apply when giving reasons violates other provisions o~~i~~f law.

6. Information provided to the ~~account holder~~ customer about online banking transactions

The Bank shall notify the ~~account holder~~ customer at least once a month of the transactions completed by online banking by the method agreed for providing account information.

7. Duty of care of the Participant

7.1 ~~Technical connection to online banking~~Protection of authentication elements

~~The Participant is obliged to establish the connection to online banking only via the online banking access channels communicated separately by the Bank (internet address, for example). For initiating a payment order or receive account information, the Participant may establish the technical connection via to the online banking via a payment initiation service provider or an account information service provider (see No. 1 para. 1 sentence 3).~~

~~7.2 Confidentiality of the personalised security features and safekeeping of the authentication instruments~~

(1) The Participant shall take all reasonable precautions to protect his/her authentication elements (see number 2 of these Terms and Conditions) against unauthorised access. Otherwise, there is a risk that online banking may be misused or used in any other unauthorised manner (cf. numbers 3 and 4 of these Terms and Conditions).

(2) In order to protect the individual authentication elements, the Participant shall pay particular attention to the following:

(a) Knowledge elements, such as the PIN, shall be kept secret; in particular, they may

- not be communicated orally (e.g. by telephone or in person),
- not be passed on outside online banking in text form (e.g. by e-mail, messenger service),
- not be stored unsecured electronically (e.g. storage of the PIN in plain text on computer or mobile device) and
- not be recorded on a device or stored as a transcript together with a device that serves as a possession element (e.g. girocard with TAN generator, mobile terminal, signature card) or for checking the being element (e.g. mobile terminal with application for online banking and fingerprint sensor).

(b) Possession elements such as the girocard with TAN generator or a mobile terminal must be protected against misuse, in particular

- the girocard with TAN generator or the signature card must be kept safe from unauthorized access by other persons,
- it must be ensured that unauthorized persons cannot access the Participant's mobile terminal (e.g. mobile phone),
- it must be ensured that other persons cannot use the application on the mobile device (e.g. mobile phone) for online banking (e.g. online banking app, authentication app),
- the application for online banking (e.g. online banking app, authentication app) on the Participant's mobile terminal must be deactivated before the participant gives up possession of this mobile terminal (e.g. by selling or disposing of the mobile phone),
- the evidence of the ownership element (e.g. TAN) may not be passed on orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service) outside the online banking, and
- the participant who has received a code from the bank to activate the possession element (e.g. mobile phone with application for online banking) must keep it safe from unauthorized access by other persons; otherwise there is a risk that other persons will activate their device as the possession element for the participant's online banking.

(c) Being elements, such as the Participant's fingerprint, may only be used as an authentication element for online banking on a Participant's mobile terminal if no other person's being elements are stored on the mobile terminal. If the mobile terminal used for online banking stores the being elements of other persons, the knowledge element issued by the bank (e.g. PIN) must be used for online banking and not the being element stored on the mobile terminal.

(3) The telephone number stored for the mobile TAN procedure shall be deleted or changed if the subscriber no longer uses this telephone number for online banking.

(4) Notwithstanding the protection obligations under paragraphs 1 to 4, the Participant may use its authentication elements vis-à-vis a payment initiation service and an account information service of its choice as well as any other third-party service (see number 1 paragraph 1 sentences 3 and 4 of these Terms and Conditions). Other third-party services shall be selected by the Participant with due care.~~(1) The Participant shall~~

- ~~keep his personalised security features confidential (see 2.1) and protect them from unauthorised access and communicate them to the Bank only via the online banking access channels provided separately by it and~~
- ~~keep his authentication instrument (see 2.2) safe from access by other persons (safekeeping obligations).~~

~~The Participant shall take all reasonable measures to fulfil the safekeeping obligations. Any other person who is in possession of the authentication instrument may misuse the online banking process in conjunction with the knowledge of the associated personalised security feature. This may entail liability of the account holder/depositor in accordance with 10.2. The confidentiality obligation regarding the personalised security features according to sentence 1 does not apply, if the Participant transmitted the data to a payment initiation service provider or an account information service provider for initiating a payment order or receiving account information (see No. 1 para. 1 sentence 3).~~

~~(2) In particular, the following shall be observed to protect the personalised security features and authentication instrument:~~

- ~~The personalised security feature must not be saved unsecured electronically.~~
- ~~When entering the personalised security feature, it must be ensured that other persons cannot observe this.~~
- ~~The personalised security feature must not be communicated by e-mail.~~
- ~~The personalised security feature (e.g. PIN) may not be stored together with the authentication instrument.~~
- ~~The Participant may not use more than one TAN to authorise an order or to lift a block.~~

~~With the mobile TAN process, the device on which the TAN is received (a mobile phone, for example) may not be used simultaneously for online banking.~~

7.~~2~~3 Security notice

The Participant shall observe the security instructions on the Bank's internet site for online banking, in particular the measures to protect the hardware and software used (customer system).

7.~~3~~4 Check of order data against data displayed by the Bank

The Bank shall display to the participant the order data received by it (e.g. amount, account number of the payee, securities identification number) via the participant's separately agreed device (e.g. mobile terminal, chip card reader with display). The Participant is obliged, prior to confirmation, to verify whether the displayed data matches the data specified for the order.~~Insofar as the Bank displays to the Participant data relating to his online banking order (amount, account number of the payee, security ID number) in the customer system or on another device belonging to the Participant (a mobile phone, for example, or a chip card reader with display) for confirmation, the Participant is obliged to check that the data displayed corresponds to the data intended for the transaction as confirmation.~~

8. Information and notification obligations

8.1 Blocking notification

(1) If the Participant becomes aware of

- the loss or theft of ~~the~~ an authentication ~~instrument~~element,
- misuse or other unauthorised use of one of his/her authentication ~~instrument~~ elements or
- of one of his personal security features,

the Participant must notify the Bank of this without delay (blocking notification).

The Participant may submit a blocking notification to the Bank at any time ~~, including~~ also via the contact information provided separately.

(2) The Participant ~~shall~~ must report any theft or misuse of an authentication element to the police immediately.

(3) If the participant suspects unauthorized or fraudulent use of any of his or her authentication elements, he or she must also submit a blocking notice.~~If the Participant suspects that another person has~~

~~gained possession of his authentication instrument or knowledge of his personalised security feature or~~

~~made use of the authentication instrument or personalised security feature without authorisation,~~

~~he must also submit a blocking notification.~~

8.2 Notification of unauthorised or incorrect orders

The ~~account holder/depositor~~customer shall notify the Bank of any unauthorised or incorrect orders as soon as they are detected.

9. Blocking use

9.1 ~~9.1~~ Block at the instigation of the Participant

At the ~~instigation~~ request of the Participant, in particular in the event of a blocking notification as per number 8.1, the Bank shall impose
a block ~~on access to online banking for him or~~

~~for all Participants or~~

- on access to online banking for him/her or all Participants or ~~of for~~ his/her authentication ~~instrument~~elements for the use of online banking, ~~in~~
- ~~particular in the event of a blocking notification as per 8.1.~~
-

9.2 Block at the instigation of the Bank

(1) The Bank may block access to online banking for a Participant if

- it is entitled to terminate the online banking contract for good cause,
- material grounds relating to the security of the authentication ~~instrument or the personalised security feature~~ elements justify it or
- there is a suspicion of unauthorised or fraudulent use of one of the authentication ~~instrument~~elements.

(2) The Bank shall notify the ~~account holder/depositor~~customer of the block, specifying the relevant reasons, if possible before the block, but at the latest immediately after the block. Reasons may not be given if the Bank would thereby violate statutory obligations.

9.3 Lifting a block

The Bank shall lift a block or replace the relevant ~~personalised security feature or~~ authentication ~~instrument~~ elements if the reasons for the block no longer obtain. It shall notify the ~~account holder/depositor~~customer of this immediately.

9.4 Automatic block on a chip-based ~~authentication instrument~~possession element

(1) The chip card with signature function is blocked automatically if the code for using the electronic signature is entered incorrectly three times in succession.

(2) A TAN generator as part of a chip card that requires the entry of its own usage code blocks itself if it is entered incorrectly three times in a row.

~~(2) The authentication instrument specified in paragraph 1 can then no longer be used for online banking. The Participant may contact the Bank to restore access to online banking.~~

(3) The possession elements referred to in paragraphs 1 and 2 may then no longer be used for online banking. The Participant may contact the Bank in order to restore the use of online banking.

9.5 Access block for payment initiation service and account information service

The Bank may refuse account information service providers or payment initiation service providers access to a payment account of the customer if objective and duly substantiated reasons in connection with unauthorized or fraudulent access of the account information service provider or the payment initiation service provider to the payment account, including unauthorised or fraudulent initiation of a payment transaction, justify such refusal. The Bank shall inform the customer of such a refusal of access by the agreed means. The information shall if possible be provided before, but at the latest immediately after, the refusal of access. Reasons may not be given if the Bank would thereby violate statutory obligations. As soon as the reasons for refusing access no longer exist, the Bank shall lift the access block. It shall inform the customer thereof without delay.

10. Liability

10.1 Liability of the Bank in the event ~~for~~ of the execution of an unauthorised order ~~online banking transaction~~ and for an ~~online banking transaction~~ order that is not completed, completed incorrectly or delayed

The liability of the Bank for an unauthorised ~~online banking transaction~~ order and for an ~~online banking transaction~~ order that is not completed, completed incorrectly or delayed is governed by the special conditions agreed for the respective order

type (conditions for transfers, for example, or conditions for securities).

10.2 Liability of the ~~account holder/depositor~~customer in the event of misuse of ~~this/her~~he ~~personalised security feature or an~~ authentication ~~instrument~~elements

10.2.1 Liability of the ~~account holder~~ customer for unauthorised payment transactions before the blocking notification

(1) If unauthorised payment transactions completed before the blocking notification results from the use of a misplaced, stolen or otherwise lost authentication ~~instrument~~ elements or any other misuse of ~~the~~ an authentication ~~instrument~~element, the ~~account holder~~ customer shall be liable for the losses incurred by the Bank as a result up to an amount of EUR 150.00, irrespective of whether the ~~cardholder~~ Participant is culpable.

(2) The ~~account holder~~customer is not liable for losses according to paragraph 1 if

- impossible for him to notice the misplacement, theft or other loss or any other misuse of the authentication ~~instrument~~element, or
- the misplacement of the authentication ~~instrument~~ element was caused by an employee, agent, branch of a payment service provider or any other party that services were outsourced to.

(3) If unauthorised payment transactions are completed before the blocking notification and the Participant has acted fraudulently or intentionally breached his duties of notification and care or has done so as a result of gross negligence, the ~~account holder~~ customer shall bear the losses incurred as a result in full. The participant may be guilty of gross negligence, in particular, if he/she has failed to comply with one of his duties of due diligence in accordance with

- number 7.1 paragraph 2,
- number 7.1 paragraph 4,
- number 7.3 or
- number 8.1 paragraph 1

of these Terms and Conditions.~~Gross negligence on the part of the Participant exists, in particular, if he~~

~~fails to notify the Bank as soon as he becomes aware of the loss or theft of the authentication instrument or the misuse of the authentication instrument or the personalised security feature (see 8.1 paragraph 1),~~

~~has saved the personalised security feature to the customer system (see 7.2 paragraph 2, 1st bullet point),~~

~~has communicated the personalised security feature to another person and the misuse was caused as a result (see 7.2 paragraph 1, 2nd bullet point),~~

~~has entered the personalised security feature so that it can be seen elsewhere than on the specifically agreed internet pages (see 7.2 paragraph 2, 3rd bullet point),~~

~~has communicated the personalised security feature outside the online banking process, by e-mail for example (see 7.2 paragraph 2, 4th bullet point),~~

~~has noted the personalised security feature on the authentication instrument or kept them together (see 7.2 paragraph 2, 5th bullet point),~~

~~has used more than one TAN to authorise an order (see 7.2 paragraph 2, 6th bullet point),~~

~~has used the device with which he receives the TAN during the mobile TAN process (mobile phone, for example) for online banking at the same time (see 7.2 paragraph 2, 7th bullet point).~~

(4) Notwithstanding paragraphs 1 and 3, the ~~account holder~~ customer is not liable for losses if the Bank did not request a strong customer authentication according to Section 1 paragraph~~.~~ 24 of the German Payment Services Supervision Act ~~(*Zahlungsdiensteaufsichtsgesetz*) although the Bank was obliged to demand strong customer authentication according to Section 68 para. 4 of the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*)~~. A strong customer authentication requires in particular the use of two elements independent of each other from the categories knowledge ~~(something the Participant knows, e.g. PIN)~~, possession ~~(something the Participant possesses, e.g. TAN generator),~~ or inherence (~~something the Participant is, e.g. fingerprint~~cf. number 2 paragraph 3 of these Terms & Conditions).

(5) Liability for losses incurred within the period to which the transaction limit applies is restricted to the agreed transaction limit.

(6) The ~~account holder~~ customer is not liable for losses according to paragraphs 1 and 3 if the Participant could not issue its blocking notification because the Bank failed to ensure a way to receive the blocking notification.

(7) Paragraphs 2 and 4 to 6 do not apply if the Participant acted fraudulently.

(8) If the customer is not a consumer, the following shall apply additionally:

The customer is liable for damages due to unauthorized payment transactions beyond the liability limit of EUR 50 according to paragraphs 1 and 3 if the Participant has negligently or intentionally violated his notification and due diligence obligations under these Terms and Conditions.

The limitation of liability in the first indent of paragraph 2 shall not apply.

10.2.2 Liability of the ~~deposit holder~~ customer for unauthorised ~~security~~ transactions ~~before~~ outside ~~the blocking notification~~payment services (e.g. securities transactions) before the blocking notification

If unauthorised ~~security~~ transactions outside payment services (e.g. securities transactions) before the blocking notification ~~before the blocking notification~~ result from the use of a lost or stolen authentication ~~instrument~~ element or from any other misuse of the ~~personalised security feature or~~ authentication element ~~instrument~~ and if the Bank incurs a loss as a result, the ~~depositor~~

customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

10.2.3 Liability of the Bank after the blocking notification

As soon as the Bank receives a blocking notification from a Participant, it shall assume responsibility for all losses incurred as a result of unauthorised online banking transactions. This does not apply if the Participant has acted with fraudulent intent.

10.2.4 Exclusion of liability

Claims for liability are excluded if the circumstances on which the claim is based are the result of an unusual and unforeseeable event that the party that cites the event has no influence over, and the consequences of which could not have been avoided by it despite exercising due care.

11. Explanations from the Bank and account statements

(1) In the course of the business relationship between the Bank and the customer, the user interface is the customer's agreed receiving device. Notifications and explanations from the Bank are made available to the customer via the user interface in electronic form, provided that written form has not been expressly agreed with the customer or is a statutory requirement.

(2) Notifications and explanations regarding the business relationship with the Bank shall be provided to the customer by the Bank in encrypted form via the user interface. Notifications and explanations provided via the user interface shall only be sent by post as well if this is a statutory requirement.

Irrespective of the use of the user interface as an electronic means of communication by the customer, the Bank is entitled to send individual notifications and explanations or, in the event of technical problems, all notifications and explanations by post or in another form to the customer, if it considers this to be expedient in consideration of the customer's interests.

The Bank shall notify the customer of the availability of certain documents via the user interface itself or via the partner of the bank by e-mail, text message or another means agreed with the customer.

(3) The customer is obliged to open notifications and explanations via the user interface regularly and promptly and to check their contents as soon as the bank has informed him of the availability of such notifications and explanations. The Bank shall be notified of any inaccuracies immediately, at the latest six weeks from their availability.

(4) All notifications and explanations communicated to the customer via the user interface are deemed to have been received when the Bank informs the customer that they are available and can be accessed via the user interface. The Bank and customer agree accordingly that the user interface shall be the device used by the customer to receive all notifications and explanations from the Bank, in particular account statements and final accounts.

(5) The Bank shall ensure that the data on the user interface cannot be altered. This obligation does not apply if the data is stored or kept outside the user interface. As a result of the specific hardware and software settings, the appearance of a printout will not always match the presentation on the screen.

(6) The Bank shall permanently save all of the documents provided by it via the user interface during the ongoing business relationship. When the business relationship comes to an end, the customer may demand copies of the account statements and final accounts from the bank in return for payment of a fee that the Bank may set at its discretion (Section 315 ~~of the German~~ German Civil Code ~~(*Bürgerliches Gesetzbuch*)~~).

(7) The information obligations resulting from Sections 675d paragraph~~.~~ 1 clause 1 ~~of the~~ German Civil Code ~~(*Bürgerliches Gesetzbuch*)~~in conjunction with Article~~.~~ 248 paragraphs~~.~~ 3-9 of the Introductory Act to the German Civil Code (*Einführungsgesetz zum Bürgerlichen Gesetzbuch*) and Section 312i paragraph ~~(~~1~~)~~ sentence 1 nos. 1 – 3 and sentence 2 German Civil Code ~~(*Bürgerliches Gesetzbuch*)~~ are waived if the customer is not a consumer as defined by Section 13 ~~of the~~ German Civil Code ~~(*Bürgerliches Gesetzbuch*)~~.