Basler Kantonalbank

Basic documents BKB

501 009 8.21

Basler Kantonalbank

Table of contents

501009 8.21

Basler Kantonalbank

Terms and Conditions

Version 2020

These conditions serve to govern clearly the relationship between the Client and the Bank. Special agreements remain reserved. Certain categories of business are subject to the Bank's special regulations as well as to established rules of banking practice.

For ease of comprehension, the masculine form is used throughout these conditions; these references are intended to include also female Clients of the Bank.

In case of differences between the German and English version of this document the German version shall prevail.

1. Power of disposition

Instructions pertaining to authorized signatures communicated to the Bank shall be valid until explicit communication of change and regardless of any other entries in the Commercial Register or public announcements. Accounts or custody accounts for which multiple persons are authorized can be used only by the authorized persons jointly.

2. Verification of authorization and due-diligence obligations

The Bank will exercise the verification of authorization with the customary due diligence.

Losses or other disadvantages resulting from the failure to recognize inadequate proof of identify, especially such arising from signature and document forgeries or the manipulation of electronic transmissions, shall be borne by the Client, provided that the Bank has exercised the verification of authorization with the customary due diligence.

In particular, the Bank is not obligated to compare information and instructions transmitted to the Bank by the Client or an agent to other information and instructions from the Client.

The Client is obligated to store his banking documentation securely so that unauthorized persons cannot access the information contained therein. If he issues instructions, the Client will take all safety precautions that reduce the risk of fraud. He will keep electronic means of authentication (incl. passwords and codes) secret, store them separately from each other, and follow any safety recommendations from the Bank regarding electronic services/products in order to prevent misuse. If the Client determines any irregularities, he will notify the Bank immediately. The Client will be responsible for any losses resulting from a breach of these due-diligence obligations.

The Bank will take reasonable measures to detect and prevent fraud. If it infringes the customary due diligence in doing so, it will assume the damage incurred.

If any losses or other disadvantages are incurred without the Bank or the Client having infringed their due diligence, then the party into whose area of influence the action causing the damage was placed shall be responsible. The Bank is not responsible for any losses or other disadvantages arising from errors in transmission, technical disruptions, and illegal intervention in the Client's hardware/software.

The Bank is authorized at any time in the course of interaction with the Client and his authorized agents to take measures for verification of authorization. The Client will be responsible for damages resulting from any delays caused by such measures.

3. Insufficient capacity to act

The Client will notify the Bank immediately in writing in case of insufficient capacity to act on the part of his authorized agents or other third parties acting on his behalf. If he fails to do so, or if the incapacity to act is on the part of the Client himself, he will be responsible for the damage resulting from insufficient capacity to act, provided that the Bank, its employees, or agents have not infringed the customary due diligence.

4. Communication from the Bank and errors in transmission

The Bank is authorized to communicate by postal service, telephone, electronic channels (e.g., email, fax, text message, online banking, mobile apps, and other electronic communications channels), as well as other transmission and transport means, to the contact data used in connection with the Bank or provided explicitly to the Bank by the Client or his authorized agents.

The Client is obligated to keep the Bank informed of updates to the information provided regarding himself or his authorized agents, such as name, address, place of residence, email address, phone number, etc.

600 9676 1.20

Communications from the Bank shall be deemed to have been delivered in a legally effective manner if sent in accordance with the latest contact data provided by the Client or otherwise deposited according to the instruction from the Client.

The date on the copies or mailing lists held in physical or electronic format by the Bank shall be considered the mailing date.

The Bank may make legally relevant information, conditions, and documents available to the Clients, as well as meet its obligations of information, disclosure, and publication (e.g., contained in financial market regulations governing investor protection and transparency), by means of publication on the Internet (at www.bkb.ch).

The Bank will exercise the customary due diligence in the use of postal services, telephone, electronic or other means of forwarding or transport. It shall be responsible for any damage specifically from loss, delays, irregularities, duplication, or technical disruptions and business interruptions, if it has infringed the customary due diligence. If the Bank has exercised the customary due diligence, then the Client shall be responsible for these damages.

5. Complaints

Complaints from a Client relating to the execution, non-execution, or incorrect execution of orders or objections to communications must be lodged immediately, and no later than the deadline specified by the Bank.

If documents or communications that the Client expects (e.g. account or custody account statements, trading statements) are not received, the Client must notify the Bank immediately.

Account and custody account statements must be contested within one month after being sent by the Bank.

If no complaints are duly lodged, the execution or non-execution and the relevant communications and statements shall be deemed to have been approved.

In any case the Client is responsible for any damage arising from a delay in the lodging of a complaint.

6. Execution of orders

If the Client issues one or multiple orders that exceed his available balance or the loan granted to him, the Bank may determine at its own discretion, without regard to the date or time of receipt, which instructions should be executed in part or in full.

If damage is incurred as a result of non-execution, insufficient or late execution of orders (excluding stock market orders), the Bank shall be liable only for the loss of interest.

In cases involving the risk of more extensive damage, the Client must draw the Bank's attention to this risk in advance; otherwise he shall be responsible for the damage.

7. Right of lien and offset

The Bank has a right of lien on all the Client's assets and on all assets it holds for the Client's account, either at its own premises or elsewhere, and a right of offset relating to all receivables for all existing or future claims, irrespective of the due date or currency or whether these claims are specifically secured.

This right of lien and offset applies also for any indemnification or exemption claims of the Bank, particularly if they are asserted in connection with transactions executed for the Client or assets held for the Client by third parties (including issuers, liquidators, trustees, receivers, institutions, and authorities).

If the Client is in arrears with his obligations, the Bank may, at its discretion, including in terms of the sequence, liquidate the pledged items either by enforcement or freely, or to initiate proceedings against the Client for distraint or bankruptcy, in accordance with the right of lien.

8. Conditions, taxes, and charges

Agreed or customary conditions (interest, fees [including balance fees], commissions, and charges) and taxes will be charged to the Client promptly, monthly, quarterly, semiannually or annually, at the discretion of the Bank. If multiple persons are named on the account, these shall bear liability jointly and severally.

The current conditions and other charges are based on available fee schedules and product data sheets. Changes are possible at any time, specifically in case of changes in money market conditions or the costs and reevaluation of business risks, through adjustment of the fee schedules and product data sheets. The Client will be advised of the changes in advance by appropriate means.

Changes or new conditions shall be deemed to have been approved if the Client does not terminate the affected product or the affected service within 30 days from communication. Notice or withdrawal periods according to separate conditions or agreements shall remain in effect.

600 9676 1.20

For services not included in a fee schedule or product data sheet that are performed by the Bank on the Client's instructions or are presumed to be in the Client's interest and are normally expected to be rendered for payment only the Bank may determine the amount of said remuneration at its own discretion.

Any taxes and charges that are imposed at or by the Bank in connection with the Client's relationship to the Bank or that the Bank must collect due to Swiss or foreign law, international agreements, or contractual agreements with foreign entities (e.g. 30 % withholding tax in accordance with the U.S. Foreign Account Tax Compliance Act, or FATCA), as well as charges incurred at the Bank, shall be charged or can be passed on to the Client.

9. Foreign currencies

Bank assets that correspond to the Client's foreign currency assets shall be invested in the same currency either in or outside the country of the currency in question in the name of the Bank but at the expense and risk of the Client. The Client shall bear the proportionate share equivalent to his balance of the risk affecting the total investment, particularly from statutory or official restrictions and taxes and other charges in all affected countries.

The Client may freely of funds in foreign currencies by sale or transfer. Other methods require the approval of the Bank.

In the absence of instructions stipulating otherwise, the Bank is entitled to credit or debit foreign currency amounts in Swiss francs – and namely at the exchange rate of the date of receipt or processing - unless the Client holds an account in the relevant foreign currency. If the Client holds accounts only in other currencies, the Bank may credit or debit the amount in one of these currencies at its discretion.

10. Bills of exchange, cheques, and similar instruments

The Bank is entitled to debit the Client's account with bills of exchange, cheques, or similar instruments previously credited or discounted in the event of their non-payment. This applies also if previously paid cheques are subsequently determined to be stolen or otherwise lost, forged, or defective. Pending the payment of any balance resulting, however, the Bank retains a claim to payment of the total amount of the bill of exchange, cheque, or similar instrument, including ancillary claims, against all obligors associated with said instruments.

11. Termination of the business relationship

The Client and the Bank may at any time discontinue existing business relationships with immediate effect or at a later date. In particular, the Bank can cancel credit limits at any time and declare their balances due for immediate payment, subject to separate agreements and terms of cancellation in effect for specific products.

12. Limitation of services, liquidation

In order to comply with legal, regulatory, or contractual requirements, to adhere to the customary due diligence, or to assure irreproachable business conduct, the Bank may limit services to the Client, either partly or completely. This applies irrespective of supplemental rules governing individual bank services. In particular, the Bank may block the account and custody account relationship, the execution of orders of any type (e.g., orders for deposits or payments, for transfers or assignment of balances, securities, and other assets, or for netting), as well as generally refuse to accept assets or credits.

In the event of a termination or if stored assets or balances can no longer be stored by the Bank due to legal, regulatory, product-specific or other reasons, the Client shall be obligated to advise the Bank, if requested, as to where these assets and balances should be transferred.

If, after a reasonable period set by the Bank due to termination of the business relationship or limitation of services, the Client fails to advise the Bank as to where the assets and balances held by the Bank should be transferred, the Bank may physically deliver or liquidate the assets. The Bank may deposit, with discharging effect, the proceeds and remaining balance of the Client to the location designated by the judge or in the form of a cheque to the Client's last known delivery address.

13. Holidays

In all business transactions with the Bank, Saturdays are treated the same as an official public holiday.

14. Outsourcing of specific Bank activities

The Bank may outsource departments and services, in part or in full, to service providers (other banks and legal entities within the Basler Kantonalbank Group or third parties) within Switzerland or abroad.
Within the scope of outsourcing, it may be necessary to transmit data to third parties. All service providers are bound to appropriate confidentiality requirements.

15. Compliance with legal and regulatory requirements

The Client is responsible for compliance with legal requirements applicable to him as well as to other persons involved in the bank relationship or the assets (including tax laws and disclosure and reporting obligations). He shall adhere to the legal requirements applicable to him at all times. On request of the Bank, the Client will document that he and other persons involved in the relationship have complied with the respective applicable regulations.

600 9676 1.20

16. Data protection and banking secrecy

Governing bodies, employees, and agents of the Bank are subject to legal obligations regarding the protection and confidentiality of data relating to the business relationship with the Client.

The obligation of the Bank to preserve banking secrecy does not apply in the event of legal or regulatory obligations of disclosure or reporting by the Bank, in case of consent by the Client, or in the presence of other legal justifications, such as in particular the safeguarding of legitimate interests of the Bank. This applies in particular:

a) Towards third parties in Switzerland and other countries (e.g., brokers, banks, transaction registers, stock exchanges, processing agents and third-party depositories, issuers, authorities responsible and other involved third parties) in transactions and services rendered by the Bank for the Client (e.g., account and custody account management or the handling of payment, securities, foreign currency and other client transactions), specifically those with international connections. Such disclosures may arise from Swiss or foreign law, self-regulation, market practices, contractual terms or conditions of issuers, service providers and other parties on which the Bank relies for the handling of such transactions and services;

b) In the event of proceedings by the Client or other parties involved in the banking relationship or the assets in Switzerland or other countries being imminent or initiated against the Bank (also as a third party);

c) To safeguard the enforcement in Switzerland or in other countries of receivables or other right towards the Client and for the realization of securities provided for the Client;

d) In the event of complaints by the Client or other parties involved in the banking relationship or the assets relating to the Bank made in public, towards the media or the authorities;

e) For the exchange of information between the Bank and other banks and legal entities of the Basler Kantonalbank Group within Switzerland for business purposes such as end-to-end and efficient performance and handling of client-facing bank business, information on the range of services of Group entities, ensuring risk management, compliance with statutory and regulatory regulations or for other compliance issues. The recipients are bound by the confidentiality provisions.

The Bank stores and processes data relating to its business relationship with the Client as well as data from third-party sources that it can use to create and process profiles. This Data may be exchanged between the Bank and other banks and legal entities of the Basler Kantonalbank Group and be used for the reasons listed in e) and for market research and other marketing purposes.

The Bank publishes the principles of its processing of personal data and any updates of such principles on its website (www.bkb.ch/datenschutzerklaerung).

The Client is aware that data that are transferred to other countries are no longer protected by Swiss law but are subject to the provisions of the respective foreign legal systems.

17. Dormancy

The Client is obligated to take necessary measures to prevent the business relationships existing between him and the Bank from becoming dormant in accordance with the pertinent regulations. In particular, the Client is obligated to notify the Bank promptly of any change of address or name (e.g., due to marriage).

The Client acknowledges that the Bank is obligated to report the business relationship to a central reporting office as soon as the relationship has become dormant.

In addition to the conditions and other charges according to the fee schedule/product data sheets, which continue to apply in the case of dormancy, the Bank is entitled to debit to the Client a special charge plus compensation for all expenses incurred in connection with the dormancy.

18. Amendments to the Terms and Conditions

The Bank may amend the Terms and Conditions at any time. The changes will be communicated to the Client in advance by appropriate means and shall be deemed to have been approved if not contested within one month.

19. Applicable law and place of jurisdiction

All legal relationships between the Client and the Bank are subject to **Swiss law exclusively.** The place of performance, place of debt collection for Clients with a foreign domicile, and **the sole place of jurisdiction for all disputes shall be Basel.** The Bank shall be entitled to initiate legal proceedings against the Client at the competent court of his domicile or at any other competent court; Swiss law shall, however, remain exclusively applicable.

Mandatory provisions as to the place of jurisdiction under Swiss law shall take precedence.

600 9676 1.20

Basler Kantonalbank

Safe custody regulations

In case of differences between the German and English version of this document the German version shall prevail.

1. Applicability

These regulations are applicable in addition to the Terms and Conditions for storage, book entry, and management of valuables and other suitable items (safe custody assets) by the Bank, especially if these are kept in the form of intermediated securities. They supplement any other contractual agreements that may exist.

2. Acceptance of items

The Bank accepts safe custody assets generally in open safekeeping accounts, specifically:

- Intermediated securities, securities, security rights, and other non-certificated money and capital market investments, as well as other financial instruments, for safekeeping (and/or book entry) and management;
- Acceptable precious metals and coins in merchantable form and quality, as well as mortgage securities and documentary evidence (e.g. insurance policies) for safekeeping.

The Bank may decline to accept such items without stating a reason. This applies in particular if the Client does not fulfill the relevant investment restrictions.

If the Bank no longer wishes to store the safe custody assets due to investment restrictions or for legal, regulatory, product-specific or other reasons, the Bank will ask the account holder for instructions on where to transfer the safe custody assets. If instructions from the Client are not received within a reasonable period set by the Bank, the Bank may physically deliver or liquidate the assets.

The Bank may verify the authenticity of the items deposited by the Client or may check them against a stopping list or have them inspected by a third party domestically or outside Switzerland without however, assuming any liability. In this case the Bank will execute sales and delivery orders and management actions only after inspection has been completed. The costs of the inspection may be invoiced to the Client.

3. Due-diligence obligation

The Bank effects with the customary due diligence book entry, safekeeping and management of the safe custody assets.

4. Return and transfer of safe custody assets

Subject to periods of notice, provisions of law, statutes of issuers, security rights of the Bank, and special contractual agreements, the Client may at any time instruct the Bank to deliver to him or transfer safe custody assets in accordance with the legal regulations in effect at the place of safekeeping and in keeping with the customary delivery period and form. The fees for delivery and transfer are based on the accessible fee schedules/product data sheets. Where delivery is made from collective safe custody deposits, the account holder shall not be entitled to any particular numbers, denominations, mintings, etc.

Transport and dispatch by postal service of safe custody assets shall be at the Client's expense and risk. If a declaration of value is required, the Bank shall execute this at its own discretion in the absence of special instructions from the Client.

5. Duration of agreement

The safe custody arrangement is of unlimited duration. It shall not lapse upon the decease, incapacity, or bankruptcy of the Client.

6. Conditions

The current conditions and other charges are based on the accessible lists/product data sheets and are subject to change, specifically in case of changes in the costs and reevaluation of business risks, through revision of the fee schedules/product data sheets at any time. The Client will be notified of such changes in advance by appropriate means.

The Bank may, at its discretion, charge reasonable compensation for any services rendered by the Bank that are not included in a fee schedule/product data sheet but that are rendered on behalf of, or in the presumed interests of, the Client and are normally expected to be rendered for payment only (e.g. commissions and third-party expenses, procedural and legal costs incurred by the Bank in connection with the safe custody assets).

7. Payments from third parties

The Bank may receive payments from third parties in connection with the sale of collective capital investments and other investment products, specifically management fees. The Bank will pass on the distribution remunerations received to the Client periodically.

600 9676 12.18

8. Storage of the safe custody assets

The Bank is authorized to hold the safe custody assets separately or in collective deposit with a third-party custodian either domestically or outside Switzerland under its own name but for the account and at the risk of the Client. In case of third-party storage, the Bank shall be liable only for the customary due diligence in the selection and instruction of the third-party custodian.

Redeemable assets may also be held in collective safe custody. Safe custody assets that need to be kept separately because of their nature or for other reasons will be excluded from collective safe custody arrangements. Safe custody assets held outside Switzerland shall be subject to local laws and practices. Third-party custodians may assert a right of lien or other security right over the safe custody assets.

If foreign legislation makes it difficult or impossible for the Bank to withdraw safe custody assets held outside Switzerland, the Bank shall be obliged only to procure a pro rata restitution claim for the Client at a correspondent bank of its choice at the deposit location, if such a claim exists and is transferable.

9. Registration of the safe custody assets

Safe custody assets of Swiss issuers made out in a particular name will be registered in the name of the Client in the relevant register (e.g., share register), if explicitly authorized by the Client. Consequently, the data transmitted for registration (in particular, the Client's identity) will be known to the relevant agency (company, registry administrator, etc.).

If registration in the name of the Client is either contrary to normal practice or not possible, the Bank may, for the account and at the risk of the Client, have assets registered in the name of a third party or in its own name.

10. Reporting and disclosure obligations

The Client is responsible for fulfilment of all duties of reporting and disclosure, as well as other obligations (e.g., disclosure of shareholdings, submission of a takeover offer), to companies, stock exchanges, authorities, or other market participants. Definitive in this regard is the applicable domestic or foreign law The Bank is not obligated to advise the Client of his reporting obligations. If the safe custody assets are registered in the name of a nominee company or in the name of the Bank, the Client must notify the Bank immediately of any reporting obligation.

The Bank may refuse, under notice to the account holder, to take, either wholly or in part, any administrative actions for safe custody assets that result in reporting or disclosure obligations for the Bank.

The Client is solely responsible for complying with any restrictions in effect, fulfilling requirements, or obtaining the required approvals in accordance with applicable domestic or foreign law if he executes or authorizes transactions with safe custody assets.

The Client is responsible for obtaining information regarding such reporting and disclosure obligations and restrictions, etc.

If such obligations are not required until after a purchase has been effected, the Bank will be authorized to sell the affected safe custody assets if it has not received the authorization for disclosure from the Client in time despite having warned the Client of the sale.

11. Conversion of safe custody assets

The Bank is entitled to have submitted documents annulled, replaced by vested rights, and to hold securities and vested rights – if the requirements are met – through credit to a securities account as book-entry securities. Similarly, the Bank is entitled, if intended by the issuer, to request printing and delivery of securities.

12. Administration

Without awaiting specific instructions from the Client, the Bank will attend to the usual administrative transactions, such as:

- Collection of interest, dividends, other distributions, and repayable capital amounts falling due;
- Exchange and subscription of safe custody assets without right of choice by the Client (splits, spin-offs, etc.);
- Monitoring of redemptions, terminations, conversions, subscription rights, amortizations of safe custody assets, etc.

If the Bank is unable to manage the individual assets in the ordinary manner, it will communicate this fact to the Client by the notice that the assets were booked into his/her custody account, or by other means.

If specifically instructed by the Client to do so in a timely manner, the Bank will also perform administrative actions such as:

- Exercise of subscription, conversion, and option rights;
- Performance of conversions;
- Payment on partly paid safe custody assets;
- Execution of orders from securities offers in connection with public takeover bids, mergers, splits, conversions, etc.

Whenever possible, the Bank will advise the Client by appropriate means of upcoming events pertaining to the safe custody assets. If instructions from the Client are not received in time, the Bank will be entitled but not obligated

600 9676 12.18

to act at its own discretion. Normally, unexercised subscription rights are sold and repurchase, replacement, and conversion options are not accepted.

The Bank will not perform any administrative acts, in particular for:

- Registered shares without coupons, if the Bank's address is not given as the postal address for dividends and distributions;
- Safe custody assets traded exclusively or predominantly in a foreign country but held as an exception in Switzerland;
- Mortgage items and documentary evidence (e.g., insurance policies).

In performing all administrative acts, the Bank will proceed on the basis of the standard banking information to which it has access, although without assuming any responsibility. For as long as the assets are managed by the Bank, the Bank will be entitled but not obligated to issue necessary instructions to and obtain required information from issuers or third-party custodians.

It is the responsibility of the Client to assert his rights arising from the safe custody assets in legal, insolvency, or similar proceedings and to procure the needed information.

13. Credits and debits

Sums will be credited or debited to an account held at the Bank designated by the Client. In the absence of instructions stipulating otherwise, the Bank will be entitled but not obligated to convert sums in a foreign currency to Swiss francs.

Credits will be made subject to collection. The Bank will be entitled to reverse entries made in error, specifically also subsequently without time limitations after completed posting to the safe custody account or the Client's account. The Client acknowledges that such adjustments by the Bank will be made without prior consultation with the Client. The provisions relative to cancellation as defined in the Law on Intermediated Securities remain valid.

Changes in instructions relating to accounts must be received by the Bank at least five bank working days before the transaction falls due.

14. Account statements

As a rule at the end of the year, the Bank will provide the Client with a statement of the safe custody assets deposited. The statement can include other assets not covered under these regulations. Safe custody assets will not be designated specifically as such.

Valuations of the contents of safe custody accounts are based on non-binding values taken from standard banking information sources. The Bank assumes no liability for the accuracy of this information or for any information in connection with the posted values.

15. Changes to the safe custody regulations

The Bank reserves the right to make changes to the safe custody regulations at any time. These changes will be communicated to the Client in advance by appropriate means and shall be deemed as approved unless written objection is received within one month.

600 9676 12.18

Basler Kantonalbank

Terms and Conditions for the use of Visa Debit card issued by Basler Kantonalbank

I. General provisions

1. General information

The following "Terms and Conditions" are applicable to the Visa Debit card (hereinafter also referred to as the "card") issued by Basler Kantonalbank (hereinafter the "Bank"). In all other respects, the "Basic Documents" apply, specifically the Bank's "General Terms and Conditions" and any other separate agreements or provisions applicable to certain transactions or services.

The card always relates to a specific bank account. The contractual relationship regarding the card (hereinafter also the "contractual relationship" or "contract") is concluded between the account holder and the Bank. Transactions are debited from or credited to this bank account. The Bank can arrange for the inclusion of other accounts held by the account holder (multiple-account function). In addition to the account holder, authorised account users or other persons designated by the account holder may be card holders. The Bank reserves the right to limit the issue of cards in the name of third parties to authorised account users. Such third parties are designated as "authorised card users". The card is issued in their name in each case. The account holder is likewise an "authorised card user". The Bank may, without being obligated to do so, make it possible for authorised account users to order cards without requiring express authorisation from the account holder. The account holder is liable for the use of all cards. The account holder is able to view the data and transactions of all authorised card users. The cards remain the property of the Bank. The issuing of cards for authorised account users and other third parties does not give rise to a contractual relationship between them and the Bank.

By ordering a card and/or using it for the first time, each authorised card user declares their consent to these Terms and Conditions.

2. Formation of the contractual relationship

If the contractual relationship including these Terms and Conditions does not come about as part of a separate card application set out in writing or in any other formal manner, each authorised card user acknowledges these Terms and Conditions and the fees as applicable at the time the card is used, at the latest upon first use of the card or if the card is not returned to the Bank within 30 days. The account holder is responsible for informing any other authorised card users about changes to these provisions and conditions where they are not communicated directly by the Bank. Authorised card users authorise the account holder to issue and take receipt of all declarations relating to the card also on their behalf. To the extent provided for by the Bank in its provisions relating to powers of attorney, authorised account users can also apply for cards made out in their own name and in this respect enter into the corresponding contractual relationship on behalf of the account holder.

3. Powers of attorney / death and incapacity to act

Revocation of an account power of attorney does not automatically lead to the respective card becoming invalid. Similarly, the death or incapacity to act of authorised card users does not automatically cause the card to be blocked. The account holder or their legal successor must expressly request the Bank to block the card.

4. Amendments to the Terms and Conditions

The Bank reserves the right to amend these Terms and Conditions (including but not limited to fees and card functions/services) at any time. The account holder shall be informed in a suitable manner of any changes at least 30 days before they enter into effect. Unless the account holder terminates the contractual relationship pertaining to the card or all cards are returned by the respective authorised card users before the amendment enters into effect, the amendments shall be deemed approved and in any event upon first use of the card after the amendments have entered into effect.

5. Bank's right to debit

The Bank is authorised to debit all amounts arising from use of the card (transactions) and fees from the relevant account printed on the card. This also applies to amounts posted as reserved or provisional. This can have effects on card limits and cause restrictions on the liquidity available in the account. Transactions in a currency other than the account currency are converted by the Bank into the account currency. The Bank is entitled to reject transactions without giving reasons if processing of such transactions would lead to a negative balance in the account. The Bank shall not be liable for any losses that may be incurred by an authorised card user because of this.

Transactions are listed at regular intervals (e.g. monthly) on the corresponding statement. On termination of the contractual relationship, there remains a right to debit all amounts attributable to prior use of the card. The Bank's right to debit shall remain in effect without any restrictions even in the event of disputes between authorised card users and third parties (e.g. points of acceptance). Any disputes regarding discrepancies and complaints about goods or services and claims arising from the same shall be settled by the authorised card user directly with the respective point of acceptance.

501 0022 8.21

6. Duration and card renewal
The card is valid until the end of the date shown on the card. Unless expressly waived by the authorised card user, the card will be automatically replaced by a new card before the expiry date shown on the card. If the holder does not receive their new card at least ten days before expiry of the existing card, they must inform the Bank immediately. The Bank has the right not to renew a card without giving reasons. After expiry of the validity period or upon receipt of a replacement or renewal card, the previous card shall be immediately rendered unusable by the authorised card user.

7. Termination and blocking
The account holder may terminate their own card or the card of another authorised card user or, where applicable, the corresponding contractual relationship. Other authorised card users may only terminate their own cards or the corresponding contractual relationship in each case. On effective termination, the card shall be immediately returned to the Bank without request. The Bank is entitled at any time to block the card without stating reasons and without notifying the authorised card user beforehand. The Bank will block the card if expressly requested by the authorised card user, if they report the loss of the card and/or the PIN code and in the event of termination. The costs associated with blocking may be charged to the account. Despite termination or blocking, the Bank is entitled to charge to the account holder all amounts that are deemed authorised by the authorised card user after termination or blocking (such as debits relating to recurring services for newspaper subscriptions, memberships or online services).

8. Assignment
The Bank may, at any time, transfer or assign the contractual relationship or individual entitlements or duties arising therefrom to domestic and international third parties (such as debt collection agencies) and may make data associated with the contractual relationship available to such third parties (including disclosure of the underlying bank relationships) to the extent necessary.

II. Card use

1. Types of use (functions)
Depending on the agreement in place, the card can be used for one or more of the following functions:

1.1 Cash withdrawal function
The card can be used to withdraw cash debited to the account printed on the card from correspondingly marked domestic and international ATMs and from authorised agents, up to the limits specified for the card. In addition to the account printed on the account holder's Visa Debit card, the Visa Debit card can additionally provide access to other accounts of the account holder held by the Bank.

1.2 Payment function
The card can be used to pay for goods and services at brick-and-mortar outlets or on the internet from domestic or international providers, up to the limits specified for the card.

1.3 The Bank's own services
The authorised card user can make use of the Bank's own services at the Bank's ATMs. Within the area of the Bank's own services, the card can be used – subject to card limits that may deviate from the usual or agreed card limits or in addition to the same – for services including but not limited to cash withdrawals within the scope of the credit balance available in the underlying account or any credit limits granted or up to card limits specifically agreed for the Bank's own services. The Bank may extend or terminate such services at any time without prior notice.

1.4. Deposit services
The Visa Debit card may be used to deposit banknotes and coins at correspondingly marked ATMs. The amount identified by the ATM and confirmed on the ATM by the depositor is automatically credited to the account named on the card or the account integrated using the multiple-account function and selected at the ATM less the fee stated in the price list; the value date is the date of deposit.

The amount shall be credited irrespective of the relationship between the depositor and the account holder, if not the same person. The depositor's right to object expires upon acceptance of the amount by the ATM.

1.5 Obligation to provide sufficient funds
The card may be used only if there are sufficient funds in the account (account balance or credit limits). If there are not sufficient funds in the account, the Bank shall be entitled to refuse transactions.

1.6 Transaction receipt
The authorised card user is given a transaction receipt for cash withdrawals with the card at most ATMs upon request, in the case of payment of goods and services this will happen automatically or upon request. This is deemed to be a notification of debit. In the case of cash deposits at the Bank's correspondingly marked ATMs, the amount automatically recognised by the ATM and confirmed by the depositor will be credited to the selected account. The transaction receipt received when depositing cash is deemed to be a notification of credit.

501 0022 8.21

1.7 Technical malfunctions and operational breakdowns
Technical malfunctions and operational breakdowns that make use of the card impossible do not entitle the authorised card user to any compensation.

1.8 Visa Debit card with third-party services or benefits
The Visa Debit card can be linked to additional services, such as insurance services, that the authorised card user uses or may use by using or holding the card. Such additional services, specifically insurance services, are – where applicable – described in product overviews and governed by separate terms and conditions. It is possible that such terms and conditions are issued by a third party, such as an insurance provider. If such terms and conditions exist or are applicable, they will be available on the Bank's website. Third-party services may consist of services that are not provided by the Bank and do not form the basis for any claims on the Bank by the authorised card user or, where applicable, other persons.

2. Authorisation options
The authorised card user is entitled to pay for goods and services or make cash withdrawals, within the scope of the specified or agreed limit(s), at the corresponding points of acceptance as follows:

2.1 With their PIN code.

2.2 By personal authorisation in a manner other than the PIN code or other means of identification (in this context, see the additional provisions for the use of online services).

2.3 On the basis of purchases of goods or services made by telephone, the internet, post or any other means where the transaction is triggered solely by stating the name of the authorised card user, the card number, the expiry date and – where required – the card verification code (CVV, CVC) printed on the card.

2.4 By using the card without entering the PIN code or other means of identification at automated points of payment (e.g. for contactless payment, car parking/ ticket machines or motorway toll points).

The account holder recognises all payments or cash withdrawals that have been authorised pursuant to this clause II 2 and the claims on the part of the points of acceptance arising from these. At the same time, the Bank is instructed expressly and irrevocably to pay the amounts to the respective point of acceptance.

3. Restriction or extension of possibilities for use
The possibilities for use of the card, PIN code and any limits may be extended, restricted or cancelled at any time. These limits may be requested from the Bank.

4. Forbidden uses of the card
The card may not be used for illegal purposes.

III. Duty to exercise due diligence on the part of the authorised card user

1. Safekeeping, loss, theft and misuse of the card.
The card must be kept in a safe place at all times. The authorised card user must immediately report any loss, theft or indication of misuse to the place specified by the Bank.

2. Keeping means of identification secret (e.g. PIN code)
The authorised card user is obligated to keep secret the PIN code and any other means of identification provided to them. These must not be passed on to any third parties or recorded in any way even in an encrypted form. Neither the PIN code nor any other means of identification may consist of easily deduced combinations, such as telephone numbers, dates of birth, car registration numbers, names of the authorised card user or their family members. The Bank will never ask the authorised card user to disclose the PIN code and/or passwords or other means of identification. The Bank refuses all responsibility/liability for any detrimental consequences arising from non-compliance with the duties of the authorised card user.

3. Duty to check and report discrepancies
Any instances of misuse or other irregularities – including but not limited to those visible from the statement of the underlying bank account – must be reported to the Bank without delay upon discovery.

Furthermore, a written complaint with all documents directly relating to the transaction(s) that are being objected to must be submitted to the Bank no later than 30 days after the bank statement was issued. This applies irrespective of whether bank statements are sent to the account holder or at the account holder's request, to a third party. The bank statement will otherwise be deemed approved with regard to the card transactions. If a claim form is sent to the account holder or authorised card user, it must be completed, signed and returned to the Bank within ten days of receipt. In the event of misuse, the authorised card user or the account holder is obligated to take all action to clarify the issue and mitigate the loss. In this respect, they shall follow the instructions issued by the Bank or third parties engaged by the Bank. The Bank can request a criminal complaint be filed with the police or the responsible criminal investigation authority and to be provided with a copy or confirmation of the complaint. The account holder and other authorised card users are liable

501 0022 8.21

to the Bank for any costs incurred by the Bank in connection with complaints made against their better judgement or with intent to defraud.

4. Communication of changes
All changes in the details of authorised card users (specifically changes of name, address and account as well as changes in economic beneficiaries or level of income) must be communicated to the Bank in writing without delay. Communications from the Bank to the last address of which it was informed are deemed duly delivered. The Bank reserves the right to charge the account holder for any costs it incurs in connection with searching for addresses.

5. Recurring services
Recurring services that are paid for with the card (e.g. newspaper subscriptions, memberships, online services) must be terminated directly with the point of acceptance if they are no longer wanted. If the card contract is cancelled, the authorised card user is required to change or renew the payment arrangements themselves at the point of acceptance or terminate the contractual relationship in question.

6. Payment transactions over the internet
If the point of acceptance offers a secure payment method (e.g. 3-D Secure), the authorised card user must make their payment by means of such secure payment method and, in doing so, comply with the additional provisions on the use of online services.

IV. Responsibility and liability

1. Assumption of losses subject to compliance with Terms and Conditions / No fault
Provided that the authorised card user has complied with the present "Terms and Conditions" in all respects (specifically their duty to exercise due diligence) and they are also not at fault in any other way, the Bank shall assume any loss incurred by the account holder from misuse of the card by third parties. This includes any losses as a consequence of forged or falsified cards. On acceptance of such compensation, the account holder assigns their claims from the loss event to the Bank. Authorised card users must contribute to the best of their knowledge to clarification of any loss event and to mitigating the loss. In this respect, the Bank's instructions must be followed.

The following are not deemed to be "third parties": authorised card users, their spouse/registered partner/domestic partner, family members related in a direct line (especially children and parents) or other closely related persons, authorised persons and persons living with them in the same household. Any losses for which compensation is payable under an insurance arrangement and any consequential losses are not assumed. If a complaint proves to be unjustified, the account holder authorises the Bank to debit the account underlying the card with the amounts credited as compensation.

2. In event of breach of the duty to exercise due diligence
Authorised card users who do not fulfil their duty to exercise due diligence shall be liable, on an unlimited basis, for all losses arising from misuse of the card until any block becomes effective. In this respect, the account holder is jointly liable with the respective authorised card user.

3. For transactions concluded using the card
The Bank refuses all responsibility for transactions concluded using the card. In particular, any complaints relating to purchased goods or services and any further differences of opinion and claims from the corresponding legal transactions shall be settled directly with the point of acceptance in question. The Bank's right to post a debit remains in place without any restrictions.

4. In the event of non-acceptance of the card
The Bank does not accept any responsibility in the event that a point of acceptance refuses for any reason to accept the card or that a payment or withdrawal cannot be made with the card for technical or other reasons. The same applies to cases where use of the card at an ATM proves to be impossible or if the card is damaged or rendered unusable by the ATM.

5. In the case of use with a PIN code or other means of identification
Every authorised use of the card with the associated PIN code or with other means of identification shall be deemed to have been made by the authorised card user. The authorised card user thereby assumes a binding obligation for all purchases, transactions or other business transactions conducted and for resulting debits made to their card. By the same token, the Bank is entitled to debit from the account transactions conducted and registered electronically in this way. The risks arising from misuse of the card using the associated PIN code or with other means of identification are thus in principle borne by the account holder.

In the case of proven illegal interventions by third parties in the equipment of network and/or telecommunications operators or in the infrastructure used by the authorised card user for payment (e.g. EFT/POS terminals), the Bank shall assume any debits for instances of misuse of the card, when notified in due time, provided that the authorised card user has fulfilled their duties to exercise due diligence in all respects and is in no other way at fault.

501 0022 8.21

6. After ending the contractual relationship, reclaiming or returning the card(s)
The right to use the card, specifically also for orders placed by telephone, by post or over the internet expires in any event when the contractual relationship ends or after the card has been reclaimed or returned. The Bank refuses all liability for losses caused by authorised card users using the card after the end of the contractual relationship or after the card has been reclaimed or returned. The account holder is liable in full for any losses arising therefrom. Illegal use of the card may be lead to civil law claims or criminal prosecution.

V. Fees (including commissions, interest and costs)

1. Fees
The annual fee for the card is due in advance and there is no entitlement to any refund of this fee, specifically in the event of the card being blocked, the contractual relationship being terminated or the card being reclaimed or returned. Use of the card and/or the contractual relationship can involve fees, commissions, interest and costs. Apart from costs incurred in extraordinary cases through culpable actions on the part of the authorised card user, the amount of the above will be communicated to the account holder in a suitable form and can be inquired from the Bank or viewed at www.bkb.ch at any time.

2. Foreign currency transactions
In the event of transactions in a currency other than the card currency (foreign currency) the account holder acknowledges a fee for processing by the Bank. The amount of this fee is based on the then current fee schedule. Conversion of the foreign currency into the card or account currency shall be performed at the conversion rate determined by the Bank.

3. Transactions abroad in Swiss francs
If a Swiss franc card is used at foreign points of acceptance for payment in Swiss francs, the Bank can charge a processing fee. The amount of the processing fee is based on the then current fee schedule.

VI. Additional terms and conditions for the use of online services

The Bank can make various services available to the authorised card user by means of the internet, an app or E-Banking (hereinafter referred to as “online services”), including but not limited to notification of transactions conducted as well as the performance of checks and confirmation of payments on the internet, for instance using 3-D Secure in an app. To obtain access to online services, the authorised card user must log on in each case using the means of identification valid for that particular online service. In addition to the present Terms and Conditions, the authorised card user must accept any further terms and conditions or provisions specific to each individual online service that are brought to their attention when logging in to, or registering for, the respective service.

VII. Data processing, disclosure of data to third parties and commissioning of third parties

1. Data processing by the Bank
As data controller, the Bank processes data of the authorised card user for the formation and handling of the card relationship. The account holder is obligated to inform third parties whose data is processed at the account holder’s instigation about such processing by the Bank.

2. Disclosure of data and data processing
The account holder and each authorised card user accept that in order to render its services the Bank may engage a third party – specifically a processor for handling and processing the card transactions. Specifically, they consent to the parties commissioned by the Bank for the handling of the card business and the subcontractors engaged by the same (e.g. for producing the cards) gaining knowledge of their data to the extent necessary for rendering the service or diligent fulfilment of the relevant tasks.

No objection to the transmission of data and the aforementioned data processing is possible other than through termination of the card agreement.

The account holder and each authorised card user acknowledges that transaction data may allow conclusions to be drawn concerning the behaviour of authorised card users (including but not limited to place of residence, place of work, health status, financial circumstances, leisure time activities, social interaction and further details).

3. Data processing for the purpose of service provision, market research and marketing as well as combating payment card misuse
Within the scope of providing customer service, the Bank can process the data of each authorised card user, specifically to ensure efficient customer care and to prepare evaluations for the authorised card user and/or the account holder and to provide notifications of the same. In particular, the Bank is also authorised to create and evaluate customer, consumption and preference profiles in order to analyse and predict the interests and behaviour of authorised card users (“profiling”), to develop products and services in conjunction with debit cards and to offer authorised card users the relevant products and services or to provide them with information on the same, as well as for the purpose of early identification of card misuse. The Bank can enrich data in this context with additional information known to the Bank on the authorised card user. Similarly, the Bank can engage third parties to assist with the aforementioned purposes and make such data accessible to them.

501 0022 8.21

4. Disclosure of data for statutory or regulatory reasons
The account holder and each authorised card user acknowledge that contractual and transaction data may be disclosed by the Bank to fulfil statutory or regulatory duties to provide information and in pursuit of legitimate interests (as part of recovery proceedings, for example). They likewise acknowledge that the Bank can send the account holder or authorised card users fraud warnings using the mobile telephone number made known to the Bank, which may potentially disclose the existence of the banking relationship and associated information.

5. Authorisation to obtain information and documents
Independently of any instances of data procurement permitted by law, the Bank is at any event authorised to obtain information from third parties required for checking the details provided by authorised card users, processing the card application and handling of the contract, including but not limited to third parties engaged by the Bank for handling the card business and credit agencies. The Bank is authorised to obtain information from third parties, including but not limited to the Central Office for Credit Information (ZEK), authorities (e.g. enforcement agencies and tax offices, residents' registration offices), employers and other statutory (e.g. the Consumer Credit Information Office, IKO) and other suitable information offices and agencies and to report blocked cards, serious payment arrears or misuse of cards and similar acts on the part of the authorised card user to the ZEK or, in the cases specified by law, to the agencies responsible. The ZEK and the IKO are expressly permitted to make such data available to their members. The account holder or the authorised card user authorises the Bank to disclose to the third parties engaged to handle the card business at their request all information and documents they require to fulfil their duties in accordance with provisions in place, to combat money laundering and the financing of terrorism, or any that may enter into effect at a later date. This includes but is not limited to all information and documents required to identify the holder or to establish the economic beneficiary of the assets transacted using the cards and to perform statutory additional clarifications in this context. In this respect, the account holder or authorised card user releases the Bank from banking secrecy in relation to the third party engaged. The Bank is authorised to inform the third party so engaged of changes to customer data.

6. Data processing by the Bank for risk assessment purposes
The Bank and third parties engaged by the Bank are authorised to store, process and combine data of all authorised card users relating to the contractual relationship and to use of the card for the purpose of calculating and assessing credit and market risks relevant to the business and for creating risk profiles (risk assessment purposes), to enrich such data with data from external sources, use such data and create profiles from the same.

7. Engagement of third parties
The Bank is authorised to commission third parties in Switzerland, in the EU or the EEA and, in individual cases, worldwide with all or part of the activities necessary for the purpose of handling all services arising from the contractual relationship including bonus programmes (e.g. reviewing the application, producing the cards, contract processing, online services, debt collection, communications with customers, any calculation of credit risks), for refining the risk models used when setting limits and for combating fraud as well as for the purpose of data evaluation and sending out offers and information pursuant to clause VII 2 and clause VII 3 above. The authorised card user authorises the Bank to provide such third parties with the data necessary for diligent fulfilment of the allocated duties and to also forward such data on to other countries for this purpose. Data is only disclosed to third parties if the recipient undertakes an obligation to maintain secrecy and/or to maintain an appropriate level of data protection and to impose such obligations on any potential contracting partners. The authorised card user accepts that data is transmitted to the Bank via global card networks even in relation to transactions within Switzerland. It is expressly pointed out that Swiss law (e.g. bank-customer confidentiality, data protection) is limited to the territory of Switzerland and therefore all data transmitted to another country no longer enjoys protection under Swiss law and, in certain circumstances, also no equivalent protection.

8. Visa Debit cards with third-party services or benefits
If the Bank offers special Visa Debit – or associated programmes or special additional services such as insurance services – in cooperation with providers of third-party services, specifically pursuant to clause II 1.8), the Bank can make any necessary personal data on the authorised card user (such as name, date of birth, address, email address, telephone number, end of studies) available to the provider of those third-party services. On the basis of this, the provider of the third-party services may contact the authorised card user directly. The authorised card user hereby releases the Bank from bank-customer confidentiality and gives their consent to the transfer of data. The Bank does not accept any liability for any transactions concluded by the authorised card user with the providers of third-party services. If the criteria for use of the respective Visa Debit card are no longer fulfilled the Bank may communicate this to the provider of third-party services and may, where applicable, demand return of the Visa Debit card in question.

9. The Bank's privacy statement
In addition to the present Terms and Conditions, the Bank's privacy statement applies, which can be viewed or retrieved at www.bkb.ch.

501 0022 8.21

Basler Kantonalbank

VIII. Communications, security of electronic communication channels

The authorised card user and the Bank may, where provided for by the Bank, use electronic means of communication (e.g. app, email, text message, internet). If the authorised card user contacts the Bank by email or if they disclose their email address to the Bank they consent, by doing so, to the Bank contacting them by email. The authorised card user acknowledges that the open nature of the internet or any other means of communication (e.g. mobile telephone network) means that there is the possibility that third parties may gain unauthorised access to communications between the authorised card users and the Bank despite all security measures implemented by the Bank. In order to keep this risk to a minimum, the authorised card user shall use all means available to them to protect the end devices they use (e.g. computer, mobile telephone, etc.) specifically by installing and regularly updating comprehensive virus protection and internet security programmes and carrying out updates of the operating systems and internet browsers used. The authorised card user shall bear all consequences resulting from any unauthorised interception of data by third parties. The Bank reserves the right to make the use of electronic means of communication, specifically for making changes to data relevant to the contract and services provided through the internet, dependent on the conclusion of separate agreements.

Version August 2021

501 0022 8.21

Basler Kantonalbank

Provisions of Basler Kantonalbank on the use of one

I. General information

1. General provisions on the use of one

1.1 Provisions on the use of one and further documents

These provisions apply to the online services made available under the "one" name (hereinafter "services") provided by Basler Kantonalbank (hereinafter "Bank") to the holders (hereinafter "authorised card users") of a main or additional card issued by Basler Kantonalbank or a Business Card of the Bank, hereinafter "card" or "cards". one is operated by Viseca Payment Services SA, hereinafter "processor". The Bank uses the processor to perform tasks related to the card business. These provisions may make reference to card products or functions that the Bank does not offer at all, does not offer yet or will only offer at a later date. Such reference does not form the basis for any customer or authorised card user claims to the provision of those services.

one is available through the one website ("website") and through the one app ("app").

The further information on one should be noted – including but not limited to the information on data processing and data security – in the provisions governing data protection contained in III below and the processor's terms of use for one digital services ("one terms of use"). The Bank's data protection statement at www.bkb.ch/datenschutzerklaerung additionally applies.

These provisions apply in addition to the terms and/or provisions for the use of the Bank's cards applicable in each case. In the event of deviating regulations, the present provisions take precedence over such terms and/or provisions. The Bank reserves the right to amend these provisions at any time. Any amendments will be communicated to the authorised card user in a suitable manner.

1.2 Content of one and ongoing development

one comprises services provided by the processor on behalf of the Bank. Registration is required before one can be used. Newly introduced services are made available to registered authorised card users by means of updates. The Bank will inform authorised card users of further developments and, where applicable, any associated amendments to these provisions, in a suitable manner.

501 0021 8.21

1.3 Functions of one

one's functions may currently, or in the future include the following:

- a user account to administer personal data;
- the possibility to check and confirm payments, e.g. by means of 3-D Secure within the app or by entering an SMS code (text message) (see clause II 1);
- the possibility to check and confirm certain actions (e.g. logins, communications with the Bank) within the app or by entering an SMS code;
- the possibility to activate cards to use payment options;
- the exchange of communications and notifications between the authorised card user and the Bank (also including the possibility to communicate any amendments to provisions) unless a special form of communication or notification is required;
- an overview of transactions or cards and displaying invoices in electronic form;
- an overview of the balance of bonus programmes and the possibility of redeeming points;
- information on use of the card (currently SMS services).

2. Use of one

2.1 Authorisation to use

The authorised card user is authorised to use one subject to the following conditions:

- They are able to implement these provisions and the associated requirements.
- They are authorised as holder of a main or additional card or of a business card of the Bank, to use a card issued by the Bank.

2.2 Consents granted during registration and as part of the further development of one

By using one, the authorised card user herewith expressly grants the Bank the following consents:

- consent to the processing of data that is, or has been collected during the use of one. This also includes but is not limited to consent to such data being linked to data already held by the Bank and to the creation of profiles, in each case for the Bank's risk management and marketing purposes or those of the processor and third parties pursuant to the one data protection statement.
- Consent to the receipt of communications and information on products and services of the Bank and third parties for marketing purposes (advertising). The Bank may deliver such communications and information by email or directly within the app or on the website.
- Consent to the use of the email address provided during registration, the website and/or the app for reciprocal electronic communication (e.g. communication of address alterations, communication of amendments to provisions or communications regarding combating card misuse).
- Consent to the receipt of communications on products and services and/or to data processing for marketing purposes can be revoked, for the future, at any time by notifying the Bank. The necessary contact details can be found in the Bank's data protection statement.

2.3 Refusal to grant consent in the course of further development of one

If the authorised card user refuses to grant consent to provisions in the course of further development of one (e.g. updates), it might not be possible, under certain circumstances, to use the app or the website or individual services, or to continue using the same.

2.4 Effect of performing confirmations

Every confirmation performed through the app or through entry of an SMS code will be deemed to be an action on the part of the authorised card holder. The authorised card holder is entitled to provide evidence to the contrary. The authorised card user undertakes responsibility for debits to their card resulting from confirmations and authorises the Bank to execute the corresponding orders and to perform the corresponding actions.

2.5 Availability/blocking/amendments

The Bank may fully or partially suspend, limit or cease to offer the possibility of using one or replace it with another service at any time even without prior notice. In particular, the Bank is entitled to temporarily or permanently block the authorised card user's access to one (e.g. in the event of suspected misuse).

2.6 Intellectual property rights

All rights (including but not limited to copyrights and trademarks) to software, texts, images, videos, names, logos and other data and information that are, or become over time accessible through one are exclusively the property of the Bank or the relevant partners and third parties (e.g. the processor, Visa, Mastercard®), unless specified otherwise in these provisions. The names and logos visible in one are registered trademarks.

For use of the app, the Bank grants the authorised card user a non-exclusive, non-transferable, indefinite, revocable and free licence to download the app, install it on the authorised card user's device and to use the same within the scope of the intended functions. Use of

501 0021 8.21

the website and the Bank's electronic channels are additionally subject to the corresponding provisions on the Bank's website.

3. Risks, warranty disclaimer, due diligence and notification obligations

3.1 Risks arising from the use of one

The authorised card user acknowledges and accepts that the use of one involves risks.

In particular, the authorised card user's cards, username and password, devices used or personal data might be misused by unauthorised third parties through the use of one. This may cause financial loss to the authorised card user (through debits to their card) and lead to violation of their personal rights (through misuse of personal data). Furthermore, there is a risk that one, or one of the services offered on one, cannot be used (e.g. if it is not possible to log into one).

Specifically, misuse is made possible or easier through:

- any breach of the due diligence or notification obligations on the part of the authorised card user (e.g. due to careless handling of username/password or failure to report the loss of a card);
- the settings chosen by the authorised card user or inadequate maintenance of the devices and systems used to access one (e.g. desktop computers, mobile telephones, tablets, etc.), for instance, failure to use a screen lock or an adequate firewall, insufficient protection against viruses or using out-of-date software;
- interference by third parties or defective transmission of data via the internet (e.g. due to hacking, phishing or data loss);
- incorrect confirmations using the app or when entering an SMS code (e.g. failure to correctly check a confirmation request);
- weak security settings (e.g. saving the login)

chosen by the authorised card user for one, especially for the app.

Authorised card users can reduce the risk of misuse by complying with the due diligence and reporting obligations regarding the handling of mobile devices and the password and the duties to check confirmation inquiries.

The Bank does not provide any assurance or warranty that the website and the app are accessible on a permanent basis or will function without disruption or that any instances of misuse can be identified and prevented with absolute certainty.

3.2 General duties of the authorised card user to exercise due diligence

3.2.1 General duties to exercise due diligence when using devices and systems, especially mobile devices

one uses, among other things, the authorised card user's mobile devices (e.g. mobile telephone, tablet; a "mobile device" in each case) for authentication purposes. For this reason, keeping these mobile devices safe at all times is a significant security factor. The authorised card user shall treat mobile devices with appropriate care and ensure they are protected appropriately.

Consequently, the authorised card user shall comply with the following general duties to exercise due diligence when using devices and systems, especially mobile devices:

- a screen lock must be activated for mobile devices and further security measures must be taken to prevent unauthorised persons from unlocking the device;
- mobile devices must be kept in a safe place, protected from access by third parties and must not be handed over to third parties for continual permanent or unsupervised use;
- software (e.g. operating systems and internet browsers) must be updated on a regular basis;
- interference with the operating systems (e.g. "jail-breaking" or "rooting") is not permitted;
- anti-virus software and internet security programmes must be installed on laptops/desktop computers and regularly updated;
- the app must only be downloaded from official stores (such as the Apple Store or Google Play);
- app updates must be installed promptly;
- in the event of a mobile device being lost, every action must be taken to prevent unauthorised persons from accessing the data transferred to the mobile device (e.g. by blocking the SIM card, blocking the device, deleting the data, e.g. by using "Find my iPhone" or "Android Device Manager", resetting the user account or having it reset). The loss must be reported to the Bank (see clause I 3.3);
- the app must be deleted prior to any sale or any other permanent handing over of the mobile device to a third party.

3.2.2 General duties to exercise due diligence when handling the password

In addition to possession of the mobile device, the username and password both act as further factors for authenticating the authorised card user. In connection with the password, the authorised card user must comply in particular with the following duties to exercise due diligence:

501 0021 8.21

- the authorised card user must specify a password that they do not already use for other services and that does not consist of easily deduced combinations (e.g. telephone number, date of birth, car registration numbers, name of the authorised card user or persons closely associated with them, repeated or sequential numbers or letter combinations such as "123456" or "aabbcc");
- the password must be kept secret. It must not be disclosed or made accessible to third parties. The authorised card user acknowledges that the Bank will never ask them to disclose the password;
- the password must not be written down nor stored insecurely;
- the authorised card user must change the password or reset the user account or have it reset by the Bank if there is any suspicion that third parties have gained access to the password or other data;
- the password must be entered in such a way that it cannot be seen by third parties.

3.2.3 Duties to exercise due diligence in connection with confirmation requests
Confirmations impose a binding obligation on the authorised card user. Consequently, the authorised card user must comply with the following general duties to exercise due diligence in connection with confirmations in the app or when entering an SMS code:

- the authorised card user may only enter a confirmation when the confirmation request is directly related to a certain action or a certain transaction on the part of the authorised card user (e.g. payment, login, contact with the Bank);
- prior to entering the confirmation, the authorised card user must check whether the subject of the confirmation request corresponds to the transaction in question. The payment details displayed must be checked particularly in connection with confirmation requests relating to 3-D Secure.

3.3 Notification obligations of the authorised card user
The Bank must be notified without delay of the following events:

- loss of a mobile device;
- confirmation requests not relating to an online payment, a login by the authorised card user, any communication with the Bank or similar transactions (suspicion of misuse);
- suspicion of any other kind that confirmation requests in the app or the SMS code do not originate from the Bank;
- suspicion of misuse of username, password, mobile devices, the website, the app etc. or suspicion that unauthorised third parties have gained access to the same;
- changes to the telephone number and other relevant personal data;
- change in the mobile device used for one (in which case, the app must be registered anew).

4. Liability

4.1 Liability in the event of loss in general
Subject to clause I 4.2 the Bank will compensate for any losses not assumed under an insurance policy,

- if such losses were incurred as a consequence of proven unlawful interference with the facilities of network and/or telecommunication system operators or with the devices and/or systems used by the authorised card user (e.g. desktop computers, mobile devices and other IT infrastructure);
- if the authorised card user has complied with the due diligence and notification obligations specified in clauses I 3.2 and 3.3 above, specifically the duties to check confirmation requests and the duty to check the monthly statement of account and to object to transactions resulting from misuse in due time and the authorised card user is likewise not at fault in any other way with regard to the cause of the loss;
- if the loss in question has been incurred exclusively due to breach of the customary duty to exercise due diligence on the part of the Bank.

Liability for any indirect losses or consequential losses of any kind on the part of the authorised card user are excluded by the Bank except in the case of intent or gross negligence.

4.2 Exceptions
The authorised card user bears the risk for losses themselves in the following cases and the Bank excludes all liability:

- if the losses in question are not borne by the Bank pursuant to clause I 4.1 (specifically in the event of breach of due diligence and notification obligations by the authorised card user) or
- if the authorised card user, the spouse or registered partner of the authorised card user, directly related family members (including but not limited to children and parents) or other persons closely related to the authorised card user, authorised persons and/or persons living in the same household performed an action (e.g. confirmation in the app or by SMS code).

501 0021 8.21

II. Special note

1. 3-D Secure

1.1 What is 3-D Secure?

3-D Secure is an internationally recognised security standard for card payments over the internet. At Visa it is called "Verified by Visa" and "SecureCode" at Mastercard®. The authorised card user is obligated to use this security standard for payments whenever offered by the point of acceptance (the retailer).

1.2 How does 3-D Secure work?

Payments made with 3-D Secure can be confirmed (authorised) as follows:

- in the app or
- by entering a code, sent by the Bank to the authorised card user by text message (SMS code), in the relevant browser window during the payment procedure.

Every use of the card authorised by means of 3-D Secure will be deemed to have been made by the authorised card user.

1.3 Activating cards for 3-D Secure

3-D Secure is activated for all cards held in the name of the authorised card user relating to a registered business relationship between the authorised card user or a third party (such as an account holder) and the Bank when registering for one.

1.4 Deactivating cards for 3-D Secure

For security reasons, 3-D Secure cannot be deactivated once it has been successfully activated.

2. Mobile payment

2.1 What is mobile payment?

Mobile payment refers to solutions for using cards through a mobile device.

Mobile payment makes it possible for authorised card users in possession of a compatible mobile device to use authorised cards through a mobile application (app) of the Bank (for details see clause II 2.7) or a third-party provider for contactless payment as well as payment in online shops and apps. In such cases, the card number is not used, due to security considerations, but another number (token) is generated and stored as a "virtual card".

Virtual cards can be used in mobile payment just like a physical card. When paying with a virtual card, it is not the card number that is passed on to the retailer but merely the number generated (token).

2.2 Which mobile devices are compatible and which cards are authorised?

Compatible mobile devices include laptops, mobile telephones, smartwatches and fitness trackers, if they support the use of virtual cards and have been approved by the Bank. The Bank further decides which cards are authorised for which provider.

2.3 Activation and deactivation

For security reasons, the authorised card user must accept the terms of use of the respective mobile payment provider and acknowledge their data protection provisions before a card can be activated. The authorised card user is liable to pay compensation to the Bank for any losses arising from a breach of such terms/provisions.

Virtual cards can be used until the card is blocked or deactivated through the app by the authorised card user. Use of the card is subject to limitations pursuant to the specific terms and conditions applicable for certain cards. The authorised card user can terminate use of mobile payment at any time by removing their virtual card(s) from the relevant provider.

Costs incurred when activating and using virtual cards (e.g. costs for mobile internet use abroad) shall be borne by the authorised card user.

2.4 Use of the virtual card (authorisation)

Use of a virtual card is equivalent to an ordinary card transaction. Every use of a virtual card will be deemed authorised by the authorised card user.

The use of virtual cards shall be authorised in the manner specified by the provider or retailer (point of acceptance), e.g. by entering a device PIN code or by fingerprint or facial recognition. The authorised card user acknowledges that the risk of virtual cards being used by unauthorised persons may be increased in cases where any means of authorisation additionally required by the provider or retailer (device or card PIN code) consists of easily deduced combinations. The authorised card user acknowledges that, depending on the provider or retailer, no authorisation is required up to an amount to be specified by the provider or retailer. In all other respects, liability will follow clause 4 of these provisions.

2.5 Special duties to exercise due diligence

The authorised card user acknowledges and accepts that the use of mobile payment involves risks despite all security measures taken. In particular, it is possible for virtual cards and personal data to be misused or viewed by unauthorised persons. This can cause the authorised card user to incur financial losses due to card

501 0021 8.21

debits arising from misuse and to suffer violation of their personal rights from misuse of personal data.

The authorised card user must treat the devices used and the virtual cards with due care and ensure they are duly protected. In addition to the duties to exercise due diligence in accordance with the card terms and conditions applicable in each case and the due diligence and reporting obligations pursuant to clause I 3.2.1 and clause I 3.3 of these provisions, the authorised card user must comply with the following special duties to exercise due diligence:

- The devices used must be used according to the intended purpose and be kept in a way that it is protected from access by third parties.
- Like physical cards, virtual cards are personal and non-transferable. They must not be passed on for third parties to use (e.g. by storing fingerprints or by scanning the faces of third parties to unlock the device used).
- When changing or passing on a mobile device (e.g. if it is sold), each virtual card will have to be deleted in the provider's app and on the mobile device.
- Any suspicion of misuse of a virtual card or a device used for the same must be reported to the Bank without delay so that the corresponding virtual card can be blocked.

2.6 Warranty disclaimer

There is no entitlement to the use of mobile payment. The Bank may suspend or terminate use at any time in particular for security reasons or in the event of changes to the range of mobile payment offerings or a limitation of the authorised cards or compatible devices. Furthermore, the Bank is not responsible for the actions and offerings of the provider or other third parties such as internet and telephone service providers.

2.7 Using cards through the one app

Authorised card users who have a compatible device can activate their card(s) in the one app and use it/them as a virtual card. To ensure the security of mobile payment, the authorised card user must specify a PIN code on activation. The Bank may modify this service at any time. In all other respects, the present provisions for mobile payment, specifically the special duties to exercise due care pursuant to clause II 2.5 apply.

2.8 Date protection for mobile payment

The third-party provider and the Bank are independently responsible for their respective processing of personal data. The authorised card user acknowledges that personal data in connection with the offering and the use of mobile payment (specifically details of the authorised card user and activated cards and transaction data from the use of virtual cards) is collected by the third-party provider and is stored and further processed in Switzerland or other countries.

The processing of personal data by the third-party provider in connection with mobile payment and the use of offerings and services of the third-party provider including that provider's equipment and software is governed by these terms of use and data protection provisions. The authorised card user consequently confirms by each card activation that they have read and understood the data protection provisions of the respective third-party provider and they expressly consent to the corresponding data processing by the third-party provider. If the authorised card user does not wish such processing, the authorised card user is responsible for refraining from activating a card or communicating to the third-party provider their objection to processing. The processing of personal data by the Bank and the processor is subject to the data protection provisions at III below, the Bank's data protection statement and the terms of use for one.

III. Data protection statement for one

The following data protection provisions provide information on how the Bank processes personal data (or "data") as data controller. Processing includes all handling of personal data, including but not limited to the procurement, storage, use, disclosure or erasure of data. The Bank's data protection statement contains the contact details for information on data protection and data processing.

Upon registering for one, authorised card users expressly declare their consent to the forms of data processing mentioned in this data protection statement. Information on further instances of data processing in the course of the card relationship are contained in the respective card terms and conditions and the general and special provisions on the use of one. Furthermore, attention is hereby drawn to the global data protection statements of Visa and Mastercard® as well as the relevant enforcement rights of third-party beneficiaries.

1. Processing of personal data

1.1 What is the one data protection statement about?

Various online services attached to use of the issued cards are provided under the "one" name ("one digital services"). The provision of these services requires processing of authorised card user data by the Bank. The present data protection statement informs authorised card users about how data is processed when using one digital services.

501 0021 8.21

1.2 How is the data obtained?

1.2.1 What authorised card user data is made known?
When registering for one digital services and when logging into and administering the user account, the authorised card user may be asked to provide their email address, date of birth, mobile telephone number, card number and activation code.

1.2.2 What data is collected automatically?
- Data on use of the authorised card user's mobile devices such as manufacturer, type of device, operating system with version number, device ID, IP address
- Data on the use of computers and browsers as well as relating to internet access, such as type of device, operating system, IP address
- Data on use of the user account, such as Number of logins with date and time, changes made in the user account, acceptance of provisions on the use of one digital services and the data protection statement
- Data on the settings specified by the authorised card user, e.g. saving of username or login name
- Data on visits and usage of the website
- Data generated when using the app, such as updates or device information on usage, for example in the app or by SMS code

1.2.3 What information is collected in one when registering and activating the services?
- Information on the authorised card user and their cards registered for one that are saved in the user account
- Information as to the fact that 3-D Secure is used for the registered cards by means of confirmation in the app or by entering an SMS code
- Delivery address and mobile telephone number

1.2.4 What information is collected when using mobile payment?
- Information on the use of mobile payment, e.g. activation or deactivation of cards and use of the cards for mobile payment
- Information on the amount of a transaction
- Information on use of the card, timing of the transaction, type of verification
- When using a mobile payment solution from a third-party provider, the third-party provider can likewise collect and process personal data on the authorised card user. Depending on the offering in question, this may include, for instance, name, card number and, if applicable, transaction data. In this respect, the terms of use and the data protection provisions of the third-party provider should be noted.

1.2.5 What data is collected when using 3-D Secure?
- Information on the retailer, on the transaction and handling of the same as well as information on confirmation of the transaction with 3-D Secure
- Information in connection with the devices used for the transaction and confirmation
- Information in connection with access to the internet or mobile telephone network, such as IP address, name of the access provider

1.2.6 What data is collected when displaying the section of the map showing the location of the retailer?
- locations of retailers domiciled in Switzerland
- location data such as retailer name, place, country and line of business
- automated periodic Google inquiry to refine the retailer's location

1.3 For what purpose is personal data processed?

1.3.1 provision of services and handling of the card relationship
- facilitation of registration, login and use of one digital services by the authorised card user
- creation of a secure connection between one digital services and the authorised card user's mobile device
- transmission of confirmation requests, such as confirmation of online payments through one digital services, through push messages or SMS code sent to the authorised card user
- transmission of information on confirmations made to the Bank
- authentication of the authorised card user when performing actions. The app and/or the mobile device used are clearly assigned to the authorised card user during registration on one. This enables the Bank to ensure that confirmation was made in the registered app or with the registered mobile device
- communication with the authorised card user and transfer of information in connection with the card relationship or use of the card, such as information on new invoices, fraud activities provided through one digital services and the mobile device
- taking receipt of messages from the authorised card user
- displaying transactions and invoices
- handling of the card relationship with the authorised card user and the transactions performed with the card. In this respect, reference is made to the Bank's data protection statement and clauses I and II of these terms of use.

1.3.2 Mobile payment
- for making decisions on approval of the card for mobile payment
- for activating, deactivating and updating cards for mobile payment

501 0021 8.21

- for preventing misuse of the cards added
- for communicating with any third-party providers of a mobile payment solution within the scope of the present provisions and the provisions on use and data protection of the provider in question applicable in the relationship between the authorised card user and the third-party provider

1.3.3 Marketing
- for linking data with data already held by the Bank (also data from third-party sources)
- for creating individual customer, consumption and preference profiles that enable the Bank to develop and offer products and services for the authorised card user
- for transmitting to the authorised card user information on existing or new products and services provided by the Bank and third parties (advertising material)
- for the purpose of processing by the third-party provider within the scope of that party's terms of use and data protection provisions

1.3.4 Further purposes of data processing
- calculating credit and market risks relevant to the business
- improving security during use of services, e.g. reducing the risk of fraudulent transactions or misuse of devices or means of identification through phishing or hacking, etc.
- as evidence of actions and defence against claims made against the Bank
- improving the Bank's services and one digital services
- fulfilling statutory and regulatory requirements
- processing by the third-party provider for that party's own purposes within the scope of their terms of use and data protection provisions

1.4 Is data disclosed to other recipients?

1.4.1 Transmission to third parties and/or data collection by third parties

Third parties are individuals or companies that process data for their own purposes. This definition does not include service providers commissioned by the Bank. Subject to the following provisions, the Bank does not, in principle, forward any data – specifically no transaction data – in connection with cards for which the Bank's General Terms and Conditions and/or specific terms and conditions apply to third parties for their own purposes unless the authorised card user has consented to such forwarding or the third parties themselves request or arrange for such forwarding.

In particular, the Bank will not pass on any customer, consumption and preference profiles to third parties without the separate express consent of the authorised card user.

1.4.2 Further categories of third parties to whom data is disclosed
- Data (also transaction data) of an additional cardholder can be disclosed to the main cardholder.
- Data of authorised card users of "business cards", etc. may be made known to the company involved.
- At the request of authorities or on the basis of statutory obligations the Bank discloses data to government bodies such as law enforcement agencies or regulatory authorities and, where applicable, forwards data to the same.

1.4.3 Transmission of authorised card users' data to third parties through the use of mobile payment
- The card and transaction data required for handling the transaction are transferred via the servers of the card organisation during the payment process. Further information on data processing, forwarding of data and the involvement of third parties can be found in the separate card terms and conditions.
- When using mobile payment through a third-party provider, such third-party provider collects and processes data in accordance with that party's own terms of use and data protection provisions.

1.4.4 Electronic transmission of data

Data of the authorised card user may come into the possession of third parties (both in Switzerland and other countries) when using means of electronic data transmission, even without the Bank's involvement.

Especially when using the app and/or mobile devices, manufacturers of devices and software (e.g. Apple or Google) may receive personal data. These manufacturers can process and forward the data in accordance with their own terms of use and data protection provisions. This may bring about a situation where such third parties may be able to infer that there is a relationship between the authorised card user and the Bank. SMS messages are subject to the statutory provisions in place to monitor telecommunications traffic and are saved on the mobile telephone. This means that the corresponding information can come into the possession of third parties.

1.5 How is authorised card user data protected?

Information transmitted between the Bank, the processor and the app and/or mobile devices of the authorised card user (but not the sending of an SMS) is encrypted. Such communications with the authorised card user are, however, made through public communication networks. Such data is generally accessible by third parties, can get lost during transmission or be

501 0021 8.21

intercepted by unauthorised third parties. For this reason, it cannot be ruled out that third parties gain access to communications with the authorised card user when using one, despite all security measures taken. In addition, use of the internet means that data can be transmitted via other countries that may not offer the same level of data protection as Switzerland even if the authorised card user is in Switzerland.

Data security also depends on cooperation by the authorised card user. For this reason, the authorised card user must use the possibilities available to them to protect their devices and data. The minimum requirements on due diligence and notifications to be complied with in this respect are listed in clause I. Appropriate security measures increase security and reduce the risks associated with the use of one.

1.6 What rights do authorised card users have with regard to their data?

- Right to information on personal data held by the Bank and how the Bank processes the same
- Right to rectification of incorrect or incomplete personal data
- Right to erasure of personal data
- Right to restriction of data processing
- Right to file a complaint to the competent authority as to the way in which personal data is processed
- Right to object to, or revoke consent to the processing of personal data

The Bank can only grant the authorised card user's rights subject to compliance with statutory requirements. Even if consent, for example, is revoked, it is still possible for personal data to continue to be processed to the extent required by law.

1.7 For how long does the Bank store data?

The Bank stores data for as long as necessary for the purpose for which it was collected. The Bank further stores personal data if there is a legitimate interest in storage of such data, e.g. if the data is required to enforce or fend off claims, to safeguard IT security or periods of limitation are expiring. Thereafter, data is stored to comply with statutory and regulatory duties.

Version August 2021

501 0021 8.21

Basler Kantonalbank

Conditions governing use of the BKB Maestro card

I. General conditions

1. Types of usage (functions)

The BKB Maestro card can be used for the following functions:

- as a cash withdrawal card within Switzerland and abroad (cf. Clause II);
- as a payment card for the payment of goods and services within Switzerland and abroad (cf. Clause II)
- for deposit services provided by the bank (cf. Clause III).

2. Place of use

The BKB Maestro cards can normally be used within Switzerland and Europe. To use the BKB Maestro card outside these regions, the BKB Maestro card needs to be released by the Bank as required. The release is possible for a maximum of two months. Then the card will automatically be reset to the standard settings. In justified cases the release can be extended. BKB reserves the right to itself expand or restrict the approved territory and the duration of the release at any time.

3. Account linkage

The BKB Maestro card is always linked to a specific account (hereafter referred to as the "account") at the issuing bank (hereafter referred to as Bank).

4. Authorized card holders

Persons authorized to use the card can be the account holder, persons authorized to use the account or third parties specified by the account holder. The BKB Maestro card is always issued in the name of the authorized card holder.

5. Ownership

The BKB Maestro card remains the property of the bank.

6. Fee

For the issuing of the BKB Maestro card and the authorization thereof, as well as for the processing of transactions conducted with it, the bank can charge the account holder fees, which are to be notified in an appropriate form. These fees will be debited from the account upon which the BKB Maestro card has been issued.

7. The authorized card holder's duty of care

The authorized card holder specifically undertakes to fulfil the following duties of care:

a) Signature

Upon receipt of the BKB Maestro card it is to be immediately signed by the authorized card holder in the space provided.

b) Storage

The BKB Maestro card and the PIN (Personal Identification Number) are to be stored with particular care and separate from one another.

c) Keeping the PIN secret

The PIN is to be kept secret and may not be revealed by the authorized card holder to any other person. In particular, the PIN may neither be noted upon the BKB Maestro card nor recorded in any other manner, or in an altered form, nor stored together with the BKB Maestro card.

d) Changing the PIN

PIN numbers changed by the authorized card holder may not consist of easily determined numerical combinations (such as a telephone number, date of birth, car licence plate number).

e) Transferring the BKB Maestro card

The authorized card holder may not give their BKB Maestro card to third parties nor make it accessible to such in any way.

f) Reporting in case of loss

If the BKB Maestro card or the PIN are lost, or if the BKB Maestro card is left behind in a machine, the specific unit indicated by the bank is to be notified immediately (cf. Clause II.5 and Clause II.10).

g) Control obligation and reporting of discrepancies

The account holder undertakes to check the relevant account statement upon receipt and to report any discrepancies, particularly debits due to misuse of the card, to the bank immediately, but by no later than within 30 days of receipt of the account statement of the respective billing period. The loss report form and the declaration of waiver are to be returned to the bank completed in full and duly signed within 10 days of its receipt.

h) Reporting to the police

In the case of criminal offences, the authorized card holder must report the matter to the police. The card holder must assist in any investigation and contribute to minimization of the loss to the best of their ability.

8. Coverage obligation

The BKB Maestro card may only be used if sufficient coverage exists in the account (credit or an approved overdraft limit). The bank is entitled to decline transactions if the necessary balance is not available in the account.

600 9676 12.18

9. Bank's right to debit
The bank is entitled to debit all amounts resulting from the use of the BKB Maestro card (according to Clause I.1) from the account (cf. Clause II.5).

The bank's right to debit also remains in unlimited force in the case of disputes between the authorized card holder and third parties.

Amounts in foreign currencies will be converted to the account currency.

10. Period of validity and card renewal
The BKB Maestro card is valid until the end of the year stated thereon. If the account is conducted properly and if there is no express cancellation by the authorized card holder, the BKB Maestro card will be automatically replaced with a new BKB Maestro card prior to the end of the year indicated on the card.

11. Cancellation
The BKB Maestro card can be cancelled at any time. The withdrawal of authorization (as in Clause I.4) has the same effect as a cancellation.

Once notification of cancellation has been made, the BKB Maestro card must be immediately, and without request, returned to the bank.

No claim can be made for refunding of the annual fee upon premature confiscation or return of the card.

Despite cancellation, the bank remains entitled to debit all amounts from the account which are based on card transactions that have been made before the effective return of the BKB Maestro card.

12. Modification of conditions and prices
The bank reserves the right to modify these conditions and prices at any time. Modifications will be notified in an appropriate form and are considered accepted if the BKB Maestro card is not returned before the modifications come into effect.

13. Terms and Conditions
Furthermore, the Bank's Terms and Conditions are applicable.

II. BKB Maestro card as a cash withdrawal and payment card

1. Cash withdrawal function
The BKB Maestro card can be used, at any time, together with the PIN to withdraw cash from ATMs marked accordingly in Switzerland and abroad or by signing the transaction voucher at providers identified accordingly, up to the limits set for the BKB Maestro card.

2. Payment function
The BKB Maestro card can be used together with the PIN to pay for goods and services in Switzerland and abroad, or by signing a transaction slip or simply by using the card (for example in parking garages, at motorway toll stations or for contactless payment) at correspondingly identified vendors, up to the limits set for the BKB Maestro card.

3. PIN
In addition to the BKB Maestro card, the authorized card holder will be sent a PIN in a separate, sealed envelope. This consists of a machine-calculated, 6-digit PIN which is known neither to the Bank or third-parties. If several BKB Maestro cards are issued, each BKB Maestro card will have its own PIN.

4. Changing the PIN
The authorized card holder is advised to select a new PIN with a minimum of 4-digits and a maximum of 6-digits at suitably equipped ATMs, which will immediately replace the previously valid PIN. For reasons of security, a 6-digit PIN should be selected. This can be changed at any time and as often as desired. To further protect the BKB Maestro card against misuse, the PIN chosen should not consist of easily determined numerical combinations (cf. Clause I.7(d)), nor should it be stored with the BKB Maestro card, nor should it be noted on the BKB Maestro card, nor in any other manner, also not in an altered form.

5. Authorization, debiting and risk assumption
Each person who authorizes the use of the BKB Maestro card through
- entering the PIN
- signing the transaction sales slip, or
- contactless payment,

is regarded as being entitled to withdraw cash or to pay for goods or services with the BKB Maestro card; this also applies if this person is not the authorized card holder. Correspondingly, the bank is entitled to charge all the amounts authorized in this way. The risks arising from misuse of the BKB Maestro card are thus assumed by the account holder.

6. Assumption of loss in the absence of fault
Assuming that the authorized card holder has adhered to the conditions governing the use of the BKB Maestro card in all aspects (particularly the duties of care according to Clause I.7) and if they are otherwise not at fault, then the bank assumes losses incurred by the account holder as a result of the misuse of the BKB Maestro card by third parties in its function as a cash withdrawal or payment card. This also includes losses due to counterfeiting or forgery of the BKB Maestro card. Not considered to be "third parties" are the authorized card holder, their partner and persons living with them in the same household.

600 9676 12.18

Losses that are covered by the indemnity liability of an insurance company, as well as all consequential losses of any kind, are not assumed.

7. Technical malfunctions and operational breakdowns
The authorized card holder has no claim to compensation if use of the BKB Maestro card for cash withdrawal or payment function is not possible due to technical malfunctions and operational failures.

8. Limits
The bank sets the usage limit for each BKB Maestro card issued and informs the account holder thereof in an appropriate manner. It is the responsibility of the account holder to inform any authorized persons regarding the usage limit.

9. Transaction receipt
For cash withdrawals, the authorized card holder receives a transaction receipt upon request at most ATMs, automatically or upon request when paying for goods and services. The bank does not issue any debit notices.

10. Blocking
The bank is entitled to block the BKB Maestro card at any time, without previous notice to the authorized card holder and without providing reasons.

The bank will block the BKB Maestro card upon request of the authorized card holder, his notification of the loss of the BKB Maestro card and/or the PIN, as well as cancellation by the same. Authorized card holders without account authorization can only block BKB Maestro cards issued in their name.

The blocking can only be requested from the specific unit indicated by the bank. The bank is entitled to debit the account for use of the BKB Maestro card before the blocking takes effect within the period of normal business. The account can be charged for costs associated with the blocking. The blocking will only be removed upon permission being provided by the account holder to the bank.

III. BKB Maestro card for deposit services

The BKB Maestro card can be used for the deposit of notes and coins at the ATMs intended for this. The amount recognized by the ATM and confirmed by the depositor to the automat will be credited automatically to the account listed on the BKB Maestro card or the account linked via the multifunction and selected at the ATM, less the fee specified in the fee schedule, at the value of the deposit date.

The credit is made regardless of the relationship between the depositor and the account holder, if these are not identical. The depositor's right of revocation expires with the acceptance of the amount by the ATM.

600 9676 12.18

Basler Kantonalbank

Conditions governing use of the BKB bank card

I. General conditions

1. Types of use (functions)

The BKB bank card can be used for the following functions:

- As cash withdrawal card at automatic teller machines (ATMs) at BKB (hereafter referred to as the Bank) (cf. Clause II)
- For deposit services provided by the bank (cf. Clause III)
- For account balance and transaction inquiries.

2. Account linkage

The BKB bank card is always linked to a specific account (hereafter referred to as the "account") at the card-issuing bank. The bank determines for which types of account a bank card is issued.

3. Authorized card holders

Persons authorized to use the card can be the account holder, persons authorized to use the account, or persons designated by the account holder. The BKB bank card is always issued in the name of the authorized card holder.

4. Ownership

The BKB bank card remains the property of the bank.

5. Fee

For issuing and authorization of the BKB bank card and processing of transactions conducted with the card, the bank can charge the account holder fees, which shall be notified in appropriate form. These fees will be debited to the account upon which the BKB bank card is issued.

6. The authorized card holder's duty of care

The authorized card holder specifically undertakes to fulfill the following duties of care:

a) Signature

Upon receipt of the BKB bank card, it shall be signed immediately by the authorized card holder in the space provided.

b) Storage

The BKB bank card and the PIN (Personal Identification Number) shall be stored with special care and separately from one another.

c) Keeping the PIN secret

The PIN shall be kept secret and may not be revealed by the authorized card holder to any other person. In particular, the PIN may neither be noted on the BKB bank card or recorded in any other manner, even in modified form, nor stored together with the BKB bank card. The PIN shall always be entered in such manner as to keep it secret.

d) Changing the PIN

PIN numbers changed by the authorized card holder may not consist of easily determined numerical combinations (such as telephone number, date of birth, car licence plate number, etc.).

e) Transferring the BKB bank card

The authorized card holder may not give the BKB bank card to third parties, nor make it accessible to such persons in any way.

f) Reporting in case of loss

If the BKB bank card or the PIN is lost, or if the BKB bank card is left behind in an ATM, the specific unit indicated by the card-issuing bank shall be notified immediately (cf. Clause II.4 and II.9).

g) Checking obligation and reporting of discrepancies

The account holder shall undertake to check the relevant account statement upon receipt and to report any discrepancies, particularly debits due to misuse of the card, to the bank immediately, but no later than 30 days following receipt of the account statement for the respective billing period. The loss report form and the declaration of waiver shall be returned to the bank completed in full and duly signed within 10 days of its receipt.

h) Reporting to the police

In the case of criminal offenses, the authorized card holder shall report the matter to the police. The card holder shall assist in any investigation and contribute towards minimization of the loss to the best of their ability.

7. Coverage obligation

The BKB bank card may be used only if there is sufficient coverage in the account (credit or approved overdraft limit). The bank shall be entitled to decline transactions if the necessary balance is not available in the account.

8. Bank's right to debit

The bank shall be entitled to debit all amounts resulting from the use of the BKB bank card (according to Clause I.1) from the account (cf. Clause II.4).

9. Cancellation

The BKB bank card can be cancelled at any time. The withdrawal of authorization (as in Clause I. 3.) has the same effect as a cancellation. Once notification of cancellation has been made, the BKB bank card must be immediately, and without request, returned to the bank. Despite cancellation, the bank shall remain entitled to debit all amounts from the account based on transactions that were made before the effective return of the BKB bank card.

600 9676 12.18

10. Amendment of conditions and prices
The bank reserves the right to amend the conditions and prices at any time. Amendments shall be notified in an appropriate form and are considered accepted if the BKB bank card has not been returned before the amendments come into effect.

11. Terms and Conditions
Furthermore, the Bank's Terms and Conditions are applicable.

II. BKB bank card as a cash withdrawal card

1. Cash withdrawal function
The BKB bank card can be used together with the PIN at any time for the withdrawal of cash at automatic teller machines (ATMs) of BKB up to the limit set for the card.

2. PIN
The PIN will be sent separately in a sealed envelope to the authorized card holder. This consists of a machine-calculated 6-digit PIN unique to the card
and known neither to the bank nor to third parties. If multiple BKB bank cards are issued, then each BKB bank card receives its own PIN.

3. Changing the PIN
The authorized card holder is advised to select a new 4–6 digit PIN at a suitably equipped BKB automatic teller machine (ATM), which will immediately replace the previously valid PIN. For security reasons, a 6-digit PIN should be selected. This can be changed at any time and as often as desired. To further protect the BKB bank card, the PIN chosen should not consist of easily determined numerical combinations (cf. Clause I.6 (d)), nor should it be noted on the BKB bank card or recorded in any other manner, even in an altered form, or stored together with the BKB bank card.

4. Authorization, debiting, and risk assumption
Any person who authorizes the use of the BKB bank card by entering the PIN is regarded as being entitled to withdraw cash with the BKB bank card; this also applies if this person is not the authorized card holder. Correspondingly, the bank is entitled to charge the amount authorized in this way. The risks arising from misuse of the BKB bank card are thus assumed by the account holder.

5. Assumption of loss in the absence of fault
Assuming that the authorized card holder has adhered to the conditions governing the use of the BKB bank card in all aspects (particularly the duties of care according to Clause 1.6) and if they are otherwise not at fault, then the bank can, after individual case examination, assume all or part of the losses incurred by the account holder as a result of the misuse of the BKB bank card by third parties. This also includes losses due to counterfeiting or forgery of the BKB bank card. Not considered to be "third parties" are the authorized card holder, his or her partner, and persons living with either partner in the same household. Losses that are covered by the indemnity liability of an insurance company, as well as all consequential losses of any kind, shall not be assumed.

6. Technical malfunctions and operational breakdowns
The authorized card holder has no claim to compensation if use of the BKB bank card is not possible due to technical malfunctions and operational failures.

7. Limits
The bank sets the usage limit for each BKB bank card issued and informs the account holder thereof in appropriate manner. It is the responsibility of the account holder to inform any authorized persons regarding the usage limit.

8. Transaction receipt
For cash withdrawals, the authorized card holder receives a transaction receipt upon request at automatic teller machines (ATMs). The bank does not issue any debit notices.

9. Blocking
The bank shall be entitled to block the BKB debit card at any time, without previous notice to the authorized card holder and without providing reasons. The bank shall block the BKB bank card upon request of the authorized card holder, his or her notification of the loss of the BKB bank card and/or the PIN, and cancellation by the same.

The blocking can be requested only from the specific unit indicated by the bank. The bank shall be entitled to debit the account for use of the BKB bank card before the blocking takes effect within the period of normal business. The account can be charged for costs associated with the blocking. The blocking shall be removed only upon permission being granted by the account holder to the bank.

III. BKB bank card for deposit services

The BKB bank card can be used for the deposit of notes and coins at the automatic teller machines (ATMs) provided for the purpose. **The amount recognized by the automatic teller machine (ATM), and confirmed by the depositor to the automatic teller machine (ATM) will be credited automatically to the account listed on the BKB bank card or the account linked via the multifunction and selected at the automatic teller machine (ATM) of the bank, less the fee specified in the fee schedule, at the value of the deposit date.**

The credit is made regardless of the relationship between the depositor and the account holder, should both parties not be identical. The depositor's right of revocation expires with the acceptance of the amount by the automatic teller machine (ATM).

600 9676 12.18

Basler Kantonalbank

Conditions for E-Banking

1. E-Banking Services

1.1 The services offered by Basler Kantonalbank (hereinafter referred to as the Bank) in E-Banking are described in the "Information on E-Banking". This forms an integral part of these conditions. The "Information on E-Banking" can be accessed on the bank's website on the appropriate login page for E-Banking. The Bank reserves the right to amend these at any time.

1.2 Payment and stock exchange orders cannot be performed round the clock. Transaction times are given in the "Information on E-Banking".

1.3 The data exchange provided for in these conditions relates to banking business which is based on separate agreements or terms of business. The following provisions take precedence over any differing conditions in the said agreements or terms of business in the terms of reference of the services via E-Banking requested by the Client.

1.4 With use of the service "E-Documents," bank documents for bank/custody accounts are delivered to the Client and/or the user electronically via E-Banking. Existing postage or archiving instructions are superseded, whereby, for example, bank/custody account statements, notices from the payment transactions, stock exchange trading invoices, and other notices/communications (hereinafter referred to as bank documents) are made available only electronically instead of in paper form within the scope of E-Banking to the person receiving the "E-Document" service. Final account settlement statements and tax certificates will continue to be issued by post. **The Bank's obligations of reporting and accountability to the Client are thereby fulfilled.**

2. User/login process/means of identification

2.1 Access to E-Banking is received by users who authenticate themselves by input of the means of identification as a part of the selected login process valid for these services. Users are defined as those persons authorized by the Client for use of E-Banking in the E-Banking agreement (i.e., the Client and/or authorized persons/users).

2.2 Required as means of identification for the use of E-Banking are:

a) the identification number provided to the user by the Bank;

and

b) the personal, freely selected password of the user;

and

c) an additional single-use code, which is sent contemporaneously in accordance with the relevant login process selected by the user, and after entering the valid identification number and the valid password must be entered or confirmed. The requirement of entering an additional code can be dispensed with according to the login process selected, for example, the use of a software certificate (SoftCert).

The individual login process made available by the Bank can also be amended according to the changed state of technology over the course of time and it will be described on the Bank's website and, if applicable, in the specific product or other documentation.

The Bank reserves the right to cancel existing login processes and introduce new ones, which can supplement or replace those described above.

2.3 Whosoever authorizes himself as per Number 2.2 (self-identification) applies as the authorized person vis-à-vis the Bank for use of E-Banking services as well as other electronic channels of the Bank, access to which requires relevant login.

The Bank may accordingly allow him within the scope and extent of the services and type of authorization selected in the E-Banking agreement by the Client, regardless of its legal relationship to the Client, unless they are identical, and irrespective of entries in the Commercial Register, publications or rules in the signature documents, as well as without further examination of their authorization and irrespective of the legal relationship of the Bank to the Client, to make inquiries, dispositions, refer electronically to documents as well as allow them to use other functions in the electronic channels of the bank, which are enabled through access to E-Banking login. It is also entitled to accept orders and legally binding notifications from them and to execute these.

2.4 The Bank has the right at any time and without stating reasons to refuse the provision of E-Banking services and to require that the user prove his identity in another form (e.g. by signature or personal appearance).

2.5 The Client accepts without reservation all transactions posted within the scope of the agreed E-Banking services by the user under use of hisr means of identification. Likewise, all instructions, orders and notifications which reach the Bank by this means are deemed to be given and authorized by the Client and electronically provided documents as rightfully retrieved from the authenticated user.

601 0352 1.20

3. Duties of care of the Client/user

3.1 The user undertakes to change the initial password assigned by the Bank immediately after receipt and to change it regularly thereafter. Passwords should not consist of easily determined combinations (such as telephone numbers, dates of birth, car licence plate numbers, etc.).

3.2 If the user receives any activation and/or verification codes for E-Banking services, then he is obligated to perform the activation and/or verification without delay and according to the instructions provided.

3.3 The user undertakes to ensure that all means of identification are kept secret and protect them against improper use by unauthorized persons. In particular, the password must not be recorded or stored without protection on the end device (such as a computer, laptop, tablet, or mobile telephone) or otherwise recorded. Likewise, the means of identification must not be disclosed or otherwise made available to third parties. In particular, he acknowledges that the Bank will never request by email that he provide his means of identification for E-Banking in any data entry screen or to send it in any way to the bank or to any other recipient.

3.4 The Client bears the risks which arise from use (including misuse) of his means of identification or those of the authorized persons unless the Bank fails to act with normal business due care.

Should damage or other detriment occur, without the Bank or the Client or user violating its or his duty of care, the party in whose sphere of influence the cause of the damage or the damaging act lies shall also be liable. The bank assumes no liability for damage or other detriments from transmission errors, technical problems and illegal interference with the devices or software of the user.

3.5 If there is cause for suspicion that unauthorized third parties have gained knowledge of one or more means of identification of an authorized user, the user must change or modify the relevant means of identification immediately. If this is not possible, he must immediately request that access to the relevant services be blocked, or block access to the services himself, by undertaking the appropriate steps on the relevant websites of the Bank or by proceeding in accordance with Number 5.1 of these conditions.

3.6 If there is cause for suspicion that unauthorized third parties have gained access to the end device of the user (for example, in the case of loss or theft of the end device), the user is also obligated to contact without delay the Bank's hotline service by telephone during the support times published on the websites of the Bank.

3.7 The user is required to examine all data entered by him for completeness and correctness. Responsibility concerning data communicated by the user remains with the Client.

4. Exclusion of liability of the Bank and its employees

4.1 The Bank accepts no guaranty for the completeness and correctness of data displayed by it in E-Banking. In particular, details of bank accounts and custody accounts (balances, statements, transactions, etc.) as well as generally accessible information, such as stock-exchange prices and currency rates, are deemed to be non-binding. Such data do not constitute a binding offer unless they are explicitly designated as such. Authoritative are the details in the statements and documents of the bank, which were delivered to the Client in paper form or electronically.

4.2 The Bank does not arrange technical access to its services. This is the sole responsibility of the user. More particularly, they acknowledge that the Bank does not distribute the special software necessary for internet access and for the use of E-Banking nor does the Bank support the user in respect of software or hardware problems. The Bank accordingly accepts no guarantee for either the network operator (service provider) or for any necessary software.

4.3 Data transactions are conducted over public telecommunications networks not specially protected (telephone, Internet, etc.). The Bank excludes liability for losses arising from use of these networks. More particularly, the Bank accepts no liability for any losses incurred by the Client/user as a consequence of communication faults, technical defects, interruptions in the telephone network or the internet, illegal tampering with network installations, overloading in the networks, wilful blocking of electronic access by third parties, breakdowns or other deficiencies on the part of the network operator.

4.4 In spite of all security measures, the Bank cannot accept any liability for the end device of the user, as this is not possible from a technical standpoint (concerning risks cf. Number 8).

4.5 Furthermore, the Bank expressly excludes liability for any software recommended or supplied by it (for example, via CD, download, or apps), as well as the consequences arising from and during transfer of the software via the Internet.

601 0352 1.20

4.6 The Bank, subject to the application of the customary degree of care, accepts no liability for the consequences of faults and interruptions, more particularly in operating E-Banking services (for example, caused by illegal access to the system).

4.7 The Bank reserves the right at any time to interrupt E-Banking for the protection of the Client/user on discovery of security risks, until their elimination. The Bank accepts no liability for any losses arising from such an interruption.

4.8 If orders are defectively or incorrectly not executed or not executed in time and losses are incurred, the Bank is liable at most for the loss of interest (does not apply to stock exchange orders).

5. Blocking

5.1 The Client can have his own access or that of users authorized by him to the E-Banking services blocked. Blocking can only be requested during the times stipulated in the "Information on E-Banking". The Bank can require additional confirmation of the block in writing. The user can also block access to the services in E-Banking himself at any time by entering an incorrect password or an incorrect additional code three times in a row if the login process used by him requires entering an additional code.

5.2 The Bank can require removal of a block requested by the Client or a user be applied for in writing.

5.3 The Bank may likewise block access of the user to individual or all services at any time without stating reasons and without prior termination of the E-Banking agreement if this in its own judgment shall appear to be indicated for objective reasons.

6. Power of attorney conditions

Entitlement of a user to the use of E-Banking services is valid until written revocation addressed to the Bank. The deletion or amendment of the power of attorney or signing rights of the authorized persons pursuant to the signature documentation lodged with the bank or the deletion or amendment of the signing rights of a user in the Commercial Register does not automatically bring about the revocation of their authorization for the use of E-Banking.

In the event of death and possible loss of legal capacity of the Client, the authorization granted does not automatically expire.

7. Financial assistant

7.1 The Bank makes a financial assistant available. This represents a service as a part of the Bank's E-Banking or of the Bank's electronic channels. The financial assistant supports the Client in the management of his personal finances.

7.2 In the framework of the financial assistant, account transactions and, insofar as explicit approval has been given for this as a part of E-Banking or the digital channels of the Bank, credit card transactions as well as data recorded from the Client will automatically be assigned to specified categories. The Client can always modify the assignment.

7.3 The confidentiality of the Client data is always safeguarded. No data which permit conclusions about a specific person, will be forwarded to third parties.

7.4 The Client can at any time deactivate the financial assistant in settings or can at any time revoke agreement to the inclusion of credit card data. At its own discretion, the Bank can temporarily or permanently discontinue the service.

8. Security in E-Banking

8.1 The Client acknowledges that the data are carried through an open network, the internet, which is accessible to everyone. The data are therefore regularly and without control transferred across borders. This also applies to data transfer where the sender and the recipient are both located in Switzerland. Although the individual data packages are transferred in an encoded form, the sender and the recipient on the other hand remain in each case unencoded and can also be read by third parties. Consequently, a conclusion may be drawn by a third party as to an existing banking relationship.

8.2 Special importance was attached to security in the development of E-Banking. A multi-step security system was developed for the security of the Client/user, which, among other things, makes use of cryptographic procedures of a very high technical standard. In principle, because of the encoding, it is not possible for any unauthorized person to view confidential Client data. However, absolute security cannot be guaranteed either by the Bank or by the Client, even with security precautions meeting the highest, most technically advanced standards. The Client/user acknowledges in particular that his end device constitutes the weak link in accessing E-Banking. Regular updates to the software (e.g. the operating system) of the end device is the responsibility of the user.

8.3 The Client/user acknowledges in particular the following risks:

- Insufficient knowledge of the system and deficiencies in system precautions may facilitate unauthorized access (for example, insufficiently protected

601 0352 1.20

data storage on the hard disk, file transfers, screen radiation, etc.). It is incumbent upon the Client/user to inform himself of the necessary security precautions.
- Nobody can exclude the creation of a user profile by the user's internet provider; that is, this provider has the means to trace with whom the user is in contact and when.
- There is a permanent risk that a third party may gain access unnoticed to the user's end device during use of the internet (for example, through a Java or ActiveX application).
- There is a permanent risk that malware (such as computer viruses) may be spread in the user's end device by use of the internet, given the end device's contact with outside systems either through computer networks or other data carriers.
- It is expected that the user works only with software procured from a trustworthy source.
- Changes to the operating system of the user's end device (such as jailbreaking, rooting) can make it easier to gain unauthorized access.

9. Import and export restrictions

9.1 The Client/user of E-Banking acknowledges that in some circumstances he may be infringing the provisions of foreign law by using E-Banking outside Switzerland. It is the Client's/user's responsibility to seek information on this point. The Bank shall accept no liability in this respect.

9.2 The Client/user acknowledges that there may be import and export restrictions regarding encoded algorithms, which, if applicable, may be infringed when using E-Banking services in or from another country.

10. Client data and marketing

The Client/user agrees to the use by the Bank of Client or user data from E-Banking for internal marketing purposes. Regarding the handling of Client data, reference is made to the "Terms and Conditions" and the "Privacy Statement" of the Bank. This can be viewed on the Bank's website at www.bkb.ch/privacy-statement.

11. Termination

Agreements for E-Banking can be terminated in writing at any time by the Client and the Bank. The Bank is entitled at its own discretion to cancel existing agreements for E-Banking and thus access to the E-Banking services without prior notice or subsequent notification to the Client, if there has been no access made within one year from the conclusion of the agreement or it has no longer been used for more than one year.

12. Reservation of particular statutory provisions

Any statutory or other provisions regulating the operation and use of the internet remain reserved and apply to existing agreements for E-Banking from their commencement.

13. Terms and Conditions

13.1 The Bank's Terms and Conditions also apply to the use of bank services in E-Banking.

14. Partial invalidity

The invalidity, illegality or unenforceability of individual or more provisions contained in these conditions shall not affect the validity of the remaining contractual provisions.

15. Amendment of the conditions for E-Banking

The Bank may amend the conditions for and the offering of E-Banking at any time. It shall notify the Client/user in a suitable way. Amendments shall be deemed to be approved if the Client/user does not make representations on the amendments to the conditions and/or services within a period of one month following notification.

16. Mobile Banking

The above conditions for E-Banking also apply to Mobile Banking services. Any variations arise from the conditions in the "Information on E-Banking".

Version: January 2020

601 0352 1.20

Basler Kantonalbank

Special conditions for SEPA transactions

The following conditions apply to the relationship between the Client and Basler Kantonalbank (the Bank) for domestic and cross-border transfers in Euro within the framework of the SEPA Payment Transactions Standards (SEPA – Single Euro Payments Area). These conditions apply in addition to the Terms and Conditions of the Bank, as well as – if the relevant services are used – the regulations applicable for payment transactions such as relevant to BKB-E-Banking.

1. Information required in the payment order

To transfer funds to a different institution as a SEPA payment, this order must be submitted electronically and the payer must provide the Bank with the following information:

- Payer:
  - IBAN (International Bank Account Number) or the payer's account number
  - First name and last name, or company name
  - Residential address / company address
  - Post code / city or town
- Recipient:
  - BIC of the payee's bank
  - Information on the payee's bank
  - IBAN of the payee's account
  - First and last name, or company name
  - Residential address / company address
  - Post code / city or town
- Transfer amount in Euro
- Desired payment date
- Fee regulation: fee splitting; i.e., the payer and the payee each pay the fee charged by their respective financial institution
- "SEPA" should be entered in the field "Instructions to the Bank". Any other entries are not permitted and will not be taken into consideration. If "SEPA" is not entered, the Bank is nevertheless authorized, though not obligated, to carry out the order as a SEPA order.

In case of a collective order, the above requirements must be met for each individual payment order, otherwise the entire collective order may be declined.

The Client acknowledges that even when all of the above information has been provided the transaction can be carried out as a SEPA payment only if the payee's bank is also a SEPA participant.

2. Processing or declining of the payment order

The Bank is authorized but not obligated to process the payment order despite deficient or incomplete information pursuant to the above Item 1, if the Bank can correct the deficiency or supply the missing information without any uncertainty.

If the desired payment date falls on a Saturday, a Sunday, or a public holiday, the Bank is authorized to post the transaction on the next banking workday. The Client acknowledges further that posting of credits to the payee's account may also be delayed due to international regulations relating to banking workdays and public holidays.

If one or more of the requirements stated above in Item 1 are not met and for this reason the payment order is not processed or is rejected by a party involved in the transfer of funds (e.g. by a clearing centre or the payee's financial institution) after the account has been debited, the Bank will notify the Client within a meaningful timeframe and in appropriate form of the reason for the non-fulfilment or rejection of the transfer and will at the same time credit the transferred amount to the account if it was already debited.

If the Bank can correct the reason for the rejection of the payment order on its own, it is authorized to do so without first consulting with the payer; however, the Bank is not obligated to re-process the payment order.

3. Credit or retransfer of received payments

Incoming payments are credited to the account in accordance with the IBAN named in the payment order. If a posting date falls on a Saturday, a Sunday, or a holiday, the Bank is authorized to post the credit on the next banking workday.

Upon receipt of the payment the Bank is authorized to deduct the relevant fees from the amount received before posting the credit.

Incoming payments for which no IBAN or a non-existent IBAN is named, or where other reasons prevent a credit (particularly statutory or regulatory requirements, official dispositions, or a closed account) will be retransferred to the payer's financial institution.

In connection with such a retransfer, the Bank is authorized to advise all parties involved with the transaction (including the payer) as to the reason why the credit could not be processed.

4. Waiver of data comparison at posting of credit

As payee, the Client agrees that the transfer amount is credited solely on the basis of designated IBAN without comparison of the account number and the payee's name and address.

The Bank reserves the right to make such comparison at its discretion and to decline the payment if the data do not match, in which case the Bank is authorized to advise the payer's financial institution that the data do not match.

600 9676 12.18

As payer, the Client agrees that the payee's financial institution credits the amount based solely on the designated IBAN without comparison of the account number and the payee's name and address. The payee's financial institution can also reserve the right to make this comparison at its discretion and to decline the payment order if the data do not match.

5. Currency conversion/currency risk

If the account of a Client that is to be credited or debited in accordance with the IBAN of a payment order is not a euro-denominated account, the Bank is nevertheless authorized to perform the debit or credit, even if the Client holds a euro-denominated account at the Bank under different IBAN.

The conversion into or from Euro in the currency of the account to be debited or credited is effected at the exchange rate on the date received or the date of processing.

All currency risk (e.g. in case of a recredit after rejection/retransfer in accordance with Items 3 and 4 above) is borne by the Client.

6. Data processing / transfer

The Client (as payer) agrees that his/her data, in particular name, address, IBAN, and other information in accordance with Item 1a above will be disclosed in the processing of domestic and cross-border payment orders to the involved banks (particularly the Bank's domestic and foreign correspondent banks), operators of payment transaction systems (such as Swiss Interbank Clearing) or SWIFT (Society for Worldwide Interbank Financial Telecommunication), and the domestic and foreign payees. The Client further agrees that all parties involved in the transaction in turn can disclose the data to authorized third parties in other countries for further processing or for data security purposes.

The Client acknowledges further that the data that are disclosed in foreign countries are no longer protected under Swiss law, but instead are subject to the laws of the respective foreign country and that the laws and official dispositions of that country may require disclosure of the data to authorities or other third parties.

7. Effective date and changes to the conditions

The Bank reserves the right to make changes to these conditions at any time. Such changes will be disclosed to the Client by written communication or in other appropriate form and will be considered approved by the Client if not contested in writing within one month after disclosure, or at the latest after issuing of the next payment order to be processed under SEPA.

600 9676 12.18

Basler Kantonalbank

Important information regarding international payment transactions

Dear Client,

As a member of the FATF (Financial Action Task Force on Money Laundering), Switzerland has adopted the FATF principles on the prevention of money laundering and terrorist financing, as laid down, for example, in the Swiss Federal Banking Commission Money Laundering Ordinance. In this context, the European Union (EU), for example, has specifically required the disclosure of the name, address and account number of any person who gives instructions for money to be transferred to a bank with its registered office in the EU.

The present information is to advise you that Basler Kantonalbank (BKB) is meeting these obligations and what this means for you as a Client in relation to payment transactions.

In order to comply with these rules and maintain an efficient payment infrastructure, BKB must specifically provide the remitter's name, address and account number when making international payments and payments in foreign currencies. Payment orders which do not include these details will no longer be accepted by banks in EU member states or in many countries outside the EU. Under certain circumstances, this information may also be required in future for payment transactions within Switzerland.

The information referred to above will be communicated to the banks and systems operators involved in processing your financial transactions. Most of these institutions will be BKB correspondent banks in Switzerland and abroad and operators of payment and securities settlement systems such as SWIFT (Society for Worldwide Interbank Financial Telecommunication), SIX SIS AG or also SIX Interbank Clearing, in so far as Swiss payment transactions are affected in future.

In most cases the beneficiary will also receive the remitter's details. In exceptional circumstances, for example involving payments in foreign currency, the possibility cannot be ruled out that even transactions within Switzerland may be processed using international channels and that data will therefore leave the country. It is also possible that the banks and systems operators involved in the transaction themselves transmit data to appointed third parties in other countries for further processing or storage.

If your remitter data is transferred abroad it is no longer protected by Swiss law. Foreign legislation and instructions from official bodies may require this information to be passed on to the authorities or other third parties.

We hope you will appreciate that BKB is obliged to comply with the applicable regulatory requirements and thank you for your understanding in this matter.

If you have any questions, please do not hesitate to contact BKB-Welcome at +41 (0)61 266 33 33.

Best regards
Basler Kantonalbank

Hint: Please be sure to provide the IBAN (beneficiary's international bank account number) and BIC (beneficiary's bank identifier code) for all your payment transactions into the IBAN countries. This will allow your payment transaction to be processed automatically, i.e. without additional charges.

600 9676 12.18

Basler Kantonalbank

Conditions for electronic communication

The use of electronic channels of communication (email or text message) chosen by the Client with his/her confirmation for electronic communication and the exchange of information via these channels are subject to the following provisions:

1. The Client authorises the Bank, without any additional verification of legitimacy, to communicate via the unsecured communication channel ('permitted communication channel') chosen with a confirmation for electronic communication and to provide him/her or the owner of the communication channel ('Owner') with all the desired information, including information on the business relationship named in the confirmation and to transmit documents. The right to information applies irrespective of any signing rights in accordance with the Bank's signature list.
2. The Client acknowledges that any communication received by the Bank via a permitted communication channel will be deemed to have been written by its Owner. The Bank reserves the right not to accept electronic communication if it arrives via a communication channel other than a permitted one.
   If the Client has reason to fear that unauthorised persons are using the permitted communication channel, he/she shall revoke such channel immediately.
3. The Client is aware of and accepts the risks of exchanging information via the permitted communication channel chosen by him/her, in particular:
   - The information is transmitted unencrypted via open networks that are accessible to everyone and can be viewed by third parties (e.g. network and service providers), which also allows the existence of a banking relationship to be inferred. **Bank Client confidentiality and data protection cannot therefore be guaranteed.**
   - Information may be transmitted across borders without control, even if both sender and recipient are located in Switzerland.
   - Unauthorised persons may be able to view and modify the communication and manipulate the identity of the sender (e.g. email address) and/or recipient.
   - The exchange of information may be delayed or interrupted as a result of transmission errors, technical faults, interruptions, malfunctions, illegal interventions, network congestion or other inadequacies of the network operators and the like. Misdirection or deletion of electronic communications (e.g. emails and attachments) may be caused.
   - The transmission of information from abroad may, under certain circumstances, violate provisions of foreign law. It is up to the Client to seek information on this point.
   - Messages may contain malicious software with significant potential for damage.
4. The Bank applies the customary business diligence when using the permitted communication channel. The Bank assumes no responsibility for the accuracy and integrity or for the receipt and dispatch of unsecured electronic communications. The Bank will bear the loss arising in particular from losses, delays, irregularities, duplicate copies or from technical malfunctions and operational breakdowns to the extent that it has failed to exercise normal business care. Insofar as the Bank has exercised the customary business diligence, the Client will bear this loss. In particular, the Bank accepts no liability for losses and other disadvantages resulting from careless use of the permitted communication channel by its Owner or from unlawful interference with its hardware and software.
5. It is the Client's responsibility to ensure that the permitted communication channel and the hardware and software used by their Owner are protected at all times and in a suitable manner against electronic attacks and use by unauthorised persons. If there is any doubt about the origin of communications received, the Bank should be contacted by telephone. The Bank recommends that the addressee be entered each time a new message is sent and that any text received in advance not be sent with it.
6. The transmitted electronic communication will be processed in the normal course of business and without time priority.
   Orders or instructions to the Bank (remuneration orders, stock exchange orders, netting orders, dispatch instructions, etc.) may not be issued via the permitted communication channel. The Bank is not obliged to execute such orders.
   Personal data will be processed in accordance with the Bank's privacy statement. The Bank advises the Client not to send sensitive or time-critical information to the Bank via the permitted communication channel, but to contact the Bank via the secure channels provided for this purpose (e.g. E-Banking, mobile banking application).
7. Neither the Client nor the Bank is obliged to use the permitted communication channel. The Bank may interrupt or suspend electronic communication at any time, in particular if misuse is to be feared or if legal or contractual provisions require this. The Bank may refuse to accept or process electronic communications or make them subject to additional clarifications. The Bank reserves the right not to communicate electronically with persons domiciled abroad.
   The Bank is not obliged to send information via all permitted communication channels and/or to several

authorised recipients, if applicable, or to inform the Client separately of communications to third parties. The Bank reserves the right to notify the Owner of changes in their contact details via the permitted communication channel

8. The contact details (e.g. phone contacts) provided to the Bank or instructions for sending by post or via 'e-documents' given to the Bank in the context of E-Banking remain in force and are not amended by the issuing of a confirmation for electronic communication. Any orders for the Bank's electronic publications (such as newsletters) are not affected by the selection of a communication channel made with a confirmation for electronic communication. They are transmitted in accordance with the Client's order and must be cancelled separately.
9. The communication channel chosen with the confirmation for electronic communication can be revoked by the Client or by the designated Owner at any time. If a designated communication channel is no longer to be used (e.g. change of email address or mobile phone number) or if the above information on the communication channel no longer applies in some other way, it is the Client's responsibility to revoke the communication channel immediately and, if necessary, to submit a new confirmation for electronic communication via unsecured communication channels.
10. The permitted communication channel will apply as of the date it is designated as such with the confirmation for electronic communication. In the absence of revocation, the choice of the communication channel will apply after the death of the Client or in the event of his/her incapacity to act or its deletion as a company (regardless of any entries to the contrary in the commercial register).

Basler Kantonalbank

Information to our Clients – Avoiding dormant assets

Dear Client,

It happens from time to time that a bank loses contact with its Clients and that assets held at the bank become contactless or dormant as a result. Problems and undesirable situations may arise for all involved, particularly when the assets are ultimately forgotten by the Clients and their heirs. The Swiss Bankers Association (www.swissbanking.org) has therefore cooperated with the Swiss banks in preparing a series of measures aimed at avoiding and handling contactless and dormant assets. These measures are outlined for you below:

What you can do to prevent contact from being lost

- Please notify us immediately if you change your address or if you find that the address we are using is not the right one and needs to be corrected (for example, due to marriage).
- Please also inform us if you will be absent for a prolonged period and want communications to be forwarded to another address.
- It is generally recommended to designate an authorized person or appoint a special person that the Bank can contact if we lose touch with you.

Measures to be taken by the Bank if contact is lost

If contact with a Client is lost, we will adopt the following measures in accordance with the code of professional conduct of the Swiss Bankers Association that applies in these circumstances:

Immediate measures

As soon as we discover that the communications mailed to a Client can no longer be delivered, due for instance to a change of address, and no more contact of any kind exists with the Client (such as a bank visit or E-Banking login), we will with due care and diligence endeavour to restore contact and ascertain the new address. If need be, we will also commission a third party to conduct a search. These third-party agents are subject to the same duty of secrecy as the bank's employees. Banking secrecy is therefore maintained.

Measures to be taken if contact is lost or assets are dormant

If our search after a loss of contact is unsuccessful or if contact with the Client is not possible for other reasons, a contactless state is fundamentally determined. In this case, we are obligated under the code of professional conduct to take the following action:

- The assets are specially earmarked and recorded centrally within the Bank and held as contactless for 10 years and subsequently for 50 years as dormant.
- The data of contactless Clients are reported to the central database for all assets over CHF 500.00 and for all safety deposit boxes. This database, which is maintained by SIX SAG, can be accessed only by the Swiss Banking Ombudsman.
- 50 years after the assets become dormant (i.e., 60 years after the last contact) the name of dormant Client accounts with a value that exceeds CHF 500.00 or the value of which is unknown in the case of safety deposit boxes shall be published on the website https://www.dormant accounts.ch.
- The assets are delivered to the Swiss federal government (Swiss Federal Tax Administration) if no legitimate claim to the assets is asserted during the publication period. Claims of any entitled persons expire upon delivery of the assets to the Swiss federal government.

Rights are upheld even if contact is lost or assets are dormant

- The rights of Clients or of their legal successors are upheld even if contact is lost or assets are dormant until the assets are turned over to the Swiss federal government. In this context, a deviation from contractual provisions is admissible only if deemed to be in the Client's best interest. For instance, current-account and similar balances can be converted into interest-bearing investments for the Client; i.e., with exercise of due care and to the extent possible, that are profitable (savings accounts, bonds, or investment funds with a conservative risk profile). Existing savings accounts will continue to be managed subject to the applicable interest rates of the Bank. The same applies to asset management mandates, provided the specified investment objective is not inconsistent with the Client's obvious interests. Safety deposit boxes, whether the rental costs are covered or not covered, can be opened and the content stored centrally in order to complete the search measures and with respect to the liquidation, subject to internal bank instructions.

Costs

The standard fees and costs apply even if contact with the Client is lost and assets are dormant. We will also charge the account for the costs incurred for searches and for special handling and supervising of contactless and dormant assets, as well as for the publication and processing of seemingly unjustified claims. Needless to say, the extent of the investigations will be determined by their reasonableness and, in particular, by the value of the assets held.

Thank you for your help in avoiding the loss of contact and dormant assets.

600 9676 12.18

Basler Kantonalbank

Explanations for tax self-declaration

Automatic exchange of information (AEOI)

I/we acknowledge that the Bank is required to report information on the account holder/beneficial owner and on the assets to the Federal Tax Administration if the account holder/beneficial owner is resident for tax purposes in a state with which Switzerland has concluded an agreement on the automatic exchange of information in tax matters.

In accordance with the statutory provisions, the Federal Tax Administration is required to forward the information received to the competent foreign tax authority/authorities.

FATCA

I/we acknowledge that the Bank is required to report information about the account holder/beneficial owner and the assets directly to the US tax authorities (IRS) if the account holder/beneficial owner is classified as a US person pursuant to US tax law.

Note on the determination of unlimited tax liability

In a first step, tax residence can be determined in accordance with country-specific regulations on unlimited tax liability. The connecting factors for unlimited taxation vary from country to country, with the following residence characteristics to be reviewed step by step:

- permanent residence in a Contracting State,
- centre of life interests in a Contracting State,
- habitual place of residence in a Contracting State, or
- citizenship of a Contracting State.

If a person is deemed to be subject to unlimited tax liability in more than one state due to the country-specific regulations, a possible double taxation agreement (DTA) between the two states should be used for the determination of tax residence in a second step. In such cases, the so-called tie-breaker rules determine in which state a person is resident for tax purposes. If there is no DTA between the two states which assigns the tax residence to one of the two, a person shall be deemed to be resident in both states for the purpose of the automatic exchange of information on financial accounts. A limited tax liability (e.g. on the basis of income from sources in a state, real estate, a shareholding in a partnership or a permanent establishment) does not normally create tax residence relevant to the AEOI. If you have any questions about your tax residence, please contact your tax advisor.

