

These Conditions for the use of E-Services govern the modalities relating to the access to E-Services between the Client<sup>1</sup>, and/or his Authorised Representative (as defined in clause 13.1 below) and bank zweiplus Ltd (the "Bank"). For the purpose of these conditions, the Authorised User (i.e. the Client and/or the Authorised Representative, together jointly referred to as "Authorised User") is the actual user of the E-Services system. The access authorisation of the Authorised User is detailed in either the **Agreement for the use of e-banking** (Client or external asset manager version) and/or its supplement **e-banking authorisation** (Client or external asset manager version), as applicable.

The Client bears complete responsibility that any Authorised User appointed by him complies fully with the obligations specified herein.

## 1. Services offering

**1.1** The term E-Services refers to the online services (including internet banking and mobile banking) provided by the Bank. These E-Services may include basic services (such as account or portfolio overviews and movements, financial market information [time delayed], performance data, asset allocation, access to bank documents, notifications and the use of Web Meeting) as well as payment and financial instrument transactions. The Bank reserves the right to adjust or amend its service offering at any time without prior notice.

**1.2** The current service offering and fee schedule for E-Services as well as the valid Conditions for the use of E-Services will be brought to the Client's attention in an appropriate manner. In addition, a Client can contact his client relationship manager for any additional information or question.

## 2. Access to E-Services and authorisation

**2.1** Technical access by the Authorised User to E-Services is via the Internet (incl. via mobile end devices such as mobile phones or tablets) through an Internet service provider selected by the Authorised User and special browser software that the Authorised User acquires independently from third parties or via a mobile end device application (the "Mobile Banking App"). Access to E-Services and the services contained therein shall only be granted once the Authorised User has legitimised himself via one of the available authentication procedures.

**2.2** Access to E-Services is generally protected by four security levels via self-legitimation, either via the Mobile Banking App, with a token (e.g. ActivCard) or SMS log-in (where offered). To access the Bank's E-Services, the Authorised User must identify himself as follows:

- a) Access with the Mobile Banking App using PushTAN:
  - user ID assigned by the Bank to the Authorised User (1st security level);
  - password assigned by the Bank to the Authorised User (2nd security level);
  - PIN code of the mobile end device of the Authorised User (3rd security level); and
  - Transaction authentication number (TAN) generated by the E-Services system and sent to the mobile end device of the Authorised User by PushTAN (4th security level).
- b) Access with a token (e.g. ActivCard):
  - user ID assigned by the Bank to the Authorised User (1st security level);
  - password assigned by the Bank to the Authorised User (2nd security level);
  - PIN code on the token (3rd security level); and
  - token transaction number regenerated by the token every minute (4th security level).
- c) Access by SMS log-in:
  - user ID assigned by the Bank to the Authorised User (1st security level);
  - password assigned by the Bank to the Authorised User (2nd security level);
  - PIN code of the mobile end device of the Authorised User (3rd security level); and
  - transaction number (log-in) generated by the E-Services system and sent to the mobile end device of the Authorised User by SMS (4th security level).

For the Mobile Banking App, the authentication procedures to access E-Services may vary. Furthermore, the Bank has full

discretion at any time to add additional authentication procedures or change or cancel existing authentication procedures. The Bank specifically reserves the right to switch the authentication procedure for Authorised Users with tokens or SMS log-in to the Mobile Banking App using PushTAN and vice-versa. Any changes to the authentication procedures shall be communicated to the Authorised User in an appropriate manner.

**2.3** The Authorised User is required to change the password issued by the Bank immediately upon receipt and subsequently to change his password on a regular basis.

**2.4** Any Authorised User identifying himself correctly as described in clause 2.2 above (self-legitimation) is entitled to use the Bank's E-Services. Consequently, the Bank may then allow the Authorised User to access the services as defined by the Client for each Authorised User. This is possible without further authentication of the Authorised User's entitlement and irrespective of the internal legal relationship between the Client and an Authorised User, if different from the Client, and irrespective of any different commercial register entries, publications or arrangements made in other Bank documents. The Bank does not check the matter of internal user entitlement for companies with several sets of authentication features. In principle, no agreement is possible with the Bank to provide access to or the use of E-Services exclusively through authentication of two or more Authorised Users (e.g. "dual signature"). However, the Bank reserves the right to allow transactions to be executed by means of collective authorisation for certain services.

**2.5** In order to protect the Client, the Bank is entitled at any time, and without giving reasons, to refuse to issue information and to refuse to accept or execute instructions, orders and messages submitted through E-Services and to insist that the Authorised User provides a different form of authentication (e.g. by signature or by personal visit).

**2.6** The Client unconditionally accepts all transactions booked to the accounts, safe custody and metal accounts specified in the agreement(s) relating to the use of E-Services, provided they have been executed with the authentication features of the Authorised User. This applies in particular also to transactions effected via the improper use of an Authorised User's authentication features. Likewise, all instructions, orders and messages received by the Bank through use of E-Services by an Authorised User are deemed to have been composed and authorised by the Client.

**2.7** The Bank may use its discretion in introducing additional technical security systems related to the use of E-Services or individual services contained therein.

## 3. Financial instrument transactions (trading venue orders)

**3.1** The Authorised User acknowledges that financial instrument orders he places via E-Services may not be executed immediately or around the clock, but may depend, amongst other things, on the trading hours/days of the relevant trading venue and on holiday arrangements/working hours of the Bank that handles the business relationship and/or the department that processes the order. The Authorised User also acknowledges that if problems occur, the Bank's trading department will only be available to offer support during normal business hours and on days on which the relevant trading venue is open for trading.

**3.2** It is at the sole discretion of the Bank which trading venues it uses and which financial instruments are offered to the Authorised User within the E-Services trading functionality.

**3.3** The Bank does not accept any liability for financial instrument orders not executed or not executed on time or for any damages (especially losses resulting from share price fluctuations) provided it has exercised due care. It is only liable in cases of gross negligence.

**3.4** When the Authorised User places financial instrument orders, he acknowledges the applicable laws and regulations (e.g. trading venue laws, ordinances, regulations, practices) as binding and undertakes to comply with them. In the case of stock exchanges, equity markets or products with special rules and requirements, the Authorised User may only be able to place financial instrument orders after complying with the necessary requirements and formalities. In some instances, it may be necessary for the Client himself to meet these requirements and formalities.

**3.5** By placing a financial instrument order via E-Services, the Authorised User confirms that he has taken note of, understands and adheres to any applicable selling restrictions (e.g. eligibility requirements) for a particular financial instrument

pursuant to the respective product documentation. With respect to collective investment schemes, the Authorised User confirms to only invest in shares/units for which the Client is eligible pursuant to the collective investment scheme documentation in question.

**3.6** The Bank is entitled to reject or cancel financial instrument orders placed by the Authorised User if the orders fail to comply with the applicable law and regulations (e.g. trading venue laws, ordinances, regulations, practices). The Bank is further entitled to reject or cancel financial instrument orders placed by the Authorised User if there are insufficient funds in the Client's corresponding settlement account, or if the execution of the financial instrument order runs counter to the letter and spirit of an existing pledge or a block on assets.

**3.7** Before placing a financial instrument order, the Authorised User is obliged to consult the brochure **Risks Involved in Trading Financial Instruments**, as amended from time to time, and any pre-trade risk or disclosure information provided within E-Services, which provide information about the particular features and risks of financial instruments. By placing a financial instrument order via E-Services, the Authorised User confirms that he has, where applicable, received all mandatory pre-trade risk and disclosure information and that he is familiar with the customs and practices of financial instrument transactions, in particular their characteristics and risks. The aforementioned brochure in its current version can also be found on the Internet or may be ordered directly from the Bank.

**3.8** For financial instrument transactions effected via E-Services, the Bank will not assess whether a financial instrument is suitable for the Client. The Bank does not solicit, recommend or advise on financial instrument transactions placed via E-Services. These execution only transactions are based on the Client's own judgment and the Client shall therefore carefully assess whether these transactions are suitable for him or her. Any prior recommendation the Bank might have provided to the Client was suitable at the time it was made. The Bank has no ongoing responsibility to ensure that a financial instrument the Bank has recommended remains suitable.

**3.9** In the case of a partial execution of financial instrument orders, higher trading venue fees and commissions may accrue (e.g. because of minimum tariffs).

## 4. Payment transactions

### 4.1 Payment transactions

The Bank reserves the right to decline at its sole discretion payment transactions submitted via E-Services (e.g. if there are insufficient funds or if the credit limit would be exceeded). The Bank accepts no responsibility for the delayed execution or non-execution of payment transactions and losses, provided it has exercised due care. The Bank assumes responsibility only in cases of gross negligence.

The Authorised User acknowledges that authorised payment orders in E-Services can only be deleted on a limited basis.

The Bank may charge a separate fee for the payment transaction services provided via E-Services.

Payment transaction services in E-Services will not be provided to external asset managers for accounts of their asset management customers.

### 4.2 Transaction signature

The Bank may require payment orders to be authorised by means of a transaction signature as an additional security measure for payment transactions. As part of the authorisation process, the Authorised User will in such cases be informed of the content of a payment order interactively by PushTAN or SMS and be requested to confirm the execution of payment order in question by using an authorisation code.

It is at the sole discretion of the Bank to decide when and under what conditions the transaction signature may apply. The Bank may also use its discretion in determining the regulations governing the use of the transaction signature. In particular, it reserves the right to require the transaction signature for certain payment orders and may authorise the Authorised User to make changes to the regulations governing the use of the transaction signature, either individually or in their entirety. The Client assumes any liability and losses resulting from changes to the regulations made by the Authorised User. The Bank may also use its discretion in introducing additional technical security systems when providing payment transactions via E-Services.

The Bank may charge a separate fee for the transaction signature provided via E-Services.

<sup>1</sup> To facilitate readability, the masculine form is used for all genders. To the extent justified by the context, the singular form includes the plural and vice versa.

**4.3 Confidential payment option**

In providing payment transactions services as part of E-Services, the Bank offers the additional functionality "confidential payments" in order to process these payments in line with conditions determined by the Bank. The following regulations apply in particular:

- Confidential payments can only be entered and/or authorised by Authorised User who have the relevant additional authorisation;
- Confidential payments will be listed on the Client's physical transaction advices without details of the payment entered; and
- Details on the executed confidential payments can only be viewed in E-Services by Authorised Users who have the relevant additional authorisation.
- The special processing conditions for confidential payments only apply to payment transactions processed via E-Services. Any right of an Authorised User with a standard authorisation to request information on confidential payments remains unrestricted.

**4.4 Collective authorisation for execution of payment transactions (any two Authorised Users)**

If the Client has declared that payment transactions may only be processed with collective authorisation, then a payment order entered may only be executed with the electronic approval of any two Authorised Users. If this authorisation is not in place, the entered payment orders will not be executed. An Authorised User must ensure that the second authorisation is promptly obtained for electronic collective authorisations. The Bank accepts no responsibility for payment transactions that are delayed as a result of a missing second authorisation. The Bank reserves the right to delete from its E-Services system those payment orders for which a second authorisation is still missing after a period of time determined by the Bank. The Client understands that it is possible for only one Authorised User to enter (but not to authorise) payment orders for collective authorisations.

**5. Financial market information and other content**

**5.1** The Bank may make available within E-Services prices/rates and a variety of information on different financial instruments, indices, listed and non-listed companies or the economy in general (the "Financial Market Information") as well as different notification options in that regard (e.g. portfolio balance limits). Part or all of the Financial Market Information available within E-Services may be obtained from third parties. Although the Bank selects such third parties carefully and/or compiles any Financial Market Information with the appropriate standard of care and diligence customary in the business, the Financial Market Information may be subject to time delays, contain errors or be incomplete and any notifications in that regard may therefore also be subject to time delays, errors or be incomplete. As a consequence, any Financial Market Information within E-Services and/or supplied via notifications are of a purely indicative nature and the Client and any Authorised User other than the Client acknowledge and agree that neither the Bank nor any third party provider do accept any liability in regard to the timeliness, accuracy or completeness of any Financial Market Information or any potential lost profits, indirect or direct, special or consequential damages resulting from any reliance or use thereof.

**5.2** The Bank, or the applicable third party owner (as may be indicated), retains all right, title and interest (including copyrights, trademarks, patents as well as any other intellectual property or other right) in all Financial Market Information and other content (including all text, data, graphics and logos) available within E-Services. The Financial Market Information is for the exclusive personal use of the Authorised User and cannot be copied, forwarded, published, (re-) sold or used for any other commercial or non-commercial, unlawful or unauthorised purpose. The Client and any Authorised User other than the Client agrees to hold the Bank and any third-party provider harmless for all damages and costs (e.g. legal fees) resulting from any use of the Financial Market Information by an Authorised User outside the contractually agreed scope.

**5.3** The Financial Market Information available within E-Services and/or supplied via notifications does neither constitute a recommendation, nor an offer or invitation to buy or sell any financial instruments, effect transactions, or to enter into any legal transaction of any kind whatsoever, unless it is explicitly stipulated as such. Any historical performance or simulation of a financial instrument does not constitute a guarantee for a simi-

lar (positive) performance in the future. The same applies to information about companies or the economy. Furthermore, certain financial instruments mentioned within E-Services may be due to product or local legal and regulatory restrictions neither be available to all Authorised Users nor tradable.

**6. Electronic delivery of bank documents / Digital signature**

**6.1** The Bank reserves the right to provide the Client or any other Authorised User at its sole discretion with bank documents by electronic means, either exclusively or in addition to normal dispatch by post. In case of an electronic delivery of bank documents, the conditions contained in this clause 6 shall apply.

**6.2** Within the framework of the service of electronic provision of bank documents, the Bank shall send to the Authorised User certain bank documents for all accounts, safe custody and metal accounts included in the **Agreement for the use of e-banking** by making them available in electronic form, instead of paper form, on the E-Services. The Client notes that all Authorised Users who have entitlement relating to the aforementioned accounts, safe custody and metal accounts are able to access the electronic bank documents. A list of the categories of bank documents provided by the Bank electronically via E-Services can be requested from the client relationship manager. The Bank expressly reserves the right, at its sole discretion, to switch further documents that are currently sent in paper form to electronic service.

**6.3** The Client hereby expressly acknowledges that the Bank fulfils in particular its duties of notification and accountability by electronic delivery of bank documents in the E-Services mailbox of an Authorised User. The Client further acknowledges that the Bank may qualify any electronic access of bank documents by an Authorised User as a contact in the sense of the legal and regulatory requirements relating to assets without contact and dormant assets.

**6.4** Electronic delivery of bank documents is done in PDF format (expressly subject to change). The Authorised User is responsible for installing the corresponding software required to display the documents.

**6.5** The bank documents provided electronically are deemed to have been delivered to the Client, irrespective of any subsequent additional dispatch by post, within the meaning of the **General Terms of Contract** of the Bank at the time when they are made available within the E-Services environment and can be accessed by an Authorised User. This applies even if the Client himself has no E-Services access and consequently has no knowledge of the bank documents sent electronically or if an Authorised User does not or cannot access the bank documents that are provided electronically. The period for making complaints in accordance with the **General Terms of Business** of the Bank also commences at the time of availability of the electronic documents.

**6.6** The Bank accepts no liability for losses due to bank documents provided electronically not having been accessed in time. This applies in particular for notification of direct debit charges with the right of objection, information about cost and charges, pre-trade risk and disclosure information or product related information.

**6.7** Electronic bank documents are available for downloading within E-Services for at least 12 months. They are then deleted. The deletion is carried out irrespective of the aforementioned period in the case of termination of the account, safe custody and/or metal account for which the electronic service of bank documents is effected or upon termination of the **Agreement for the use of e-banking**. It is the responsibility of the Authorised User to access the bank documents beforehand if necessary and to save them. The Bank accepts no liability for losses caused by the deletion of bank documents.

**6.8** If necessary, bank documents provided electronically may subsequently be requested in paper form against payment of a fee.

**6.9** The Bank is entitled to send the bank documents scheduled for exclusive electronic delivery either additionally or exclusively in paper form by post to the Client's domicile address last notified to the Bank, if the Bank considers this, at its sole discretion, appropriate for justified exceptional cases (particularly where it is deemed to be in the interest of the Client). The Bank accepts no liability for any damages resulting from postal dispatch. Furthermore, the Client expressly releases the Bank from its confidentiality duty and expressly acknowledges that he bears any and all damages resulting from the use by the Bank of such postal dispatch.

**6.10** The electronic bank documents have the same periodicity as bank documents dispatched by postal service. Modification of this periodicity within E-Services is not possible. The Authorised User may, however, generate ad-hoc and customised bank documents within E-Services based on specific parameters set by the Authorised User himself (e.g. account statements for a specified time period). The Authorised User takes note that such ad-hoc and customised bank documents may not contain the same information and/or meet the same standards as bank documents which are periodically issued by the Bank.

**6.11** The Bank can provide no guarantee that bank documents accessed electronically and subsequently printed out meet the standards of proof required in court or other administrative proceedings (e.g. tax assessment procedure). This particularly applies to ad-hoc and customised bank documents which are generated by the Authorised User himself based on specific parameters.

**6.12** Unless exclusive delivery of bank documents was requested by the Client for all existing correspondence instructions, the existing other instructions for dispatch or retention are not cancelled with regard to the bank documents in question and continue to apply. This especially applies for dispatch or retention instructions relating to third parties.

**6.13** The electronic delivery of bank documents (exclusive or in addition to normal dispatch by post) may be cancelled by the Client or by the Bank in writing at any time without stating reasons. The cancellation then also applies for electronic delivery to all Authorised Users. In the case of cancellation of the electronic delivery, and in the absence of any instructions to the contrary, all documents shall be sent only to the Client at his last domicile address notified to the Bank as of the time of the cancellation.

**6.14** Digital signature  
The Bank may allow, from time to time, the Client to sign and execute certain bank forms and other documents via E-Services using digital signature (e.g. advanced signature or qualified signature) as implemented by the Bank. The Client acknowledges and agrees that any bank form and other document signed digitally, using any form of digital signature recognized by the Bank, are deemed to be validly signed and executed and binding upon the Client. The Bank, however, reserves the right to request, where appropriate, in addition a hand-written duly signed original.

**7. Duty of care of the Authorised User**

**7.1** The Authorised User is obliged to keep secret all the personal identification details (see clause 2.2 above) and to prevent them from being misused by unauthorised persons. In particular, after changing the password, the Authorised User must not write down the password or store it in an unprotected form on the Authorised User's computer or mobile end device. Furthermore, the password and user ID should not be codes that are easy to guess (e.g. dates of birth, phone numbers). Individual identification details must be kept separate from each other. The Client bears all risks deriving from the disclosure or use (including misuse and illegal use) of an Authorised User's identification details. The Bank does not accept any liability in this respect.

**7.2** The duty to keep identification details secret applies to each individual Authorised User. The Client is therefore also liable for any losses resulting from Authorised Users misusing the identification details of other Authorised Users.

**7.3** If there is any reason to suspect that unauthorised third parties may have discovered an identification detail of an Authorised User, the relevant identification detail must be changed, the Bank must be informed immediately and if necessary the Client or any Authorised User must block access to E-Services or request the Bank to block access (see clause 10 below).

**7.4** Authorised Users who access E-Services via a mobile end device and who lose their mobile end device must inform the Bank promptly and arrange for their service provider to block its use immediately.

**7.5** The Authorised User must notify any token loss (e.g. ActivCard) to the Bank immediately, and must also arrange for E-Services access to be blocked as soon as possible in accordance with clause 10 below. Requests to issue replacement tokens, including replacements for Authorised Users, to the Bank's branch where the business relationship is maintained may only be submitted by the Client, not by an Authorised User other than the Client.

**7.6** The Authorised User must check all data they enter and the confirmations from the E-Services system to ensure they are complete and accurate. Responsibility for data sent by the Authorised User remains with the Client until confirmation is received from the Bank's E-Services system.

**7.7** The Authorised User must minimise security risks associated with the use of the Internet or mobile end device network (e.g. viruses, unauthorised access by third parties) by use of suitable protection mechanisms (in particular anti-virus programs with active updates, a secure firewall, a high security level on the used internet browser and an operating system with current service packs applied).

**7.8** If the Authorised User has issued an order relating to a payment or financial instrument transactions to the Bank by electronic means and after issuing the order the Authorised User is able to ascertain that the order has not been executed or has not been executed correctly by the Bank, the Authorised User is required to raise a corresponding query with the Bank immediately.

## 8. Scope of the liability of the Bank and its employees (jointly referred to as the "Bank")

**8.1** The Bank does not guarantee in any way the timeliness, accuracy, completeness or relevance of the data displayed or transmitted via E-Services, including ad-hoc and customised bank documents generated by the Authorised User based on specific parameters. In particular, details of accounts, safe custody and metal accounts (e.g. balances, statements, transactions) as well as any generally available information such as financial instrument prices are not legally binding unless certain information is explicitly stipulated as such within the framework of a specific service. E-Services data does neither constitute a recommendation, nor an offer or invitation to buy or sell any financial instruments, effect transactions, or to enter into any legal transaction of any kind whatsoever, unless it is explicitly stipulated as such.

**8.2** The Bank accepts no liability for orders that it fails to carry out or does not carry out in time and for any losses as a consequence thereof except in the case of gross negligence.

**8.3** The Bank accepts no liability for losses suffered by Clients or any other Authorised User as a result of their failure to meet their contractual obligations towards third parties or for direct, indirect or consequential losses such as loss of earnings or third-party claims.

**8.4** E-Services traffic runs via an open network, the Internet, which uses public telecommunication channels without any special protection. The Bank accepts no liability for damages resulting from the use of the Internet (incl. via mobile end devices). In particular the Bank accepts no liability for damages suffered by the Client or any other Authorised User as a result of transmission errors, technical faults, malfunctions, illegal intrusion into network equipment, network overload, malicious blocking of electronic access by third parties, Internet malfunctions, interruptions or other shortcomings on the part of network operators.

**8.5** The Bank does not accept liability for the consequences of malfunctions or interruptions, in particular in processing, in the Bank's E-Services operation (e.g. caused by illegal hacking into the Bank's system), except in the case of gross negligence.

**8.6** The Bank also accepts no liability for any software or the Mobile Banking App supplied by it (e.g. via download or otherwise) or for any consequences that result from or during the transportation of the software via the network (e.g. the Internet).

**8.7** If the Bank discovers security risks, it reserves the right to suspend its E-Services temporarily at any time in order to protect the Client or the Bank until these risks are eliminated. The Bank is likewise entitled to interrupt the relevant services for maintenance works. The Bank does not accept liability for any damages arising from such interruptions.

**8.8** In the case of slight negligence the Bank does not accept liability for damages caused by its auxiliary staff in the performance of their work.

**8.9** The Bank is entitled to engage specialists to optimise the E-Services it offers. In this case it undertakes only to exercise due care in selecting and instructing third parties who are otherwise bound by applicable confidentiality and data protection laws.

**8.10** The Bank does not accept any responsibility for the computer or mobile end device of the Authorised User, technical access to the E-Services or for the software required for it.

## 9. Security

**9.1** In order to protect the Client, a multi-level security system has been developed which uses amongst other things an encryption procedure customary in the banking business. As in most cases, however, absolute security cannot be guaranteed: the Authorised User's computer or mobile end device, the provider's computers and the public networks are part of the E-Services system and may become a weak point in the system since they are outside the Bank's control.

**9.2** The Client or any other Authorised User acknowledges the following additional risks, for which the Bank cannot accept any liability:

- Insufficient knowledge of the system on the part of the Authorised User and inadequate security measures on the computer or mobile end device of the Authorised User may make it easier for unauthorised parties to enter the system (e.g. inadequately protected storage of data on the hard disk, file transfers, display insight by unauthorised third parties). It is the responsibility of the Authorised User to obtain information about the necessary security measures.
- It is impossible to exclude the possibility of traffic monitoring by network operators (e.g. Internet service providers); this means a network operator may be able to track when the Authorised User has made contact with whom.
- There is a latent risk that a third party may gain access to the computer or mobile end device of the Authorised User without being detected while they are using E-Services (e.g. via Java or ActiveX application).
- When using a public network (e.g. the Internet) there is a danger that viruses or other harmful programs (e.g. trojans or spyware) may infect the Authorised User's computer or mobile end device if the computer or mobile end device is connected to the Internet. Virus-scanning programs with active updates, a secure firewall, a high security level on the used internet browser and an operating system with current service packs applied may support the Authorised User in their security measures.
- It is important that the Authorised User only work with software from trustworthy sources.
- The availability of the Internet or mobile end device network cannot be guaranteed. In particular it is possible that transmission errors, technical faults, malfunctions, illegal intrusion into network equipment, network overload, malicious blocking of electronic access by third parties, interruptions or other shortcomings on the part of network operators may occur.
- Data downloaded by the Authorised User while using E-Services (e.g. Client data such as overviews of accounts, safe custody and metal accounts) are automatically placed in temporary storage by the Authorised User's browser software on the Authorised User's computer or mobile end device (temporary Internet files/cache). At the same time the Authorised User's browser software stores all the Internet addresses (history) accessed by the Authorised User. This can enable a third party who gains access to the Authorised User's computer or mobile end device to access Client data and draw conclusions about an existing banking relationship. The Bank therefore recommends that the cache and history be cleared at the end of every use of E-Services and to restart the Internet browser or other E-Services access software before every E-Services session.
- Client data exported from E-Services into other programs (e.g. Excel, Word) by the Authorised User or electronic bank documents will be saved unprotected on the computer or the mobile end device if the Authorised User fails to take any further precautions. This may enable a third party gaining access to the computer or the mobile end device of the Authorised User to access Client data and draw conclusions about an existing banking relationship.

**9.3** When using E-Services, cookies (strings of information sent by a website and stored on the Authorised User's computer or mobile end device) will be temporarily stored or accessed on the Authorised User's computer or mobile end device. In this way the Bank is able to provide navigation shortcuts for the benefit of the Authorised User. Only a minimum of information will be stored in the cookies created by the Bank. By modifying the Internet browser or other E-Services access software settings it is possible to prevent cookies being placed on a computer or mobile end device. Depending on the browser or other access

software settings selected, it is possible that blocked cookies may reduce the functionality of E-Services or prevent access to them. The Bank accepts no liability for such restriction.

## 10. E-Services block

**10.1** The Client can block his own access and that of any Authorised User to the Bank's E-Services, while an Authorised User other than the Client can only block his own access. A request for access to be blocked can only be made during normal business hours on bank working days and only to the Bank's branch where the business relationship is maintained and it should be confirmed to the Bank in writing immediately thereafter.

**10.2** In addition, the Authorised User may block his own access within the E-Services system.

**10.3** Any blocks can be cancelled upon request by the Client at the Bank's branch where the business relationship is maintained. The request must be submitted or confirmed in writing. Authorised Users other than the Client can only remove blocks they have placed themselves on their own access.

**10.4** The Bank is entitled to block Authorised Users from accessing individual services or all services at any time without stating reasons or prior notice if in their opinion this is appropriate under the circumstances (primarily to protect the Client). The Bank accepts no liability for damages resulting from such a block.

## 11. Confidentiality / Data protection - profiling and marketing

**11.1** Swiss confidentiality and data protection laws apply only to data stored within Switzerland. Any data transmitted abroad is no longer protected by Swiss law.

**11.2** Data may be transported amongst other things via an open network that is accessible to the public (e.g. the Internet and/or mobile end device networks). This also applies to data sent by e-mail or SMS. Consequently, data is frequently transmitted across borders without controls. This can even happen with a data transfer where the sender and recipient are situated in Switzerland.

With the exception of e-mail and SMS, individual data and PushTAN is transmitted in encrypted format within the E-Services system. However, the sender and recipient of e-mails and SMS are identifiable. They can be seen by third parties. It is therefore possible for a third party to draw conclusions about an existing banking relationship.

**11.3** The Client and any Authorised User other than the Client authorises the Bank to process all information (e.g. personal data, geodata, device information) associated with the use of E-Services and the functionalities offered with it where this is necessary to provide services as part of E-Services and to ensure its security. The aforementioned information may also be used by the Bank to provide Authorised Users, where appropriate, with tailored offers and information about the Bank's products and services as well as for market research, marketing and risk management purposes. Additionally, the Bank is for security reasons and due to legal and regulatory requirements also authorised to record any telephone conversation and any other communication (e.g. messaging, video call, live chat) an Authorised User may conduct with the Bank.

The Client and any Authorised User other than the Client hereby acknowledge to have taken note of the data protection information and the Data Privacy Statement for the use of the Bank's website (incl. E-Services) contained on the Bank's website ([www.bankzweiplus.ch/datenschutz](http://www.bankzweiplus.ch/datenschutz)) and that the aforementioned provisions shall apply for the use of E-Services.

## 12. SMS and PushTAN / Web Meeting

### 12.1 SMS and PushTAN

The transmission of SMS via public networks (e.g. the Internet) is done unencrypted and they may be intercepted, read and altered by third parties. This also applies for SMS which are deployed in the use of E-Services of the Bank (including SMS for login and transaction signing). Any communication via PushTAN is encrypted, using a separate, cryptographically isolated, secure out-of-band channel.

Subject to any separate agreements, messages and orders by SMS are not binding for the Bank for reasons of security. The Bank is authorised but not obliged to reply by e-mail to SMS from the Authorised User. Furthermore, and unless agreed otherwise, payment orders may not be submitted by SMS. The Bank does not accept liability for any losses resulting from the non-execution of such payment orders.

The Bank never accepts liability for damages incurred from the use of SMS and PushTAN. Although the aforementioned services are provided by the Bank free of charge, costs for provision of SMS or PushTAN may be charged to the Authorised User by their service provider for SMS or PushTAN data service. The Bank excludes any liability for these costs. The Bank cannot provide any guarantee that the information and notifications sent by SMS or PushTAN at the request of the Authorised User will be received by the Authorised User or that they will arrive without delay.

**12.2** Bank documents and other communication via E-Services

Bank documents (e.g. periodic statements, transaction advice, applicable bank forms) and other notification can be made available by the Bank to every Authorised User via E-Services. These communications are sent encrypted. Accessing these communications requires a successful identification check of the Authorised User with the Authorised User's personal E-Services authentication features.

A communication from the Bank to the Authorised User is deemed to have been received when it is available in his E-Services. The Authorised User is entitled to download such communications. The Authorised User is responsible for taking note in good time of the communication addressed to him. The Authorised User has the option to receive push notification on its registered mobile device. Such information is sent unencrypted via public networks and therefore provides no protection of confidentiality. Furthermore, the Bank cannot accept responsibility for notifications reaching the Authorised User or for them arriving in time.

**12.3** Web Meeting

Every Authorised User and the Bank can use within the E-Service environment Web Meeting to communicate with each other. BJSS Web Meeting is a communication channel solution that is hosted and managed by the Bank and that contains the following features: messaging, live chat, call and video call (incl. screen sharing). Web Meeting is an end-to-end communication channel where the flow of information is encrypted.

Messages or instructions sent to the Bank via Web Meeting are checked, replied to or processed within the framework of the existing business processes during normal business hours on bank working days. They do not have priority for processing. On the basis of the self-legitimation which takes place, the Bank may assume that instructions which it receives via Web Meeting within the E-Service environment have come from the Authorised User and may execute the instructions. However, no messages or instructions that are critical in terms of time or associated with a deadline (e.g. payment transactions, financial instrument transactions, cancellations of orders, credit card blocks) must be sent to the Bank via Web Meeting unless they are being provided to the Bank in the course of a live chat, call or video call. Subject to any separate agreements, Authorised Users may only give instructions on the basis of their actual authorisation on the account, safe custody and metal account. In all instances, the Bank is entitled, but not obliged, to act upon any instructions or other communications conveyed via Web Meeting and the Bank reserves the right to request an instruction or other communication in the form of a written duly signed original.

Authorised Users undertake not to record any content that is exchanged, discussed or displayed via Web Meeting whether by video or sound recording, screenshot, screen grab or otherwise. The Bank may however for business purposes and/or to comply with legal or regulatory requirements at any time and without prior notice record and keep recordings of all content that is exchanged, discussed or displayed via Web Meeting in accordance with applicable laws and regulations and the Bank's internal policies.

**12.4** Joint provisions

The Bank is entitled, without prior announcement, to delete the history of the Authorised User communications over BJSS Web Meeting, bank documents and/or other communication made available in E-Services that are older than 12 months or if a maximum storage space per Authorised User is exceeded. The deletion may be carried out without regard to the aforementioned period in the case of termination of an account, safe custody and/or metal account for which the communications are sent or if the Agreement for the use of e-banking is terminated. It is the responsibility of the Authorised User to download and save the communications beforehand. The Bank accepts no liability for losses caused by the deletion of communications.

**13. Conditions governing Authorised Representatives**

**13.1** In this agreement, an Authorised Representative refers to someone who has been granted access to use E-Services by the Client as an Authorised User via form **Authorisation to use e-banking** as well as an external asset manager (including its appointed employees) who has concluded the **Agreement for the use of e-banking (for Client Accounts by an External Asset Manager)** based on a **Power of Attorney for the Management of Assets for External Asset Managers** or similar authorisation granted by a Client. Any such Authorised Representative's E-Services access remains in place unless the aforementioned underlying authorisation is expressly revoked.

An external asset manager who concludes the **Agreement for the use of e-banking (for Client Accounts by an External Asset Manager)** in the name of and for the account of their asset management customers based on a **Power of Attorney for the Management of Assets for External Asset Managers** or similar authorisation granted by a Client is under an obligation to seek the Client's consent relating to the conclusion of any E-Services agreement as well as these conditions and to inform the Client of the risks associated with the use of E-Services.

**13.2** The Authorised Representative shall maintain his E-Services access even in the event of death, declaration of disappearance, incapacity or inability to act or bankruptcy (or in the case of a legal entity, also its winding up) of the Client or the external asset manager appointed by the Client. The Authorised Representative is aware that he must protect the interest of the Client (and/or in certain cases of his appointed external asset manager), his legal successor or any appointed representative in the event of the Client's (and/or in certain cases of his appointed external asset manager's) death, declaration of disappearance, incapacity or inability to act or bankruptcy (or in the case of a legal entity, also its winding up). The Client, his authorised signatory(ies) (if a legal entity), power of attorney holder(s), duly legitimised heirs, executors, personal representatives or liquidators as well as the Client's appointed external asset manager (in regard to its own appointed employees only) can revoke an Authorised Representative's E-Services access at any time. Any revocation must be confirmed in writing and must be forwarded to the Bank where the business relationship is maintained.

**13.3** The revocation of a standard authorisation (e.g. power of attorney or authorised signatory right) with the exception of the **Power of Attorney for the Management of Assets for External Asset Managers** or similar authorisation does not automatically result in the revocation of an Authorised Representative's E-Services access; the Authorised Representative's E-Services access must be explicitly revoked as specified in clause 13.1 above. Similarly, the revocation of the Authorised Representative's E-Services access does not automatically result in the revocation of a standard authorisation. However, the Bank reserves the right to make an Authorised Representative's E-Services access other than the one of an external asset manager dependent on the existence of a standard authorisation.

**13.4** It is at the Bank's sole discretion whether it requires separate authorisations for additional functionalities made available via E-Services. In such a case, the provisions of clauses 13.1 – 13.3 above apply as well.

**14. Country-specific restrictions / Foreign import and export restrictions**

**14.1** The range of financial services offered to Authorised Users outside Switzerland may be subject to local legal and regulatory restrictions. Certain products and services may therefore not or only partially be available in the jurisdiction in which the Authorised User is located or accessing E-Services. The Bank may at any time and without prior notice restrict its service offering for Authorised Users outside Switzerland via E-Services due to local restrictions. The Bank does not accept any liability in this regard.

**14.2** The use of the Bank's E-Services abroad may furthermore under certain circumstances contravene the laws of a foreign country. The Authorised User shall be responsible for finding out about and complying with all relevant restrictions and laws.

**14.3** Authentication features or procedures (e.g. via encryption algorithms) to access E-Services may be subject to specific import/export restrictions as well as restrictions of use

abroad. Furthermore, country-specific restrictions in regard to authentication features may exist if the Authorised User is travelling to third countries. The Authorised User shall be responsible for finding out about and complying with all relevant restrictions and laws. The Bank does not accept any liability in this regard.

**15. Amendments to these conditions**

The Bank reserves the right to amend these conditions, its E-Services offering and its fee schedule at any time. Any such amendment will be notified to the Client and any Authorised User other than the Client via E-Services or in another appropriate manner. Any additional provisions or amendments or modifications to existing provisions, agreements and services shall be regarded as accepted with binding effect by the Client and any Authorised User other than the Client upon the next E-Services access by an Authorised User by using the personal means of authorisation, but in any event when the relevant service is first used by an Authorised User. In case the Client or the Authorised User other than the Client objects to such amendments, the Bank shall be free to terminate with immediate effect E-Services or the service in question subject to special agreements.

**16. Termination**

Either the Client, his authorised signatory(ies) (if a legal entity), power of attorney holder(s), duly legitimised heirs, executors, personal representatives or liquidators as well as the Client's appointed external asset manager (in regard to its own appointed employees only) as well as the Bank can terminate the **Agreement for the use of e-banking** and any associated supplementary agreements at any time. Any termination must be confirmed in writing and must be forwarded to the Bank where the business relationship is maintained.

**17. Validity of other legal regulations**

The validity of other provisions of law, in particular those governing the operation and use of telecommunications equipment and networks, is not affected by these conditions and they apply to the Bank's E-Services as soon as they come into effect.

**18. Severability**

The invalidity, illegality or unenforceability of one or more clauses of these conditions does not affect the validity of the rest of the agreement.

**19. Place of performance**

The place of performance is **the location of the Bank with which the business relationship with the Client is maintained or the City of Basel.**

**20. Applicable law and place of jurisdiction**

These conditions and all legal relations between the Client or any Authorised User other than the Client and the Bank are governed by **Swiss substantive law.**

The **exclusive place of jurisdiction** for all legal proceedings between the Client or any Authorised User other than the Client and the Bank as well as the place of debt collection (Betreibungsort/for de la poursuite/luogo dell'esecuzione) for clients or any authorised users other than clients registered or domiciled abroad is **the location of the Bank with which the business relationship with the Client is maintained or the City of Basel**, or the defendant's registered office or place of domicile. The Bank shall also have the right to refer any claim against the Client and any Authorised User other than the Client to any other court of competent jurisdiction.

Clients and any authorised users other than clients domiciled abroad are advised that mandatory consumer protection provisions may apply depending on the particular circumstances and applicable legal issue.