

Special Conditions regarding the use of E-Banking

1. Scope

The following terms and conditions govern the access, the use and the functions of the electronic online banking solutions offered by EFG Bank von Ernst (the "Bank") via the internet (hereinafter the "E-Banking Terms and Conditions").

The E-Banking Terms and Conditions shall apply between the Bank and the account holder (the **Account Holder**) and/or any persons with an authorisation provided by the Account Holder to use the E-Banking services on behalf of the Account Holder (the **Authorised User**, which for the avoidance of doubt includes the Account Holder). **An Authorised User shall be subject to the same obligations, and shall have the same rights, as the respective Account Holder for the purposes of these E-Banking Terms and Conditions. The Account Holder shall be entirely responsible for ensuring that the Authorised User appointed by him fully complies with the obligations specified herein.** The term **EDP system** refers to electronic data processing systems (hardware and software) including mobile devices, fixed-line and mobile phones and other technical means used to access and to use E-Banking.

General provisions

2. Personal means of access

Access to E-Banking and the functions offered with it is granted once the Authorised User has identified himself to the Bank using the personal means of access, i.e.

- his user name;
- the temporary activation passcode for the initial access, and the new password set by the Authorised User for subsequent access; and
- the second factor authentication code

(the **Means of Access**).

The personal Means of Access provided to the Authorised User by the Bank may only be used in accordance with the applicable provisions. The Bank may substitute or modify the personal Means of Access at any time. The Bank has the right to revoke access to E-Banking at any time. The Bank may also change the process described in the present section at any time and shall inform the Account Holder accordingly.

3. Identification and access blocking

For the use of E-Banking and the functions offered with it, the Bank does not check the identity by means of signature or identity document verification. The verification of the user's authorisation shall be established solely on the basis of the personal Means of Access provided.

Any person successfully completing the process to access the E-Banking shall be deemed to have been duly authorised to have such access; this shall apply irrespective of whether this person is actually an Authorised User and/or was authorised by the Account Holder accordingly.

All directives and instructions received by the Bank concerning E-Banking shall be deemed to have been issued by the Authorised User.

The Bank shall be deemed authorised to execute these directives and instructions in the standard course of business and to follow the instructions and messages where they are based on a correct verification of identity.

The Bank is authorised to block or to temporarily suspend access to E-Banking in full or in part at any time, without explanation, and without prior notification, if there is a reasonable cause or if the Authorised User fails to authenticate for 3 times.

An Authorised User may request E-Banking to be blocked. An Authorised User may also block his own access/authorisation by entering his Means of Access incorrectly until the system shows it is blocked.

The Authorised User shall bear the risk of the use of his personal Means of Access during the customary processing period of an access blocking request until the point in time when the blocking of the access takes effect.

Access authorisations / personal Means of Access do not become invalid automatically, e.g. as a result of death, declaration of absence or incapacity, cancellation of the authority to sign or deletion from a register. Consequently, **the Account Holder / his legal successors / the Authorised User must always explicitly request the blocking of the access authorisation or the personal Means of Access.**

4. EFG hardware and software (incl. apps)

The Authorised User may use the hardware (e.g. hard tokens) and software (e.g. EFG mobile app) provided specially by the Bank to use E-Banking. These must be checked within 30 calendar days of receipt. The Bank must be notified immediately of any defects, otherwise the hard-/software shall be deemed to have been accepted as fully functional.

As far as legally permissible, the Bank gives no guarantee that the hard-/software provided is absolutely error-free. Moreover, the Bank gives no guarantee that all elements of the hard-/software correspond to the Authorised User's expectations or will function without error in relation to all applications and in conjunction with any other programs and device/network configurations selected by the Authorised User. In the event that defects or errors impair or hinder the functionality, the Authorised User must refrain from using the hard-/software and immediately notify the Bank.

The use of hardware and software provided by the Bank on devices not controlled by the Bank, especially **the use of apps on a mobile device, may mean that third parties (e.g. device manufacturers, providers of app distribution platforms, network providers) are able to conclude that there is a banking relationship with the Bank or may even access bank client information (e.g. when bank client information is saved on the device or the device is lost).** By using the hardware and software provided by the Bank on the devices not controlled by the Bank, the Authorised User acknowledges that these are used at his own risk.

For the use of software, the Bank grants the Authorised User the nonexclusive, non-transferable right to download the software, install it on a device owned and controlled by the Authorised User and deploy it to use Digital Banking and the functions offered with it.

For reasons of security, the Bank is authorised to block the use of software provided by the Bank, e.g. on devices with potentially harmful software or on which the usage restrictions have been removed (rooting/jailbreaking).

Provided the Bank exercises the level of care and diligence customary in the business as set out in the relevant provision of the General Conditions and Custody Account Regulations of the Bank (the **General Conditions**), the Bank offers no guarantee for the provision of fault-free, uninterrupted access to its services. The Bank will therefore accept no further liability for damages as a result of faults or interruptions of E-Banking services or its EDP systems.

5. Notification services

In E-Banking and the functions offered with it, the Authorised User has the option to be informed of certain events by e-messages (e.g. email, SMS). For system-related reasons, **these notifications are sent via unencrypted communication channels**. For technical reasons, the Bank is unable to guarantee that messages are actually received by the user in every case.

In the absence of any special instructions, **as part of the Account Holders entire banking relationship** (including future banking relationships), **the Bank reserves the right to send e-messages** such as security notifications and recommendations, event reports, tips, confirmations of meeting requests, publications and general and personalised product and service information **to telephone numbers or email addresses provided to the Bank using unencrypted communication channels. These messages may reveal that the Account Holder has certain products and services of the Bank and allow third parties, such as network and service providers, to conclude that a banking relationship exists.**

6. Obligations to exercise due care

The Authorised User must obey instructions of the Bank relating to the use of E-Banking, especially those on security precautions. The Bank may provide these instructions on its website under E-Banking or in another suitable manner.

The Authorised User shall store the personal Means of Access separately from other belongings and take particular care when storing them. Means of Access (especially passcode/password and the second factor authentication code) **may not be passed on or otherwise made available to other persons. The temporary activation passcode must be modified immediately upon receipt, the password determined and kept secret.** Passcode/password may not be noted on the Means of Access and must be encrypted if stored electronically. The password must be chosen in such a way that it is not easy to determine (no telephone numbers, dates of birth, car number plates, simple numeric sequences, etc.). The Bank strongly recommends to the Authorised User to change the password from time to time and to choose a password by a combination of several letters and numbers.

No replies may be sent to emails, SMS or other messages allegedly sent by the Bank and requesting disclosure of personal Means of Access (e.g. by entering user names, contract numbers, passcodes, passwords, second factor authentication codes or security codes on websites accessed by links), unless this has been specifically requested by the Authorised User through the Bank's self-service application. The Bank must be informed immediately of any such requests. **If there are reasons for suspecting that any other person has obtained knowledge of a passcode/password, the Authorised User must ensure that these are changed immediately. The loss of a Means of Access must be reported to the Bank immediately.**

Where the Authorised User connects to E-Banking via the internet or other digital networks, he is obliged, for the

purposes of combating mistakes and fraudulent use, to verify the correctness of the chosen address of the Bank and the authenticity of the respective server certificate (fingerprint), unless this is executed automatically by the software of the Bank or the personal Means of Access used for the login. In case of irregularities, no login is to take place and/or the connection is to be aborted immediately and the Bank has to be contacted. The personal Means of Access may only be submitted to the Bank. Login may only take place on the login page of the Bank and never on the website of a third-party provider.

It is possible that unauthorised third parties may attempt to gain unnoticed access to the **EDP system of the Authorised User**. The Authorised User is therefore obliged to take standard security measures in order to minimise existing security risks (e.g. risks in the internet). In particular, the operating system and browser must be kept up to date. In other words, the Authorised User must install the security patches provided and recommended by the respective providers. The security precautions customary for public digital networks must be adhered to (e.g. by using a firewall and an anti-virus program that must be updated regularly). It is the responsibility of the Authorised User to obtain information about and implement the security precautions required.

To increase security, the Authorised User may be asked to confirm selected transaction data when placing orders, including for example the beneficiary, or the entire transaction. In this case, the Authorised User will be required to review the information displayed for confirmation purposes for correctness in accordance with the original (physical) order instruction, i.e. independently of the information displayed in E-Banking, and, where this information is correct, to confirm the same using the personal Means of Access. The exact procedure is described in the Instructions. The Authorised User shall be solely responsible for the correct and careful execution of the confirmation. The Bank may modify the existing protective mechanisms at any time in addition to introducing new ones.

The Account Holder shall be entirely responsible for ensuring that any other Authorised User appointed by him fully complies with the aforementioned obligations.

7. Risks

Taking into account the identification process and the risks associated with the use of the internet and EDP systems set out above, the Authorised User shall bear any risks, which result from (i) manipulation on the EDP system of the Authorised User, (ii) fraudulent utilisation of personal Means of Access, (iii) breaches of duties of care, or (iv) interference by unauthorised third parties during data transmission.

The Authorised User is aware of the risks of transmitting information and data over public and private networks and of using the hardware and software provided by the Bank. Even though data transmitted over the internet in E-Banking is automatically encrypted (apart from the sender and recipient), the risk of targeted manipulation of the Authorised User's EDP system falls within the area of responsibility of the Authorised User and must accordingly be borne by the Account Holder and/or any other Authorised User. The Bank hereby excludes all liability in respect of loss or damage suffered due to transmission errors, misrouting, technical faults or defects, breakdowns or illegal/fraudulent intrusions in the EDP systems of the Authorised User or any third party (incl. systems and transmission networks that are generally accessible to the public), save in respect of loss or damage suffered as a result of gross negligence or wilful misconduct of the Bank.

8. Information from machines, terminals, monitors and other EDP systems

The Bank exercises the appropriate standard of care and diligence customary in the business when displaying information via machines, terminals, monitors or other EDP systems (including apps). The Bank excludes any further warranty and accepts no further liability for accuracy, completeness and relevance. **The information and messages**

displayed shall be regarded as provisional and shall not be legally binding unless certain information is explicitly stipulated as such within the framework of a specific function.

9. Special terms and conditions of use and legal notices

Some functions offered by E-Banking may require an additional agreement. The Bank may submit this to the Account Holder and/or any other Authorised User in E- form once they have authorised themselves via E-Banking. This shall also apply to amendments or additions to the present Special Conditions regarding the Use of EFG Bank von Ernst E-Banking. The functions shall be activated as soon as the Authorised User successfully applies for them, where necessary, and electronically accepts the respective function-specific provisions.

Upon acceptance, the provisions shall become binding for the Account Holder and/or any other Authorised User. Agreements concluded electronically shall be regarded as equivalent to agreements signed by hand. The Bank is free to change its service offering at any time.

Due to the internationalisation of markets and the ongoing expansion of the E-Banking services, the Bank is obliged to display additional legal notices on electronically communicated information and services. Once displayed, these shall become binding for the Account Holder and/or any other Authorised User. In the event that the Account Holder and/or any other Authorised User do not wish to accept these, he shall be obliged to cease using the information/services concerned.

10. Country-specific restrictions, foreign import and export restrictions

The range of financial services offered to Authorised Users abroad may be subject to local legal restrictions. If the Bank does not have the necessary local approvals, the scope of the services available to Authorised Users from the country concerned must be restricted. These restrictions are constantly changing in line with legal developments and the regulatory environment of the respective country. **The Bank shall be authorised to adjust or restrict at any time the range of functions available without prior notice.**

The personal Means of Access provided by the Bank may be subject to specific import/export restrictions as well as restrictions of use. Furthermore, the export/import and use of the personal Means of Access by the Authorised User in third countries, i.e. countries other than the country in which the Bank originally supplied the Means of Access, may be subject to additional country-specific laws. The Authorised User shall be responsible for being aware of and complying with all relevant restrictions and laws. The Bank accepts no liability whatsoever in this regard.

In all other respects the country-specific and/or page-specific information and notices on the respective websites shall apply.

11. Prices, fees and conditions

The fees, if any, for using E-Banking, the functions provided therein and the provision of the personal Means of Access (incl. replacements and additional orders) and the accompanying hardware are detailed in the brochure "Bank's Service Charges". The personal Means of Access provided by the Bank may, when imported abroad, be subject to specific duties and taxes on import. In addition, further fees, e.g.

customs clearance commissions, may arise. Since the Bank delivers duty unpaid,

all duties and fees in connection with any import abroad are at the expense of the Account Holder. The fees stated in the contract with the Authorised User's network provider shall apply to the transfer of data via the internet (incl. roaming).

The Bank reserves the right at any time to introduce new fees for E-Banking services or to adjust existing fees, if any, according to its brochure "Bank's Service Charges". Above amendment to the present terms and conditions shall be communicated to the Account Holder and be deemed to have been accepted by the Account Holder in accordance with the provisions set out in the General Conditions.

12. Banking secrecy and data protection, profiling and marketing

The Bank is authorised to gather individual cookie data on the Authorised User about his use of E-Banking in order to continuously improve E-Banking and the functions offered with it, to develop it according to the needs and interests of the Account Holder (e.g. to more quickly repair technical errors, make it easier to find content, personal tips on using offers of the Bank) and to identify any security risks. This allows the Bank to identify the Authorised User individually as a person. Some cookie settings can be configured by the Authorised User himself on the respective website. The Bank never passes cookie data to third parties that could identify the Account Holder personally or as a client of the Bank. Please refer to the Bank's Website Privacy Policy (at <https://www.efgbankvonernst.com/Datenschutz/website-privacy-policy.html>). Additionally, the Bank's Data Privacy Notice shall apply (at <https://www.efgbankvonernst.com/Datenschutz/data-privacy.html>).

13. Amendments and Termination

The Bank reserves the right to amend the framework contract at any time. Without prejudice to art. 11 above, changes to the framework contract shall be proposed in writing at least one month prior to their planned implementation.

changes to the framework contract shall be deemed to have been accepted unless the Account Holder notifies the Bank that he/she does not accept them before the date of their proposed entry into force. In this case, the Account Holder's right to use the services governed by this framework contract ceases on the date of the proposed entry into force of the changes.

The Account Holder and the Bank shall be entitled to terminate the use of E-Banking or individual functions offered by E-Banking in writing and without stating any reasons at any time, either with immediate effect or with effect at a later date. After full termination of E-Banking, the Means of Access provided must be uninstalled and/or rendered unusable/unreadable and must be returned at once to the branch of the Bank holding the account.

Notwithstanding such notice of termination, the Bank shall still be authorised to execute with legally binding effect all transactions initiated for the Account Holder before the personal Means of Access were returned.

The termination of the E-Banking Terms and Conditions does not imply termination of any other contractual relationship between the Account Holder and the Bank, but, as a consequence, the Account Holder and Authorised User will be fully restricted from the use of any E-Banking solutions offered by the Bank.

14. General Terms and Conditions and other provisions

In addition to these Special Conditions regarding the Use of EFG Bank von Ernst E-Banking, the Bank's contractual documents shall apply, including without limitation the provisions in the General Conditions on banking secrecy and data protection, outsourcing, distribution fees and

other monetary benefits, limitation of liability, amendments, applicable law and place of jurisdiction.

Function-specific provisions

The following function-specific provisions shall apply in addition to the general provisions above. The scope of the services offered may vary in eBanking and mobile banking.

15. Secure electronic communication

The Bank and the Authorised User can send each other messages via the electronic communication channel determined by the Bank (the **Secure Message**).

Secure Messages sent to the Account Holder and/or any other Authorised User shall be deemed to have been duly received when they are electronically available in the inbox of the Secure Message messenger. The Account Holder and/or any other Authorised User thus bear full responsibility for promptly reading and duly noting the content of any Secure Messages addressed to them.

Secure Messages sent to the Bank will be dealt with on bank business days during normal business hours by the relevant specialist unit of the Bank as part of current business processes, with no priority treatment. Hence the Bank suggests that Secure Messages which are time-sensitive or subject to time limits (e.g. time-sensitive payment and stock exchange orders, instructions to subscribe to issues or to carry out any other securities transactions subject to time limits, cancellations of orders and powers of attorney, blocking instructions for credit cards and other services, etc.) **are not sent to the Bank via the Secure Message messenger.** Rather, the Bank suggests using the channels designated by it for these purposes (e.g. E-Banking, telephone) and verifying executed transactions immediately.

The ability to save Secure Messages is limited in both duration and scale and may not be used to comply with any legal duties of retention.

The Bank is authorised to delete opened and unopened Secure Messages if they are older than 12 months or if a maximum storage capacity limit has been exceeded.

16. Electronic delivery of correspondence (E-Document/-s)

In the absence of any special instructions, the Account Holder authorises the Bank to make available all information and correspondence and other documents to the Authorised User exclusively **electronically** (the **E-Document/s**) via the Bank's E-Banking and the functions offered with it in an electronic inbox (the **E-Document Application**). **This applies to all products and services (e.g. accounts, credit cards) belonging to the banking relationship in question.** Should the delivery by postal mail of a specific document be required in individual cases (e.g. if physical delivery is deemed necessary for legal purposes or useful to the Bank), the Authorised User may request the Bank to provide a copy for an appropriate processing fee as set out in the brochure "Bank Service Charges". If required for regulatory reasons, the Bank reserves the right to make available all correspondence via the E-Banking of the Bank to the competent authorities.

If instructed by the Account Holder or in justified cases (e.g. if the Account Holder fails to consult certain E-Documents), the Bank will send the documents again by postal mail to

the address provided by the Account Holder at his expense and risk. E-Documents accessible in the Bank's E-Banking at that time remain available electronically to the addressee in the E-Documents Application.

The Account Holder hereby **expressly accepts** that, by making available any documents and advice in connection to the account electronically to the E-Documents Application by eDocument, the Bank fulfils its information and reporting obligations towards him. Any E-Documents made available electronically shall have the same legal effects as if sent by postal mail and shall represent the original document (or the original version of any copies, duplicates, etc. sent electronically). The Authorised User shall check the received E-Documents carefully for completeness and accurateness. Any complaints must be raised immediately in writing in accordance with the provisions set out in the General Conditions; otherwise the documents shall be considered accepted.

Documents are deemed duly received by the addressee once accessible electronically via E-Banking and the functions offered with it in accordance with the applicable provision of the General Conditions of the Bank. The Account Holder and/or any other Authorised User thus bear full responsibility for promptly reading and duly noting the content of any documents addressed to them.

There is no fixed time limit for saving delivered documents. However, the Bank reserves the right to impose limits on how many delivered documents can be saved as well as how long they can be stored. Attention is expressly drawn to the fact that in view of the formal legal requirements for an electronic archive, the addressee may not use the saving function in E-Banking for archiving purposes. Additionally, the Bank expressly reserves the right to send, at its sole discretion and without having to disclose its reasons, all information and correspondence in physical form per postal mail to the address of the Account Holder.

17. Further functions

Further terms may be agreed separately between the Bank and the Account Holder regarding the functionalities of the E-Banking solutions. Such agreement may be provided through the applicable means of communication.