

Schroders Private Banking eServices Regulations

August 2010

eServices Regulations

These regulations set out the terms upon which Schroder & Co. Limited provides the Client or Authorised Parties with access to eServices. You are strongly recommended to read them. If you do not understand any point please ask for further information.

eServices and changes in eServices

The eServices provided by Schroder & Co Limited (hereinafter the "Bank") allow valuations, deposit account and account movements, information about transactions as well as other information on a Client's Account and/or Portfolio (**eReports**) to be consulted. The Account/Portfolio information can be further used with the aid of an export function. Individual or overall transaction records can be obtained and stored directly through eServices. Furthermore, eServices allow secure communication with the Bank's relationship manager (**eMessages**) and the creation of electronic PDF documents (**eDocs**). However, if you choose to issue instructions to the Bank online using eServices, you acknowledge and accept that eMessages may not be received, read or actioned in a timely manner and that there is risk of technical failure/interference, as explained further below. In essence, eServices is an electronic information system and convenient means for non-time critical communications.

The current range of services as well as any expansion or changes to eServices are described on the Bank's webpage or will be notified to the Client via eServices. **The Bank is entitled to amend or limit the range of services offered at any time without prior notice.** The range of services offered by the Bank is aimed at Clients or Authorised Parties (each hereinafter referred to as the "User").

Local access restrictions

The Bank's eServices are not aimed at persons located in countries where online access to the corresponding range of services is prohibited under local law. Persons subject to local restrictions are not entitled to apply for and use the Bank's eServices. The Bank does not authorize usage in the following non-exhaustive list of countries in particular: Burma/Myanmar, Iran, North Korea and United States of America. Other countries may also impose restrictions, and it is up to the Client or Authorised Party to make any necessary clarifications beforehand. In particular, attention is drawn to the fact that in some countries, use of eServices may infringe import and export restrictions for encryption algorithms in force.

Access to eServices

Technical access to eServices takes place through an internet provider selected by the User and the User's own browser software. Access to eServices takes place through three security levels by means of self-identification via RSA SecurID (token). Access is provided to a person who has identified him/herself by entering the following information:

- the user identification code assigned individually by the Bank, known as the WebUserID (1st security level);
- the initial PIN code provided by the Bank, which must be changed by the User the first time he/she registers (2nd security level);
- the PIN code on the token (RSA SecurID) (3rd security level).

The Bank may change the access requirements for eServices at any time by additional self-identification procedures, modify existing self-identification procedures or eliminate them. In particular, the Bank is entitled (but in no way obliged) to change over from existing self-identification procedures to other procedures employing different or new technologies. The User will be appropriately notified of any changes to the self-identification procedure.

The User is obliged to change the first PIN code provided by the Bank as soon as he/she receives it. In order to protect the Client, the Bank may ask for additional verification of identity (however in no way and under no circumstances is it obliged to do this). The Bank may ask for such verification at any time without providing any reasons. The Bank may block access, request information and demand that that User provides additional identification (by means of signature or a personal interview).

Blocking access to eServices

The Client can block its own access and access of an Authorised Party whereas an Authorised Party may only block its own access to the Bank's eServices. Requests to block access may only be made during ordinary business hours at the branch office where the Account is held and must also be immediately confirmed in writing to the Bank afterwards.

The Bank is entitled to block the right of access of a User to one or all of the services at any time, without giving any reasons, and without previous notice as it sees fit, if it considers that this is necessary to protect the Client or for other objective reasons (e.g. maintenance work). Furthermore, the Bank reserves the right to block access to eServices if they are not used for long periods.

eReports

The Bank provides the User with electronic access via the internet to all legitimate Account/Portfolio information that is currently available in printed form. Information displayed will be as at the close of business on the previous Bank working day but is provided "as is" and without warranty as to its accuracy. Prices, performance and valuation data are subject to review and may change as part of internal checks performed during our quarterly statement production process. Prices shown may not reflect the actual realisable values of investments held in a Portfolio. Interest rates and foreign exchange rates shown in eReports may not reflect our current rates and are subject to change in accordance with our Terms of Business. Account/Portfolio information may be further used by means of an export function.

The Bank provides no guarantee for the accuracy and completeness of the eServices data it transmits. In particular, details on Accounts and deposit Accounts (balances, extracts, transactions etc.) as well as generally available information such as stock exchange prices and exchange rates are not binding. eServices data does not constitute a binding offer.

eMessages

Amongst the services provided by the Bank to the User is a mailbox in which messages and PDF documents can be received from the Bank and sent to the Bank. These messages are encrypted, but you should be aware of the security and operational risks detailed below. Successful self-identification must take place before sending or obtaining access to such messages.

eMessages must not be used for requesting any time-critical transaction orders or for static data change requests (such as address changes). The messages may not be received by the Bank due to technical or operational issues affecting the internet. Messages received the Bank are checked, processed and answered if appropriate within ordinary business processes and during ordinary business hours on Bank working days. They do not enjoy any kind of priority handling or automated processing. You therefore accept the risk that eMessages you send may not be received, read or actioned in a timely manner.

Messages sent by the Bank to Users are regarded as having reached their destination as soon as they can be retrieved from the User's mailbox. It is the obligation of the Client or the Authorised Party to regularly read the messages sent by the Bank and in so doing to take cognizance of them. Users should not respond to e-mails asking for their account or security details, as it is the Bank's policy not to ask for such details by e-mail and any such e-mails are likely to be fraudulent.

The Bank automatically deletes messages that have been read after five years without prior notice. It is entitled to delete messages from the mailbox of a User earlier if the maximum storage space per user has been exceeded. Early deletion also takes place if the Account is closed or the agreement pertaining to eServices is terminated. It is the responsibility of the User to retrieve the messages earlier if need be and to back them up.

eDocs

The User can create electronic PDF documents from the respective Portfolio (portfolio reports) in accordance with his/her needs. Documents created in this way are stored for two years within the eServices system and then are automatically deleted.

Security and operational risks

Despite the multilevel self-identification procedure, use of eServices is not absolutely secure. In addition, various parts of the system are beyond the control of the Bank, in particular the computer used by the User, the providers' computers and the public networks. In particular, the User should be aware of the following risks associated with use of eServices:

- Insufficient system knowledge and a lack of security precautions on the terminal device of the User may facilitate unauthorised access (e.g. insufficient protection of stored data).
- The creation of a traffic characteristic of the User by a network operator (e.g. internet provider) allowing it to understand when the User has established contact with the Bank cannot be excluded.
- eServices traffic takes place over the internet which makes use of public telecommunication devices without special protection. There is a risk that an unauthorised third party may obtain access to the terminal device of the User during use of eServices (e.g. through a Java or ActiveX application). Even when data content in eServices is automatically encrypted (except for the sender and the receiver) via the internet, targeted manipulations of the computer or other electronic data processing system of the User by unauthorised persons are still possible.
- There is a risk that viruses or other harmful programs (e.g. Trojans or spyware) may establish a foothold on the terminal device of the User during use of eServices on the internet. The User is solely responsible for taking sufficient security measures, in particular through the use of up-to-date virus scanners, secure firewalls, a high security setting on the internet browser and an operating system with all the latest patches. He/she should also only acquire software from a reliable source. The User acknowledges that the Bank does not market any software for obtaining access to eServices.
- The operational reliability or readiness of the internet cannot be guaranteed. In particular, network operators may suffer from transmission errors, technical defects, delays, disruptions, lawful interventions in the network, overloading of the network, wanton blocking of electronic access by third parties, interruptions and other shortcomings.
- Data retrieved by the User during use of eServices (e.g. Client data such as Account summaries) is automatically buffered (temporary internet files/cache) on the terminal device of the User by the browser software of the latter. At the same time, the browser software of the User stores all the internet addresses he/she has visited (path/history). This allows third parties who have obtained access to the terminal device to access Client data and to make inferences about an existing bank account. Therefore, the Bank recommends the User to restart their internet browser each time before they use eServices and to clear the browser's cache and history each time after log out of eServices.
- If the User exports Client data or other stored electronic records obtained from eServices to other programs (e.g. Excel, Word), the data and records are simply stored on the terminal device without any protection. Subsequently, a third party who has obtained access to the terminal device can access Client data and make inferences about an existing bank account.

The duty of care of the User

The User is obliged to keep all his/her personal identification characteristics confidential and to protect them against misuse by unauthorised persons. In particular, the PIN may not be recorded or stored without protection on the terminal device. The PIN and WebuserID should not be easy to guess (e.g. no dates of birth or telephone numbers). The various personal identification characteristics must be stored separately from one another. The User is solely responsible for any damage resulting from the disclosure or misuse of his/her personal identification characteristics. The Bank will not accept any liability in this respect.

If a User suspects that an unauthorised person has gained access to his/her personal identification characteristics, he/she must immediately change the personal identification characteristic concerned and notify

the Bank if necessary in order to block access to the eServices. If a User loses the token (RSA SecurID), he/she must immediately report the loss to the Bank in order to block access to the eServices. The User can order a replacement token at the branch office where the Account is held. A replacement token for an Authorised Party must be ordered by the Client.

The User must not respond to e-mails apparently sent by the Bank asking him/her to reveal his/her personal identification characteristics (e.g. by inserting them on a webpage which can be accessed through a link). Wherever appropriate, he/she should immediately inform the Bank.

The User should reduce the security risks associated with use of eServices (e.g. viruses, unauthorised access by third parties) wherever possible by taking suitable protective measures. In particular, he/she should maintain the operating system and the browser up to date. He/she should install the security patches made available and recommended by each provider. He/she should take the usual security precautions for public networks (e.g. installation of a firewall or deployment of anti-virus programs that are continually updated). He/she should take any necessary precautions in order to backup any data stored on his/her computer or other electronic data processing system.

Responsibility of the User and exclusion of liability of the Bank

Each User who obtains access to eServices with his/her personal means of identification and the identification procedure described in the instructions provided by the Bank (Security Details) is considered to be in possession of the rights of access vis-à-vis the Bank. The Bank is authorised to grant a User who has proven his/her identity in this way unrestricted access to the information pertaining to the Account as set out in the eServices service offer. It is irrelevant whether or not the person accessing the eServices is actually the authorised User.

The User bears the risks deriving from (1) manipulations of his/her computer or other electronic data processing system by unauthorised persons; (2) misuse of personal identification means; (3) their own or their Authorised Party's violations of contractual or statutory duties of care; (4) intrusions by unauthorised persons in the transmission of data or other technical or operational issues affecting the internet; (5) any other security or operational risk described above unless caused by the Bank's negligence, fraud or wilful default; and (6) any delay in the Bank acting upon a request sent by eMessage.

The User bears the risk of unauthorised access to eServices up to the point in time that an application to block access takes effect within a period that is customary in business practice.

The Bank will accept no liability for loss or damage to the computer or other electronic data processing system of the User or a third party caused by transmission errors, input errors, mistakes, technical faults, computer viruses and disruptions, business interruptions or illegal intrusions.

The Bank is in no way liable for loss incurred by the Client due to the use of eServices by an Authorised Party, regardless of whether the Authorised Party has adhered to the duties of care set out in these regulations or not. The Client shall hold the Bank harmless for any damage incurred by the Bank due to the failure of an Authorised Party to abide by its duty of care when using eServices.

The Bank is not liable for the consequences of disruptions and interruptions during processing and in the Bank's eServices operations (e.g. interruptions caused by illegal intrusions in the Bank's system) unless this is due to negligence, fraud or wilful default of the Bank or its Associates.

The Bank is entitled to interrupt the provision of services in order to identify security risks, carry out maintenance work or for other objective reasons. The Bank is not liable for any detriment caused to the User as a result of blocking, modifying or cancelling eServices. Furthermore, the Bank is not liable for any detriment caused to the User deriving from the deletion of eMessages from his/her mailbox or the deletion of eDocs. The User should export any data to their computer or other electronic data processing system should they require these for longer than two years.

Remember that past performance is not a guide to future performance. You may not get back the amount originally invested as the value of investments, and the income from them, can go down as well as up and is

not guaranteed. Exchange rate changes may cause the value of overseas investments to rise or fall. Investors should be aware that investment in emerging markets, derivatives or hedge funds involves a higher degree of risk and should be regarded as a longterm investment. The content of the eServices should not be used as the sole basis for any financial decisions. Please seek our advice or further information if you are unsure as to the nature, merits or risks associated with any investment in a Portfolio.

The Bank will not be liable for any damage caused by a failure to comply with contractual duties towards third parties nor for direct or indirect loss or loss of profit or opportunity that the Client may suffer as a result of use of eServices. The Bank is authorised to engage external specialists in order to optimise its eServices service offer. In this respect, it is only responsible for exercising proper care when selecting and instructing the external personnel.

Nothing in these regulations excludes or restricts any duty or liability that the Bank may have under the Financial Services Markets Act 2000 (and any secondary legislation thereunder) or part 6 of the Payment Services Regulations 2009.

No warranty for faultless operation

The Bank does not provide any kind of warranty that eServices will function as intended, without interruptions and free from faults.

Provisions regarding the authority to act for others

The Bank also reserves the right to make an authorisation to use eServices dependant on the existence of a Power of Attorney or other authorisation to manage assets or receive information from the Bank. In principle, it is not possible to grant collective authorisations for eServices. However, the Bank reserves the right to enable tasks to be carried out by means of a collective authorisation for certain supplementary services.

The Authorised Party's authorisation will remain valid until it is expressly revoked. It must be expressly cancelled either by the Client or his/her legal successor. It does not automatically become invalid, for example in the event of the Client's death, incapacity to act or bankruptcy or by cancelling the signing authority or deleting the Authorised Party from a register. Following the death of the Client, the Authorised Party must safeguard the interests of the heirs and obtain their instructions and has a duty to render account to them. The Bank reserves the right to make the Authorised Party's legal transactions dependent on the submission of documents pertaining to the law of succession and/or written declarations of consent by the heirs. The authorisation may be revoked at any time and must be addressed to the branch office where the Account is held. A revocation must always be confirmed in writing.

The revocation of a Power of Attorney or other authorisation to manage assets or receive information from the Bank does not automatically lead to the cancellation of an authorisation to use eServices. Rather, a specific revocation is required for this purpose. Similarly, the revocation of an authorisation to use eServices does not automatically lead to the revocation of a Power of Attorney or other authorisation.

Client confidentiality and data protection

The parties to the Agreement shall not, except as set a. out below, disclose information of a confidential nature acquired in consequence of it, except for information which they may be entitled or bound to disclose by law or which is requested by regulatory or fiscal authorities, or which is disclosed to their advisers or auditors or agents where reasonably necessary for the performance of their professional services or the protection of their interests. The Bank may disclose the information it holds about the Client or Authorised Party to Associates, but only if they agree to keep that information confidential to the same extent and use it only for permitted purposes.

The Bank will act as data controller (and in certain circumstances, data processor) within the meaning of the Data Protection Act 1998 (the Data Protection Act). The Client and Authorised Party hereby consent to the processing and use by the Bank and its agents and Associates of personal data (as defined in the Data Protection Act) given by the Client and Authorised Party under this Agreement for the provision of services to you (including without limitation services agreed under the Banks Terms of Business), which may include the

transfer of such data to any country outside the EEA (as defined in the Data Protection Act). The Bank may retain personal data for such period as it considers necessary to comply with its legal or regulatory obligations or to defend any potential claim. Under the Data Protection Act the Client or Authorised Party have the right to see the personal records the Bank holds about them.

Such data may also be used by the Bank and its agents and Associates to update client records, to help prevent fraud, and to research, develop and advise the Client of other products and services, unless you have indicated otherwise. The Client and Authorised Party undertake to supply personal data to us in accordance with the provisions of the Data Protection Act.

The Client furthermore acknowledges that data is transmitted over an open network (e.g. internet) that is accessible by anybody. This means that data is regularly sent across borders without controls. This may also apply to data transmissions where the sender and the receiver are both in the United Kingdom. It is true that individual data is transmitted in an encrypted form. However, the sender and receiver can still be identified. Such data can also be read by third parties. Therefore, it is possible for third parties to make inferences about an existing Account during use of eServices. This also applies to authorised external asset managers, but does not apply to the Account of the Clients whose assets are managed by them, provided these Clients do not use their own terminal device but instead, the external asset manager uses his/her own terminal device.

As part of a cooperative effort with partners in the technological sector, the Client or Authorised Party authorises the Bank to pass on its personal and authentication data to third parties for the purpose of developing more secure procedures and for processing, evaluation and product development, provided suitable protective measures are taken. Transaction data is not included in such data.

Modifications to the contract

The Bank reserves the right to modify or amend these regulations, the fees, if applicable, the instructions for using Security Details and any special regulations pertaining to individual services or Client Accounts or Portfolios, at any time. Users will be notified appropriately. In the absence of a written objection, any amendments or modifications will be regarded as having been confirmed within one month of notification, or if earlier the next time a User logs into eServices.

Termination of the contract

Each User can terminate the agreement regulating one or all of the eServices at any time in writing with immediate effect. The Client can also terminate the agreement entered into by the Authorised Party. The notice of termination must be addressed to the branch office where the Account is held or to the Client relationship manager. Following notice of termination concerning all of the eServices, the User must promptly return the token to the Bank without being requested to do so. This does not affect the rule regarding the blocking of eServices by the Bank. Termination of the Client's relationship with the Bank in accordance with the Terms of Business will automatically terminate access to eServices for the relevant Client and any Authorised Party.

Other terms

These eServices Regulations together with the application are an integral part of the agreement to use eServices. They are supplemented by the instructions on how to use the personal means of identity and any special provisions pertaining to individual services or Client Accounts and the Bank's Terms of Business currently in force.

Severability

Each provision of the Agreement is severable and if at any time any provision becomes invalid, illegal or unenforceable, then this will not affect any of the other provisions.

Applicable law and place of jurisdiction

The Agreement will be governed by and construed in accordance with English law. The English courts will have exclusive jurisdiction to settle any disputes or claims which may arise out of or in connection with the Agreement for which purpose all parties agree to submit to such jurisdiction.

Definitions

Account any or all accounts held with the Bank by the Client or to the Client's order, including without limitation any *Investment Deposit Account, *Fixed Deposit Account and/ or *Cash Management Support Account.

Associate an undertaking in the Schroders Group or a person whose relationship with the Schroders Group might reasonably be expected to give rise to a community of interest between them with may involve a conflict of interest in dealings with third parties.

Authorised Party a person authorised by the Client to access eServices in relation to the Client's Account or Portfolio.

Bank Schroder & Co Limited

Business Day any day, other than a Saturday, Sunday or public holiday in England.

Client means a person to whom the Bank provides investment, banking and/or custody services.

Portfolio a portfolio of assets (including cash held in a *Cash Management Support Account or Investment Deposit Account (as the case may be)) entrusted from time to time by the client to the Bank, and any *ISA.

Schroders Group us, Schroders plc (our ultimate holding company) and any of our or its subsidiaries (as defined in sections 1159 and 1160 of the Companies Act 2006 and any regulations made thereunder).

Terms which are not defined in these regulations shall have the same meaning as set out in the Bank's Terms of Business as amended from time to time.