Annex 8

ERSTE BEFEKTETÉSI ZRT'S (the "Company") DATA MANAGEMENT NOTICE

1. It is important for the Company to respect and enforce the rights of Customers and all other natural persons concerned (Customers and other persons concerned are hereinafter collectively referred to as "Data Subject") related to the processing of their personal data. For the purposes of controlling, recording, processing and transferring the Data Subject's personal data, the Company shall act in compliance with the provisions of Act CXII of 2011 on Informational Self-Determination and the Freedom of Information (hereinafter the "Freedom of Information Act"), Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter the "Bank Act"), Act CXXXVII of 2007 on Investment Firms and Commodity Brokers, and on the Regulations Governing their Activities (hereinafter the "Investment Firms Act") and other data protection laws. In order to comply with the data security requirements, the Company shall ensure the protection and safeguarding of the Data Subject's personal data, in particular against unauthorised access, modification, transfer, disclosure, deletion or destruction as well as accidental destruction or damage.

2. Definitions

a) Data Subject: shall mean any natural person identified or directly or indirectly identifiable by reference to specific personal data;
b) Customer: the Data Subject that uses the Company's investment and ancillary services.
c) Personal Data: shall mean data relating to the Data Subject, in particular by reference to the name and identification number of the Data Subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the Data Subject;
d) Consent: shall mean any freely and expressly given specific and informed indication of the will of the Data Subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations;
e) Objection: shall mean a declaration made by the Data Subject objecting to the processing of his/her personal data and requesting the termination of data processing, as well as the deletion of the data processed;
f) Controller: shall mean a natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor;
g) Data Processing: shall mean any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data as well as preventing their further use, taking photos, making audio or visual recordings;
h) Data Transfer: shall mean ensuring access to the data for a third party;
i) Disclosure: shall mean ensuring open access to the data;
j) Data Deletion: shall mean making data unrecognisable in a way that they can never again be restored;
k) Data Destruction: shall mean complete physical destruction of the data carrier recording the data; Data Processing: shall mean performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;
l) Data Processing: shall mean performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;
m) Data Processor: shall mean any natural or legal person or organisation without legal personality processing the data on the grounds of a contract entered into with the controller, including contracts concluded pursuant to legislative provisions;
n) Third Party: shall mean any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor;
o) Third Country: any State that is not an EEA Member State

3. The Principles and Legal Basis of Data Processing

3.1 Personal data may be processed only for specific and explicit purposes, where it is necessary for the exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness.

3.2 The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose.

3.3 In the course of data processing, the data in question shall be treated as personal as long as the Data Subject remains identifiable through it. The Data Subject shall, in particular, be considered identifiable if the Company is in possession of the technical requirements necessary for identification. The accuracy and completeness, and - if deemed necessary in the light of the aim of processing - the up-to-date nature of the data must be provided for throughout the processing operation, and shall be kept in a way to permit identification of the Data Subject for no longer than is necessary for the purposes for which the data were recorded.

3.4 Personal data may be processed under the following circumstances:
a) when the data subject has given his consent, or
b) when processing is necessary as decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest (hereinafter referred to as “mandatory processing”).

Where data processing is mandatory, the type of data, the purpose and the conditions of processing, access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or municipal decree in which it is ordered.

3.5 Personal data may be processed also if obtaining the Data Subject’s consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary:
a) for compliance with a legal obligation pertaining to the Company, or
b) for the purposes of the legitimate interests pursued by the Company or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

3.6 Prior to data processing being initiated the Data Subject shall be informed whether his consent is required or processing is mandatory. The data subject shall be clearly, plainly and elaborately informed of the data to be processed as well as all aspects concerning the processing of his personal data, such as the purpose and legal basis of data processing, the person entitled to control the data and to carry out the processing, the duration of the processing operation and the persons to whom his data may be disclosed.

3.7 Where personal data is recorded under the Data Subject’s consent, the Company shall - unless otherwise provided for by law - be entitled to process the data recorded where this is necessary
a) for compliance with a legal obligation pertaining to the Company, or
b) for the purposes of legitimate interests pursued by the Company or by a third party, if enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data, without the data subject’s further consent, or after the data subject having withdrawn his consent.

4. The aim of data processing

4.1 The Company shall process the Data Subject's personal data disclosed or made available to the Company by the Data Subject (including on any documents, contracts, certificates, forms or otherwise submitted by the Data Subject to the Company) in accordance with the laws on investment privacy and data protection, for the purposes of the performance and execution of the contract for investment and ancillary services between the Company and the Customer, the provision of services under such contract, the certification of rights and obligations related to such contract, the enforcement, collection and sale of claims arising in relation to such contract (if any), risk management (risk analysis, risk mitigation, risk assessment), customer rating, statistical analysis, complaint management, business offers, market research, customer satisfaction survey, marketing, liaising, compliance with any statutory data processing obligation (e.g. customer due diligence to prevent and combat money laundering and terrorist financing, compliance with the Company's tax liabilities in respect of the Customer), prevention of abuse of identity documents and the tasks associated with fraud management. Any other data processing aims related to the contract between the Company and the Customer are provided for in the specific contracts.

5. The set of controlled data

5.1 The Company normally controls the Customers' following personal data:
a) Family name
c) First name
d) Permanent address
e) Tax identification code
f) Nationality
g) Place of birth
h) Date of birth
i) Mother's name
j) Name at birth
k) Type and number of identity document

l) Number of Permanent Address Card
m) Mobile number
n) Email address
o) Mailing address (if different from the permanent address)
p) FATCA audit result
q) TTNY and PEP statements result
r) Copy of identity document
s) other documentation

5.2 The list of personal data controlled in relation to a specific transaction shall be provided for in the relevant contract or other forms related to the given service.

6. The duration of data control

6.1 The maximum duration of data control by the Company shall be different in the case of data processing based on the Data Subject's consent and mandatory data control. For data control based on the Data Subject's consent, the Company shall not control the Data Subject's personal data for longer than the end of the 5th (fifth) year following the termination of the contractual relationship between the Company and the Data Subject or the termination of any claims under such contractual relationship, and in the absence of a contractual relationship for longer than a period of 5 (five) years after the data are recorded, but even within that period only until the Data Subject withdraws his consent. For statutory mandatory data control, the Company shall control the Data Subject's personal data provided for in the law until the statutory deadline and for the statutory purposes. All other data control durations applicable to the specific transaction are provided for in the relevant general contractual terms and conditions and the specific contracts.

7. Photo and video recordings

7.1 In order to avoid interruptions to its business and to protect human life, physical integrity, personal freedom, property as well as bank, securities and business secrets, ERSTE Bank Hungary Zrt. may make photo and video recordings at its premises (jointly used with the Company) open to customers. ERSTE Bank Hungary Zrt may store such recordings for security purposes and use them as evidence. ERSTE Bank Hungary Zrt may retain the recordings for a maximum of 50 (fifty) days after which it is required to delete them. ERSTE Bank Hungary Zrt may place the signs informing Customers that photo and video recordings may be made at the entrance of its premises open to customers. The photo/video recording system is operated by ERSTE Bank Hungary Zrt and the images are stored locally until deletion. ERSTE Bank Hungary Zrt shall separately inform those concerned about the rules of photo and video recording. This information shall be posted at the premises open to customers.

7.2 If the circumstances referred to in Section 7.1 occur in relation to the Company and require the use of the photo or video recordings, the Company may receive such photo or video recordings from ERSTE Bank Hungary Zrt to the extent necessary.

8. Complaint management, sound recordings

8.1 Where complaints are received by telephone, the conversation between the Company and the complainant Customer shall be recorded by the Company and the Company shall retain such sound recording for 5 (five) years. At the complainant Customer’s request, the Company shall enable the Customer to listen to the sound recordings and shall also make available certified minutes taken of the sound recordings free of charge. In all other respects, the Company shall retain the complaint and the answer for 5 (five) years. Where phone conversations not involving a complaint are recorded, the retention period of such sound recordings shall be 5 (five) years.

8.2 In order to comply with the rules applicable to investment privacy, the Company may only and exclusively disclose general information in standard electronic letters (e-mail without encryption or electronic signature) and may not disclose information that qualify as bank and investment secret. The Company shall only respond to complaints sent by the Customer through standard e-mail messaging and containing or requesting such information in a letter sent by post to the Customer's notified mailing address.

8.3 The Company has a Complaint Management Policy in place that is attached to these General Terms of Business.

9. Data processing

9.1 The rights and obligations of data processors engaged by the Company in connection with the process of personal data shall be determined by the Company within the scope of the Freedom of Information Act and

other legislation on data processing. The Company shall be held responsible for the legitimacy of its instructions.

9.2 In the performance of its duties, the data processor may not subcontract another data processor.

9.3 The data processor may not make any decision on the merits of data processing and shall process any and all data entrusted to him solely as instructed by the Company; the processor shall not engage in data process for his own purposes and shall store and safeguard personal data according to the instructions of the Company.

9.4 Contracts for the process of data shall be executed in writing.

9.5 The Company may only outsource activities related to its investment and/or ancillary services or prescribed by statute that involve data control, data processing or data storage activities if it complies with all applicable data protection regulations. The contributor performing the outsourced activities may only subcontract any of its tasks with the Company's prior written consent.

9.6 The list of contributors performing outsourced activities shall be included in the Company's General Terms of Business.

9.7 The Company may engage an intermediary for the provision of the Bank's investment and ancillary services. The list of intermediaries engaged by the Company from time to time is available at the website of the National Bank of Hungary.

10. The conditions of data transfer (data disclosure)

10.1 Personal data may be transferred with the data subject's consent or if allowed by the law.

10.2 Subject to the Customer's consent, the Company may transfer data recorded in relation to certain Customer contracts to Erste Group Bank AG (Austria), the Company's shareholder, for the purposes of customer rating, risk management, statistical analysis, supervision and court cases, in accordance with the provisions of the Investment Firms Act and the data protection laws.

10.3 Subject to the Customer's consent, the Company may transfer the Customer's personal identity data (name and name at birth, place and date of birth, mother's name, type and number of identity document, home address and number of the residence card); contact details (address, email address, telephone number); NetBroker system ID and user name; securities account number(s), account balance(s) and the details of the given transaction; MIFID test results; and tax identification code to ERSTE Bank Hungary Zrt with a view to the provision of the services requested by the Customer (i.e. to access certain functions of NetBroker / Hozam Plaza / Portfolio Online Tőzsde from NetBank).

10.4 Pursuant to the applicable data protection laws, transfers of data to EEA Member States shall be considered as if the transmission took place within the territory of Hungary. The Company shall only transfer personal data to a third country (non-EEA Member State) with the Data Subject's express consent or if the conditions of data processing provided for in Sections 5-6 of the Freedom of Information Act are met and the appropriate level of protection for the personal data is ensured in such third country.

11. Information obligation

11.1 Prior to data processing being initiated the Data Subject shall be informed whether his consent is required or processing is mandatory.

11.2 Before processing operations are carried out the Data Subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal basis, the person entitled to control the data and to carry out the processing and the duration of the proposed processing operation.

11.3 Information shall also be provided on the Data Subject’s rights and remedies.

11.4 The Company occasionally uses Rich Internet Application (pl. Adobe Flash) based technologies on its public websites that are suitable for displaying images and sound, during which the website stores the settings required for displaying images and sound on the visitor's computer (by means of persistent cookies and Local Shared Objects) in order to enhance the customer experience, in a way that can be modified or deleted by the user at any time.

11.5 The Company occasionally uses web applications (such as time booking tool etc.) on its public websites that may store data on the user's computer (by means of session cookies) for the duration of the service in

order to identify the user or to apply the security time limit. The stored data are automatically deleted when the user no longer uses the service or when the security time limit is reached.

11.6 In the course of the use of the services provided by the Company's contracted partners, a third party may store data on the user's computer concerning the user's settings (until they expire or are deleted manually) through the electronic services provided by the Company with a view to enhancing the user experience. The deletion of such data may adversely affect the functioning of the services provided by the Company (persistent cookies).

11.7 If the user has permitted the use of cookies in his web browser, the websites operated by the Company will automatically store the required cookies on the user's computer until their expiry of deletion. The Company shall not store cookies about its own users in its own IT systems.

12. The Data Subject's rights and the enforcement thereof

12.1 The data subject may request from the Company
a) information on his personal data being processed,
b) the rectification of his personal data, and
c) the deletion or blocking of his personal data, save where processing is rendered mandatory.

12.2 Upon the Data Subject's request the Company shall provide information concerning the data relating to him, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, legal basis and duration of processing, the name and address of the data processor and its activities relating to data processing, and – where the Data Subject's personal data are transferred – the legal basis and the recipients thereof.

12.3 The Company shall comply with requests for information without delay and provide the information requested in an intelligible form, in writing within not more than 30 (thirty) days.

12.4 The information shall be provided free of charge provided that the Data Subject has not yet submitted a request for information to the Company for the category of data concerned in the given year. A charge may be imposed in all other cases. The Company may only refuse to provide information to the Data Subject in the cases defined by the law.

12.5 Should a request for information be denied, the Company shall inform the Data Subject in writing about the provision of the Freedom of Information Act serving as the grounds for refusal. Where information is refused, the Company shall inform the Data Subject of the possibilities for seeking judicial remedy or lodging a complaint with the National Data Protection and Freedom of Information Authority (seat: 1024 Budapest, Szilágyi Erzsébet fasor 22/c, hereinafter referred to as the "Authority").

12.6 Where personal data are inaccurate, and the correct personal data are at the Company's disposal, the Company shall rectify the personal data in question.

12.7 (2) Personal data shall be deleted if:
a) processed unlawfully;
b) so requested by the Data Subject (unless processing is based on a mandatory provision of law);
c) incomplete or inaccurate and it cannot be lawfully rectified, provided that deletion is not disallowed by statute;
d) the purpose of processing no longer exists or the statutory time limit for storage has expired (unless the data carrier is to be archived pursuant to the act on the protection of archival material);
e) so ordered by court or by the Authority.

12.8 (4) Personal data shall be blocked instead of deleted by the Company if so requested by the Data Subject, or if there are reasonable grounds to believe that deletion could affect the Data Subject's legitimate interests. Personal data blocked in the above manner shall be processed for only as long as the purpose which prevented their deletion exists.

12.9 If the accuracy of an item of personal data is contested by the Data Subject but its accuracy or inaccuracy cannot be ascertained beyond doubt, the Company shall mark that personal data for the purpose of referencing.

12.10 When data are rectified, blocked or deleted, the Data Subject and all recipients to whom it was transmitted for processing shall be notified. Notification is not required if that does not violate the rightful interest of the Data Subject in light of the purpose of processing.

12.11 If the Company refuses to comply with the Data Subject's request for rectification, blocking or deletion, the factual or legal reasons on which the decision for refusing the request for rectification, blocking or deletion is based shall be communicated in writing within thirty days of receipt of the request. Where the request for rectification, blocking or deletion is refused, the Company shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

13. Objection to processing personal data

13.1 The Data Subject shall have the right to object to the processing of his personal data:
a) if processing or disclosure is carried out solely for the purpose of discharging the Company's legal obligation or for enforcing the rights and legitimate interests of the Company, the recipient or a third party, unless processing is mandatory;
b) if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and
c) in all other cases prescribed by law.

13.2 The Company shall investigate the cause of the objection as soon as possible but no later than within 15 (fifteen) days, adopt a decision as to the merits thereof and shall notify the Data Subject in writing of its decision.

13.3 If the Company concludes that the Data Subject's objection is justified, it shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

13.4 If the Data Subject disagrees with the Company's decision or if the Company fails to meet the deadline specified in the Freedom of Information Act, the Data Subject shall have the right to turn to court within thirty days of the date of delivery of the decision or from the last day of the time limit. The action shall be heard by a competent municipal court. At the Data Subject's option, the action may be brought before the municipal court in whose jurisdiction the Data Subject's home address or temporary residence is located.

The Company shall be liable for damages caused to others by the illicit processing of the Data Subject's personal data or the violation of the data security requirements. The Company shall also be liable to the Data Subject for damages caused by the data processor. The Company shall be released from liability for damages if he demonstrates that the damages were brought about by unavoidable reasons beyond his data processing activity.