Terms governing the protection of personal data during the operation of Xnet Order Routing Network

PREAMBLE

i. Athens Exchange, as operator of the electronic network for the routing of buy or sell orders for securities, either listed or admitted to trading on the markets of EU Member States other than Greece, or of a third country, processes personal data of the Order Originator in the framework of their cooperation based on the Regulatory Framework for the Operation of the Xnet Order Routing Network of Athens Exchange. Consequently, according to the definitions of the regulatory framework for the protection of personal data, Athens Exchange acts as Processor on behalf of the Order Originator, which has the role of Controller.

ii. Personal Data (hereinafter 'Data') is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

iii. Other terms relating to personal data, which are used herein and for which no definition is provided, shall have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter 'GDPR').

iv. 'Third countries' shall mean countries outside the European Economic Area (EEA).

v. The terms of this Annex shall under no circumstances relieve the Processor of its obligations under the GDPR or other legislation on the protection of personal data.

1. Rights and obligations of the Controller

The Controller shall:

1.1. comply with the legislative framework on the protection of Personal Data and bear the burden of demonstrating its compliance therewith;

1.2. ensure the existence of a legal basis for the lawful processing of Data which are processed by the Processor;

1.3. have the right and the obligation to take decisions relating to the purposes of and means for processing the Data;

1.4. provide written instructions to the Processor concerning the Processing of Data performed by the latter on its behalf;

1.5. take appropriate measures to provide data subjects with all necessary information relating to the processing of their Data by the Processor.

2. Obligations of the Processor

2.1. The Processor shall:

2.1.1. be fully aware of and comply with the GDPR and generally any legislation on the protection of personal data which may be in force from time to time;

2.1.2. refrain from fulfilling its obligations under the terms hereof, with regard to Data, in a manner that compels the Controller to breach any of its obligations under applicable legislation on the protection of personal data;

2.1.3. process the Data only on the basis of documented instructions from the Controller, unless otherwise required by an applicable law to which the Processor is subject, and regarding which the Processor must inform the Controller before processing the Data.

Any amendments and/or additions to the aforementioned instructions during the processing of Data must always be made in writing, including in electronic form;

2.1.4. immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. In the event that the Controller insists on an instruction which, in the opinion of the Processor, infringes the GDPR or other Union or Member State data protection provisions, the Processor reserves the right to refuse execution of the instruction and/or terminate the principal Contract (Master Agreement) and this Agreement;

2.1.5. maintain a record of all processing activities it carries out on behalf of the Controller, in accordance with par. 2, Article 30 of the GDPR.

3. Confidentiality

3.1. The Processor must ensure that persons authorised to process Data (permanent/temporary employees, representatives, agents, servants in general and associates) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,

are aware of and follow the instructions of the Controller with respect to the processing of Data and take all appropriate measures to safeguard the Data.

4. Security of processing

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall – during the entire duration of processing – implement appropriate technical and organisational measures to ensure that the Data are safe in accordance with the requirements of applicable legislation and protected against risks to the rights and freedoms of natural persons, particularly due to unauthorised access, disclosure, alteration, deletion or loss.

4.2. The Processor shall assist the Controller in ensuring compliance with the latter's obligations pursuant to Article 32 of the GDPR, by providing, inter alia, the Controller with information about the technical and organisational measures already implemented by the Processor.

5. Subprocessors (Subcontractors)

5.1. The Processor may not engage another processor (subprocessor / subcontractor) to carry out all or part of the processing tasks which it performs on behalf of the Controller without the prior written authorisation of the Controller.

5.2. The Processor must receive from the Controller general authorisation for the use of subprocessors to carry out all or part of the processing tasks which it performs on behalf of the Controller. The Processor shall provide the Controller with prior written notification of any intended changes concerning the addition or replacement of subprocessors at least ten (10) business days before the planned addition or replacement, so as to give the Controller the opportunity to object to such changes prior to the use of a subprocessor.

5.3. The Processor may use only subprocessors that provide sufficient guarantees as to the implementation of appropriate technical and organisational measures, in such a manner that the processing will meet the requirements of the GDPR. The Processor must enter into a legally binding contract with each subprocessor which (contract) contains at least the same Data protection obligations set out herein, including the obligation to allow for and facilitate audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, particularly in order to ensure provision of sufficient guarantees as to the implementation of appropriate technical and organisational measures in compliance with the requirements of the GDPR.

5.4. In every case, the Processor shall remain fully liable to the Controller for any act or omission of the subprocessor or of any third party appointed by the latter, as if such acts or omissions were those of the Processor.

6. Transfers of data to third countries or international organisations

6.1. Any transfer of personal data to third countries or international organisations by the Processor shall take place only on the basis of documented instructions from the Controller and always in compliance with Chapter V of the GDPR.

6.2. In the event of transfers of data to third countries or international organisations, which the Controller has not instructed the Processor to carry out, but which are required under EU or Member State law to which the Processor is subject, the latter shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

6.3. Consequently, without documented instructions from the Controller, the Processor shall not, in the framework hereof:

a. transfer personal data to a controller or processor in a third country or international organisation;

b. entrust the processing of personal data to a processor in a third country;

c. itself carry out the processing of personal data in a third country.

7. Assistance to the Controller

7.1. Taking into account the nature of data processing, the Processor should assist the Controller with appropriate technical and organisational measures, to the extent possible, during fulfilment of the Controller's obligations to respond to requests relating to the exercise of data subject rights, as stipulated in Chapter III of the GDPR.

7.2. The Processor shall promptly forward to the Controller any request it may receive concerning the exercise of the rights of subjects whose Data are processed on the basis hereof. The Processor shall not reply to the aforementioned requests unless it has been authorised to do so by the Controller.

7.3. The Processor, taking into account the nature of data processing and the information available to it, shall assist the Controller in ensuring its compliance with:

- the obligation of the Controller to carry out a data protection impact assessment. The assistance of the Processor shall be made available through its participation in interviews and/or the completion of questionnaires in order to provide the necessary information to the Controller, concerning the processing carried out by the Processor on behalf of the Controller;

- the obligation of the Controller to consult the supervisory authority, prior to processing, where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

8. Notification of a personal data breach

8.1. The Processor shall promptly notify the Controller as soon as it becomes aware of any accidental, unauthorised, or unlawful destruction, loss, alteration, or disclosure of Data or any accidental, unauthorised, or unlawful access to Data (hereinafter 'Data Breach'). Moreover, the Processor shall provide the Controller with any information it has and which the Controller may reasonably request in connection with the Data Breach.

8.2. The Processor shall immediately take any possible measure to mitigate the consequences of the Data Breach, and take any necessary measure for its remediation.

8.3. The aforementioned notification must be made within forty-eight (48) hours from the moment the Processor has become aware of the Data Breach.

8.4. The Processor shall assist the Controller in the fulfilment of its obligations to investigate the possible incident, notify any Data Breach to the competent supervisory authority, and make an announcement on the breach to the Data Subjects.

8.5. The above obligations fall on the Processor also in cases where the breach involves a subprocessor used by the Processor.

8.6. The Controller is entitled to request any additional information concerning the incident and the circumstances, technical or other, in which the breach arose, and the Processor shall be obliged to respond immediately.

9. Deletion/Destruction of Data

9.1. Upon expiry of the cooperation or at any time, the Processor shall, at the request of the Controller, immediately delete/destroy any data of the Controller along with all existing copies of such data which may have been created, unless the Processor has a legal obligation to continue storing the data. In the latter case, the Processor shall inform the Controller at the earliest

regarding the aforesaid legal obligation and undertake the commitment to process the Data exclusively for the purposes and duration laid down in the relevant legislation.

9.2. The Processor shall ensure that the deletion/destruction of Data is carried out, taking the appropriate technical and organisational measures for the security of the relevant processing.

9.3. The Processor shall perform the aforesaid deletion within the timeframe set by the Controller and confirm in writing the deletion/destruction of the Data to the Controller.

10. Audits and Inspections

10.1. At the request of the Controller, the Processor shall make available to the latter all information necessary to demonstrate its compliance with provisions on the protection of personal data and with the terms hereof and allow for and facilitate audits, including inspections, conducted by the Controller or by another person mandated by the Controller.

10.2. The Controller shall provide the Processor with written notification of any audit at least ten (10) business days prior to the audit, informing the latter of the identities of the natural persons who will perform the audit and its estimated duration.

11. Commencement and Expiration

11.1. The terms of this Annex shall be applicable for the entire duration of the processing of Data by the Processor, irrespective of any termination of cooperation, and they cannot be nullified unless they are replaced by other terms that govern the processing of Data by the Processor.

11.2. If the Data processing activities of the Processor cease and the Data are deleted or returned to the Controller in accordance with the provisions herein, the terms of this Annex shall cease to have effect.

12. Other terms

12.1. This Annex constitutes a single integrated whole with the Regulatory Framework for the Operation of the Xnet Order Routing Network.

Personal Data Processing Appendix

A1. The purpose of the personal data processing on behalf of the Controller (order originator) is:

The provision of services for the operation of the electronic network for the routing of buy or sell orders for securities, either listed or admitted to trading on the markets of EU Member States other than Greece, or of a third country, which enables the receipt of orders by intermediaries that have undertaken obligations to execute them vis-à-vis order originators.

A2. The processing of personal data by the Processor on behalf of the Controller (order originator) relates primarily (nature of the processing) to:

The transmission of securities buy or sell orders of the order originator.

A3. The processing includes the following personal data:

The data of orders from order originators, as such data are set out in paragraph 6.1 of the Regulatory Framework for the Operation of the Xnet Order Routing Network.

A4. The processing includes the following categories of data subjects:

Investors (clients of the order originator).

A5. Transmission of data:

The order originator instructs Athens Exchange to transmit its data via Xnet to the Intermediary Firm contracted by the order originator as well as to ATHEXCSD.

B. Subprocessors

Upon commencement hereof, the Controller approves the use of the following subprocessors:

NAME/LEGAL NAME	ADDRESS/REGISTERED OFFICE	PROCESSING DESCRIPTION

C. Security of processing – Technical & Organisational Measures

Organisational measures:

1. Definitions of critical roles: definition of Chief Information Security Officer and of Data Protection Officer.
2. Organisation/Management of personnel: specification of employee roles and authorisations, commitment to confidentiality on the part of employees and training in matters of information security and data protection.
3. Management of information goods: recording, classification of information.
4. Management of providers: recording, contract awards in writing, security measures relating to processors, commitment to confidentiality on the part of processors' personnel.
5. Procedures for handling personal data breach incidents and personnel training.
6. Implementation of an Information Security Management System in accordance with ISO 27001 quality standards.

Technical measures:

7. Logical access control: management of user accounts, access control mechanisms, password management, disabled computers, separation of Client data from other information of ATHEX.
8. Keeping of backup copies.
9. Malware protection.
10. Log files of user activity and security incidents: keeping and checking of log files.
11. Adoption of communications and network security measures: network device control, remote access control.
12. Perimeter security.
13. Software security: application design and development processes, protection of operating system files.
14. Change management policy and processes and creation of a safe test environment.

Physical security measures:

15. Physical access control throughout the building and particularly the Data Center, restriction of access only to authorised persons.
16. Protection measures against physical damage to IT and electromechanical support infrastructures.