

Terms of personal data protection during the provision of the AXIASMS service

PREAMBLE

- i. The company "HELLENIC CENTRAL SECURITIES SERVICES S.A." (ATHEXCSD), as its provider AXIASMS service, supporting the communication of ATHEXCSD Participants with their investor clients, whom they have registered with said service so that they can be centrally informed about:

1. The start, change or interruption of AXIASms services
2. The modification on static data in investor share code and securities account
3. The change in the securities balance of the securities account
4. Transactions in the trading system of Athens Stock Exchange
5. Transaction confirmations
6. The composition and valuation of the beneficiary's portfolio

According to the regulatory definitions personal data protection framework, ATHEXCSD acts as its Executor Processing on behalf of Participants who own the role of the Controller.

- ii. Personal Data (hereinafter Data) is defined as any information that concerns identified or identifiable natural person ("data subject") the an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier ID, such as name, ID number, location data, online identifier or to one or more assigning factors whether physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person in question.
- iii. Other terms related to personal data, which are used in present and for which no definition is provided have the meaning given to them attributed to Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016, for the protection of natural persons against of the processing of personal data and for the free circulation of this data and the repeal of Directive 95/46/EC (General Data Protection Regulation) (hereafter "GDPR" or "GDPR").
- iv. "Third countries" means countries outside the European Economic Area Area (EEA).
- v. The terms of this annex do not exempt him under any circumstances Carrying out the Processing from the obligations to which it is subject under the GDPR or other legislation regarding the protection of personal data.

1. The rights and obligations of the Processor

The Controller:

- 1.1. complies with the legislative framework for the protection of personal data data and bears the responsibility of proving its compliance with it,
- 1.2. ensures the existence of a legal basis for the lawful processing of the Data which are processed by the Processor,
- 1.3. has the right and the obligation to make decisions about the purposes 2 and the means of processing the Data,
- 1.4. provide written instructions to the Processor regarding the Processing of the Data that he will carry out on his behalf,

1.5. takes appropriate measures to provide data subjects with each necessary information regarding the processing of his Data by Performing Processing.

2. Obligations of the Processor

2.1. The Processor is obliged to:

2.1.1 is aware of and complies with the GDPR and the generally applicable law legislation on the protection of personal data,

2.1.2. fails to fulfill its obligations hereunder in relation to the Data; in a way that causes the Controller to violate any of its obligations based on the current legislative framework for the protection of personal data.

2.1.3 processes the Data only on the basis of recorded instructions of the Controller Processing, unless otherwise required by the applicable legislative framework, at which the Processor falls under and for which he should provide relevant information to the Data Controller before processing the Data. Any modifications and/or additions to the above orders during the processing of the Data, will always take a written form, including electronics.

2.1.4 immediately inform the Controller if, in its opinion, any order violates the GDPR or other EU or national protection provisions personal data. In the event that the Controller insists on an order which, in the opinion of the Processor, infringes the GDPR or other EU or national provisions on personal data protection, the Processor reserves the right to refuse the execution of the order.

2.1.5 keeps a record of processing activities for the processing it carries out for him Processing Manager, in accordance with the provisions of article 30 par. 2 of the GDPR.

3. Compliance with Confidentiality

3.1. The Processor ensures that the persons authorized to process the Data (permanent/temporary employees representatives, assistants fulfilment, generally added and partners) have undertaken a compliance commitment of confidentiality or are subject to an appropriate regulatory obligation of compliance confidentiality, have knowledge and follow the instructions of the Controller regarding the processing of the Data and apply all appropriate measures for the safeguarding of this Data.

4. Security of processing

4.1. Considering the latest developments, implementation cost and nature, the scope, context and purposes of the processing, as well as the risks different likelihood of occurrence and seriousness for rights and freedoms of natural persons, the Processor ensures throughout its duration processing, to take the necessary technical and organizational measures so that the Data be safe in accordance with the requirements of existing legislation and to are protected against threats to the rights and freedoms of individuals persons, in particular from unauthorized access, disclosure, alteration, deletion or loss.

4.2. The Processor shall assist the Controller in ensuring that compliance with the latter's obligations arising from Article 32 of the GDPR,

providing, among other things, to the Controller information about the technical and organizational measures already implemented by the Processor.

5. Subprocessors (Subcontractors)

5.1. The Processor does not engage another processor (sub-processor/ sub-processor) to fulfill all or part of the processing operations performed on behalf of the Controller Processing without the prior notification of the Processor.

5.2. The Processor receives from the Controller general permission to the use of sub-processors for the assignment of all or part of the operations processing performed on behalf of the Controller. The Executor of it Processing informs in advance, in writing, the Controller of any anticipated changes relating to the addition or replacement of subcontractors processed at least ten (10) business days before the intended addition or replacement, giving the Controller the possibility to object to such changes before using any sub-executor.

5.3. The Processor only uses subprocessors that provide sufficient assurances for the application of appropriate technical and organizational measures measures, in such a way that the processing meets the requirements of the GDPR. The Executor of it Processing must contractually bind the respective subcontractor processing at least with the same obligations regarding the protection of Data provided herein, including the obligation to allows and facilitates controls, including inspections that are carried out by the Data Controller or by another controller authorized by him Controller, in particular to provide adequate assurances for the implementation of the appropriate technical and organizational measures, meeting the requirements of the GDPR.

5.4. In any case, the Processor remains fully responsible for of the Processing Manager to fulfill the obligations of the subcontractor processing or any other third party regarding protection data.

6. Data transfers to third countries or international organizations

6.1. Any transmission of personal data to third countries or internationally organizations by the Processor the Processing is carried out only on the basis of recorded instructions of the Controller and always in compliance with chapter V of the GDPR.

6.2. In case of data transfers to third countries or international organizations, the which the Processor has not received an order from the Controller to perform, but which are required under EU or member state law to to which the Processor is subject, the latter informs the Responsible Processing for the legal requirement in question prior to processing, unless Art due to law prohibits this type of information for serious public reasons interest.

6.3. Therefore, without recorded orders from the Controller, the Executor Processing may not, in the context of this:

- a. to transmit personal data to a controller or executors

- the processing in a third country or in an international organization;
- b. to transfer the processing of personal data to subcontractors processing in a third country;
- c. to process personal data himself in a third country.

7. Subscription to the Controller

7.1. Taking into account the nature of the processing, the Processor assists the Processing Manager with appropriate technical and organizational measures, to his extent possible, when fulfilling the obligations of the Processor to responds to requests for the exercise of the subject's rights data, as defined in chapter III of the GDPR.

7.2. The Processor is obliged to immediately forward to the Responsible Processing any request that may be received for the exercise of their rights subjects whose Data is processed pursuant to this.

The processor does not respond to the above mentioned requests unless it has authorized for this purpose by the Data Controller.

7.3. The Processor, taking into account the nature of the processing and the information it has, helps the Controller to ensure the its compliance with:
- the obligation of the Processor to carry out an impact assessment study regarding Data protection. The assistance of the Processor is achieved by participating in interviews and/or completing questionnaires to provide the necessary information to the Responsible Processing, regarding the processing that the former carries out on its behalf Processing Manager. The obligation of the Processor to seek the opinion of the competent supervisory authority principle, before processing, when the impact assessment on protection data indicates that the processing would cause a high risk in the absence risk mitigation measures by the controller.

8. Notification of personal data breach

8.1. The Processor is obliged to inform the Responsible without delay Processing upon becoming aware of potential, accidental, unauthorized, or illegal destruction, loss, alteration, or disclosure of Data or any eventual, accidental, unauthorized or illegal access to them (hereinafter "Data Breach"). In addition, he is obliged to provide the Controller any information, which it has, and which the Controller can reasonably request in connection with the Data Breach.

8.2. The Processor must immediately take all possible measures for him limiting the effects of the Data breach, as well as to receive any measure necessary to remedy the breach.

8.3. The Processor assists the Processor in its fulfillment of his obligation to investigate the possible incident, to notify the competent authority supervisory authority any breach of the Data, as well as to carry out notification of the breach to Data Subjects.

8.4. The above obligations fall on the Processor and on case where the violation concerns another sub-executor of the processing that the Executor uses Processing.

8.5. The Controller is entitled to request any additional information about the event and the circumstances, technical or otherwise, from which the breach occurred and the Processor is obliged to respond immediately.

9. Data Deletion/Destruction

9.1. At the end of the cooperation or at any time, at the request of the Manager Processing, the Processor must immediately delete/destroy any Data of the Data Controller and any existing copy thereof has been created, unless there is a legal obligation of the Processor to preserve them. In the latter case, the Processor informs the Data Controller as soon as possible about the said legal obligation and undertakes to process the Data exclusively for the purposes and the duration provided for in the legislation.

9.2. The Processor ensures that the deletion/destruction of the Data is carried out by taking the appropriate technical and organizational measures for its security of said processing.

9.3. The Processor must carry out the deletion in question within the time frame set by the Data Controller and confirm in writing to the Data Controller the deletion/destruction of the Data.

10. Audit and Inspection

10.1. The Processor is obliged at the request of the Controller Processing to make available to him any necessary information for the purpose of verification of the former's compliance with the provisions for the protection of personal data and the present and enables and facilitates the implementation of supervisory controls, including inspections, by the Responsible Processing or by another person acting at the behest of the Controller Processing.

10.2. The Controller will inform the Processor in writing for conducting the audit at least ten (10) working days before conducting the control, disclosing the identity details of natural persons, which will conduct the audit as well as its estimated duration.

11. Commencement and Termination

11.1. The terms herein apply throughout the Data processing by the Processor regardless of any termination of the cooperation and may not be terminated unless their place has been taken by other terms which govern the processing of Data by the Processor.

11.2. If the Data processing operations by the Processor are terminated and the Data deleted or returned to the Controller as set forth herein, this shall cease to apply.