

ACRO SECURITIES HF.

RULES ON HANDLING INFORMATION ABOUT CUSTOMERS

AUGUST 2021

# **RULES ON HANDLING INFORMATION ABOUT CUSTOMERS**

AUGUST 2021

## **1. Purpose and scope**

- 1.1. These goals are set, based on Art. 19 (b) of Act no. 161/2002 on Financial Undertakings to ensure the protection of information about clients of ACRO Securities hf. (hereinafter "*the company*").
- 1.2. The goals of the rules are to promote that the company's employees' handling of information about clients will conform to good business practice and the fundamental principles of the protection of personal data and respect for private life, cf. Act no. 90/2018 on Data Protection and the Processing of Personal Data, and confidentiality under Art. 58 of Act no. 161/2002 on Financial Undertakings.
- 1.3. The Rules apply to the work of all employees, board members, chartered accountants, contractors, and all others undertaking work on behalf of the company (hereafter jointly called employees). The rules cover all information in the company's custody regarding clients' trading or private matters in whatever form the information may be.

## **2. Saving of information about clients**

- 2.1. The company saves information that clients provide when they begin trading with the company, as well as information acquired later from clients.
- 2.2. Depending on circumstances, information about clients is saved digitally or on paper. Information in digital form shall be saved in a secure medium where security measures are taken. Documents on paper shall be filed in document storage suitable for saving documents. When deciding on the storage media of paper documents and digital data, consideration shall focus on the value of the content being preserved and its importance.
- 2.3. Information about clients shall be destroyed when there is no longer an objective reason to preserve it. The objective reasons to preserve information include instructions in statutes, or that the company still works with disclosures accordant with the original purpose of collecting them. When destroying information, the means used shall ensure certain and permanent destruction.

## **3. Employees' access to documents**

- 3.1. Employees' authorisation to access and utilise information about the company's clients solely covers what is necessary for their work.
- 3.2. Employees' access to documents shall be controlled to ensure this goal, for example, through access to workstations, the allocation of access, and passwords.
- 3.3. When in doubt, the compliance officer shall be consulted.

## **4. Confidentiality and dissemination of information**

- 4.1. Employees shall be bound by confidentiality regarding everything of which they gain knowledge in carrying out their work, and regarding clients' business or private matters, cf. Art. 58 of Act no. 161/2002 on Financial Undertakings. Confidentiality continues even if employees quit their job.
- 4.2. Despite Art. 4.1, employees may provide information about clients:
  - 4.2.1. based on a clear statutory duty to do so.
  - 4.2.2. if a lawful request comes from the client involved, his guardian or agent; or

4.2.3. if a lawful request comes from official parties, such as the police or the Financial Supervisory Authority, Iceland.

4.3. Despite the above, the company may, on their own initiative, need to disseminate information, for example, as a mandatory notification party, based on current provisions of law.

4.4. A request to disseminate information about clients to a third party shall be in writing. In doubtful instances, the compliance officer will make a decision on the dissemination of information in consultation with the managing director.

4.5. If information is disseminated to a third party, based on the above authorities, an employee shall admonish the recipient that he is bound by confidentiality under Art. 58 of Act no. 161/2002.

## **5. Clients' right to information**

5.1. The company's clients can request to know which information about them the company has processed and the purpose of that processing.

5.2. Such a request shall be in writing, logically supported and objective, and sent to the compliance officer, who is the intermediary regarding the delivery of information. The compliance officer may reject a client's request if delivery of the information contravenes the perspective of personal data protection and the company's confidentiality under Art. 58 of Act no. 161/2002 on Financial Undertakings.

## **6. Security measures**

6.1. The company is responsible for the processing of personal information being accordant with laws and regulations and take appropriate security measures to ensure this is so.

6.2. All information regarding clients' business or private matters shall be handled with the utmost caution to ensure that it is not lost or falls into the hands of unauthorised parties. Particular caution shall be employed in its preservation, photocopying, transmission, computer registration, and destruction.

6.3. Digital storage of data shall be in a secure medium, where security measures are accordant with demands each time. In selecting security measures, consideration shall be given to the risk of the processing and the nature of the data to be protected.

## **7. Supervision**

7.1. An internal chartered accountant supervises that these rules are followed.

## **8. Entry into force and publication**

8.1. These rules enter into force when signed by the Board of Directors and shall be published on the company's homepage.

Approved by the Board of Directors of ACRO Securities on the 10<sup>th</sup> of August 2021