INTERNAL REGULATIONS
FOR SAFETY, MANDATORY FOR
EMPLOYEES HAVING ACCESS TO RECORDS OF PERSONAL DATA
OF INVESTMENT INTERMEDIARY "FACTORI" AD

I. GENERAL

Art. 1. (1) These internal rules regulate the conditions and procedure for keeping records under the Personal Data Protection Act (PDPA), as well as the organization and procedure for exercising control over the processing of personal data by the employees of an Investment Intermediary (II)" FACTORI" AD.

(2) Processing of personal data is any action or set of actions that can be performed in relation to personal data by automatic or other means, such as collection, recording, organization, storage, adaptation or modification, restoration, consultation, use, disclose or transmit, distribute, provide, update or combine, block, delete or destroy the data.

(3) Processing of personal data also consists in ensuring access to certain information only for persons whose official duties or a specifically assigned task require such access.

Art. 2. (1) The internal rules are adopted in order to regulate:

1. Creation of procedures and mechanisms to guarantee the inviolability of the personality and private life of clients and employees of the II by providing protection against unlawful processing of the personal data related to them in the process of processing and movement of the data;

2. The types of registers that are kept at the II and their description.

3. The necessary technical and organizational measures to protect the personal data of the above-mentioned persons from illegal processing (accidental or illegal destruction, accidental loss, illegal access, modification or distribution, as well as from all other forms of personal data processing).

4. The rights and obligations of the officials processing personal data and/or the persons who have access to personal data and work under the direction of the personal data processors, their responsibility in case of failure to fulfill these obligations.

5. Incident Reporting, Management and Response Procedures.

(2) The internal rules are approved, supplemented, amended and canceled by the Board of Directors (BoD) of II "FACTORI" AD.

Art. 3. These internal rules apply to personal data within the meaning of the Personal Data Protection Act and are issued on the basis of Ordinance No. 1 on the minimum level of technical and organizational measures and the permissible type of personal data protection of the Personal Data Protection Commission.

Art. 4. The II is a personal data controller within the meaning of Article 3, Paragraph 1 of the Personal Data Protection Act and is registered with the Commission for Personal Data Protection.

Art. 5. (1) Personal data is any information relating to a natural person who is identified or can be identified directly or indirectly through an identification number or through one or more specific characteristics.

(2) Personal data are collected for specific, precisely defined and legal purposes, are processed lawfully and in good faith and may not be further processed in a manner incompatible with these purposes.

II. PROCESSING OF PERSONAL DATA

Art. 6. (1) The administrator entrusts the processing of personal data to his employees. The processing can be assigned to more than one data processor, according to the specifics of the official functions performed by them and in order to distinguish their specific duties.

(2) Those processing personal data act only on the instructions of the administrator, unless otherwise provided by law.

Art. 7. (1) The personal data in the registers are collected by the personal data administrator, respectively - the personal data processor, through an oral conversation and/or on paper, as well as by copying the identity card of the clients of the II given the requirements of the Law on the markets of financial instruments, the acts on its implementation and the directly applicable Delegated Regulations of the EC.

(2) The data processor informs the person, respectively the client of the II, about the need to collect the data and the purposes for which they will be used.

(3) The storage of personal data on paper is carried out by storing the data: in folders in certain lockable cabinets and the paper media are not taken out of the office (address of management) of the II.

TYPES OF REGISTERS TO BE KEPT WITH THE INVESTMENT INTERMEDIARY TYPES OF REGISTERS	TYPES OF PERSONAL DATA	DIRECTION
1. Register "Employees"	Three names, address, phone, social security number, criminal record Paper and electronic media; The protection measures taken are described in these rules; Data are reviewed every 6 months; Provision to third parties is defined in these Rules.	**"Financial - Accounting"**
2. Register "Customers"	Three names, address, telephone, e-mail, nationality, copy of ID card (identity document) Paper and electronic media; The protection measures taken are described in these rules; Data are reviewed every 6 months; Provision to third parties is defined in these Rules.	**Back Office, Regulatory Compliance**

III. FORMS OF KEEPING THE REGISTERS

Art. 8. Form of organization and storage of personal data on paper:

(1) Folders are located in the II's office in special lockable cabinets. The rights and obligations of employees are regulated in their job descriptions. The granting, modification or termination of authorized access to registers is controlled by the Executive Director and the Regulatory Compliance Department of the II.

(2) The location of the cabinets with personal data of employees and contractors is in a separate part of a room intended for independent work of the personal data processor.

(3) Carrier (form) for provision of data by natural persons - personal data for each person is collected in fulfillment of a legal obligation (the provisions of laws, by-laws, codes and others) through:

- oral interview with the person;
- paper medium - written documents (applications) on current issues in the work process submitted by the person;
- copies of identity documents provided with the consent of counterparties/clients and employees of the II.

(4) Personal data from customers is submitted to the II, represented by certain officials (brokers and members of the Board of Directors).

(5) The possibility of giving others (the person himself and authorized state bodies) access to personal data during their processing is expressly regulated in these Internal Rules.

Art. 9. Form of organization and storage of personal data on a technical medium:

(1) Personal data (three names, social security number, nationality) are entered on a hard disk of a server on the computer network (in case they are processed by more than one employee) or on an isolated computer (in case they are processed by only one employee or from the respective workplace cannot be provided access to a server). The computer is connected to the local network, with secure access to personal data, with which only the personal data processor can work with low and medium level protection measures, in accordance with the requirements of Ordinance No. 1 of the CPLD.

(2) When working with the data, the corresponding processing software products are used. They can be adapted to the specific needs of the data controller. Data is entered into the computer from paper.

(3) Only those working with it have access to the files for processing personal data. Media containing personal data may only be distributed if the data is encrypted or if some other mechanism is used to ensure that the data cannot be read or altered in transit.

(4) The location of the server is in the premises of the II, and a backup server for back-up (reserve archive copy, according to the requirements of the Financial Supervision Authority) of the data is maintained on a separate server. The location of the computers is in an isolated room for the individual work of the personal data processor under the register (working room of the "Back Office" department).

(5) Only a person/persons processing personal data designated by the Executive Director can access the files for processing personal data through a password for opening these files known to him/her. In the case of II, these are the employees of the "Back Office" Division.

(6) Protection of electronic data from illegal access, damage, loss or destruction is ensured by maintaining anti-virus programs, periodic archiving of data, as well as by storing the information on paper. When the data resides on a server, it is backed up automatically. When the data is located on isolated computers, it is backed up by the operator of the relevant computer (the personal data processor).

IV. MEASURES TO GUARANTEE THE LEVEL OF SECURITY

Art. 10. (1) Technical measures to guarantee the level of security:

- the computer servers for the database of the Investment intermediary are at a modern technical level.

- computer work configurations use licensed operating systems in accordance with the requirements of the application software for working with personal data, they are competently balanced and functionally optimized.

(2) Uninterruptible power supplies (UPS) should be provided for all computer configurations, servers and communication means on which the proper maintenance of personal data bases depends.

(3) The minimum set of system software of each working computer configuration includes:

1. modern operating system according to the requirements of the used application software with installed security packages;
2. anti-virus software with automatic update and constant scanning enabled;
3. an activated firewall and uninstalled communicators providing access outside the II's computer network and creating prerequisites for identifying the user's II address and for malicious software and mobile code to access the computers.

(4) Access to the computer network and to the software for working with personal data is carried out by officials with special passwords, which are provided by an employee responsible for the IT security of the II, in accordance with the requirements of the Internal Rules of the II and the Financial Supervision Authority. The systems log the access time. The exchange and sharing of personal passwords or passwords to access II systems between employees is prohibited.

(5) Any erasure, modification of personal data stored on automated information systems is prohibited, except when this is done for the purpose of error correction or when destruction of personal data carriers by the II in the presence of the legal conditions for destruction.

Art. 11. Physical measures to ensure the level of security:

(1) In the premises where computer and communication equipment are located, the following shall be ensured:

- access restriction system;

(2) All work premises are locked outside the established working hours and access to them is regulated.

(3) All magneto-optical media, which are used to record personal data as a result of archiving and making copies of the databases, are transferred and stored in a fireproof and waterproof cabinet, which is locked, and the key is kept by "Kadri and TRZ" at the II. The control over the use of these media is carried out by the executive director and the internal control of the II.

(4) The II has a special secret safe for storing personal data and magnetic carriers with such data.

(5) The II defines an area with controlled access around the work desks of the back office employees and the internal control officer.

(6) The II has 3 types of fire extinguishers, providing extinguishing of fires with water, dust and gas in view of potential fire threats. There is a centralized fire alarm and fire extinguishing system in the II office.

(7) The building in which the II office is located is guarded around the clock and has centralized access control and video surveillance.

Art. 12. Organizational measures to guarantee the level of security:

(1) Security of the work premises is organized within the framework of the security of the entire building.

(2) It is prohibited to use portable personal data carriers in the II units where personal data is processed (flash drives, portable hard drives, etc.).

(3) Working computer configurations, as well as the entire IT infrastructure, including Internet access, are used for official purposes.

(4) A check of all working computer configurations is carried out every 12 months by a relevant person responsible for the IT and technical security of the II.

(5) The transfer of personal data over (via) the Internet is prohibited, and when this is done via e-mail, encryption of the data must be ensured.

(6) When repairing computer equipment on which personal data is stored, its provision to the service organization is carried out without the devices on which personal data are stored.

(7) The executive director of the PE determines the processors of personal data for the various types of registers that are kept in the investment intermediary.

(8) The II provides the following basic measures for personal protection and, in relation to its employees, provides:

1. knowledge of the regulations in the field of personal data protection;
2. knowledge of the internal rules for the protection of personal data;
3. knowledge of the dangers for the personal data processed by the administrator;
4. sharing of critical information between staff (e.g. IDs, access passwords, etc.);
5. consent to undertake an obligation not to distribute personal data;
6. training;
7. training of personnel to react to events threatening data security.

(9) Personal protection measures guarantee access to personal data only to persons whose official duties or a specifically assigned task require such access, subject to the "Need to Know" principle.

(10) Persons may start processing personal data after becoming familiar with:

1. the regulations in the field of personal data protection;
2. the policy and guidelines for the protection of personal data;
3. the dangers for the personal data processed by the administrator.

(11) The employees of the II sign a declaration of non-disclosure of personal data to which they have gained access during and on the occasion of the performance of their duties.

(12) Documentary protection is a system of organizational measures in the processing of personal data on paper. The main measures of documentary protection are:

1. determination of the registers to be maintained on paper;
2. determination of the conditions for processing personal data - personal data are processed when concluding contracts with clients/counterparts and when starting work at the II. The processing takes place in a specially separated part of the II's office by Back Office and Front Office employees;
3. regulation of access to the registers - access to the registers is carried out by the "Back Office" and, accordingly, by the "Regulatory Compliance" department;
4. control of access to the registers - carried out by the Executive Director and by the "Regulatory Compliance" department;
5. determination of storage periods - according to the requirements of the PFFI, the investment intermediary stores the personal data of its clients for at least 5 years from the establishment of relations with clients;

6. reproduction and distribution rules - personal data are not reproduced or distributed, except in the cases provided for by law, to authorized state institutions or to the persons who provided the data;

7. destruction procedures - carriers of personal data are destroyed by an II committee consisting of: a member of the Board of Directors, an employee from the "Regulatory Compliance" department and a Back Office employee. The destruction takes place only if there are legal prerequisites for it, an assessment of the regulatory risk, absence of legal obstacles and when a protocol for the destruction is drawn up;

8. procedures for verification and control of the processing - the control of the processing of personal data is carried out by the executive director and the "Regulatory Compliance" department regularly and/or incidentally.

V. RIGHTS AND OBLIGATIONS OF EMPLOYEES

Art. 13. Employees of the II are obliged to observe and implement the Internal Rules, in accordance with their job characteristics.

Art. 14. When processing personal data, the employee signs a declaration that he is familiar with the Personal Data Protection Act, as well as with the current Internal Rules.

Art. 15. (1) The administrator provides personal data in fulfillment of legally established obligations.

(2) Personal data is provided ex officio between employees in the II after a justified request, in accordance with the functional duties of a given employee or unit and upon notification to the "Regulatory Compliance" department. The request may also be in oral form when the official duties of the person require the processing of personal data or when the right of access is part of the employee's job description.

Art. 16. (1) Every client (counterparty) of the II who is a natural person, has the right of access to personal data concerning him, stored and processed by the II.

(2) The right of access is exercised with a written application/or an electronic application in accordance with the Law on Electronic Documents and Electronic Signatures/ to the Executive Director of the II or by a person expressly authorized by him, through a notarized power of attorney. Submitting the application is free.

(4) The application is submitted to the II.

(5) Access to the person's data is provided in the form of: verbal reference; written reference; review of the data by the person himself or by the authorized person; a copy of the processed personal data on a preferred medium or provision by electronic means, except in cases where this is prohibited by law.

(6) Upon submission of an application for securing access to personal data, the representative of the Investment Intermediary or a person authorized by him shall examine the applications and order the personal data processor to provide the requested access to the person in the form preferred by him.

(7) The deadline for considering the application and ruling on it is 14 days from the day of its submission.

(8) The investment intermediary shall notify the applicant in writing of its decision - it may be to grant access or deny access. The notification is made in person against a signature or by mail with return receipt.

(9) Denial of access to personal data must be motivated. The grounds for refusal are: 1. when the data does not exist; 2. when the data cannot be provided on a certain legal basis.

Art. 17. (1) Personal data shall be provided to third parties only after obtaining written consent from the person to whom the data refer.

(2) If consent is not received from the person or if consent is expressly refused, the data shall not be provided.

(3) The person's consent is not required in cases where the II is an obliged subject by law and the data is requested by state bodies and institutions within their powers

VI. REPORTING PROCEDURES, INCIDENT MANAGEMENT AND RESPONSE

Art. 18. (1) When an incident occurs and is established, it is immediately reported to the person responsible for personal data protection;

(2) A diary is kept for the incidents, in which the supposed time or period of occurrence, the time of detection, the time of reporting and the name of the employee who made the report must be entered.

(3) After analysis by the Executive Director and the "Regulatory Compliance" department, the consequences of the incident and the measures taken to eliminate them are recorded in the diary.

(4) In cases of the need to restore data, the procedure is carried out after the written permission of the person in charge of personal data protection, and this is reflected in the data backup and recovery log.

(5) In cases of password compromise, it is replaced with a new one, and the event is reflected in the incident log.

Art. 19 (1) Every employee of the II is considered informed of the risks of leakage of personal data for a client and of the responsibility that is borne in such an event. The risk of leakage of personal data is related to the violation of the privacy of a client/contractor, as this would make known the name, address and social security number of a given client.

(2) Each employee of the II understands, agrees and accepts to comply with the ban on non-distribution of personal data of clients and/or contractors of the II, which became known to him during or on the occasion of the performed functions.

ADDITIONAL PROVISIONS

For the purposes of these Internal Rules:

§1. "Administrator of personal data" is II "FACTORI" AD represented by the Executive Director

§2. "Processor of personal data" are officials at FACTORI AD.

§3. The internal rules enter into force from the day of their adoption by the Board of Directors of the II. An integral part of these Rules is the assessment of the level of impact of each registry.

§4. These Rules have been adopted by Decision of the Board of Directors of FAKTORI JSC on the basis of Art. 23 of the Personal Data Protection Act.

All employees and persons working under an II contract have been notified of these Rules and of their obligation to comply with them.