

# **REGULATION OF THE MINISTER OF THE INTERIOR**

## **(No 13, January 23, 2008)**

### **Procedure for the registration and processing of data collected by the Financial Intelligence Unit**

The regulation is enacted by § 43 (6) of the Money Laundering and Terrorist Financing Prevention Act.

#### **Chapter 1**

#### **GENERAL PROVISIONS**

##### **§ 1. General provisions**

- (1) The present regulation shall govern the procedure for the registration and processing of the data collected in the Financial Intelligence Unit.
- (2) The supervisory activities of the Financial Intelligence Unit (hereinafter the "FIU") shall be governed by the code of conduct for the supervisory activities of the FIU approved by the head of the FIU.
- (3) A notification in the meaning of the present regulation is a written notice or a notice which can be reproduced in a written form prepared according to the form confirmed by the regulation of the Minister of the Interior submitted by obligated persons (hereinafter "obligated person) specified in section 3 of the Money Laundering and Terrorist Financing Prevention Act to the FIU as regards a suspicion of a money laundering or terrorist financing transaction or as regards a transaction specified in subsection 32(3) of the Money Laundering and Terrorist Financing Prevention Act.
- (4) RABIS is the FIU's electronic database into which the notifications and other information received from obligated persons are collected and stored and in which this data is processed.

##### **§ 2. The records of the FIU**

- (1) The records of the FIU shall:
  - 1) consist of the notifications received from obligated persons in the meaning of the Money Laundering and Terrorist Financing Prevention Act concerning transactions concerning a money laundering or terrorist financing suspicion;
  - 2) consist of the notifications concerning the application of financial sanctions provided in the International Sanctions Act;
  - 3) be composed as a result of the analysis carried out by the FIU and include additional information as regards transactions, participants thereof and other circumstances concerning the transaction collected by the FIU in the cases provide by law;
  - 4) include information about all of the suspicious and unusual transactions and activities which have become known to the FIU in other ways.
- (2) The records of the FIU also include the data concerning bank or business secrets collected when exercising supervision prescribed in clauses 37 (1) 4) and 9) and chapter 5 of the Money Laundering and Terrorist Financing Prevention Act over the activities of the subjects of the act.

### **§ 3. Records management of the FIU**

- (1) The correspondence of the FIU shall in general be exchanged by means of digitally signed e-mails. Documents shall be digitally signed by the head of the FIU, an official substituting for him or her or an official appointed by him or her.
- (2) The letters and other postal items addressed directly to the FIU shall be opened only in the FIU.
- (3) Notifications shall be registered in the RABIS database.
- (4) The FIU has its own separate document register which is located in an FIU desktop computer connected to a local area network. Access to this document register is granted only to the employees of the FIU. All of the letters and postal items sent and received by the FIU in connection with the prevention of money laundering and terrorist financing shall be registered in the register. The letters sent are put into an envelope carrying an address and the closed envelopes are forwarded to the records management office of the Central Criminal Police for sending.
- (5) Precepts are registered in a separate document register of the FIU. An electronic copy of the precept is stored in the RABIS database with the folder in the framework of which the precept was drafted.
- (6) Internal orders, directives and other correspondence related to the position of the FIU in the structure of Central Criminal Police and its administrative management are registered pursuant to the procedure provided by the records management guidelines of the Central Criminal Police.

## **Chapter 2**

### **REGISTRATION AND PROCESSING OF INFORMATION**

#### **§ 4. Collection of information**

- (1) A notification is sent to the FIU by means of a web-based notification form available at the public webpage of the FIU, or by e-mail, fax or post.
- (2) Enquiries and information received from investigative bodies or agencies which discharge the functions of foreign FIUs are treated as notifications.
- (3) The notification concerning a suspicious transaction determined in the course of supervision procedures is made by the supervision service.

#### **§ 5. Registration of information**

- (1) The notification received by the FIU is registered in a separate database of the FIU – RABIS – in which it will be assigned a registration number, also in which its sender's identity, the number given to the notification by the sender, its date, data about the client or parties to the transaction and other information concerning the transaction will be recorded. Other materials added to the notification will be recorded in RABIS with the notification.
- (2) Notifications sent via the web-based notification environment on the public webpage of the FIU are available in a encrypted form. Encrypted notifications are dumped by the data processing specialist of the FIU to the RABIS database in which it is decrypted.
- (3) Notifications received by e-mail are opened by the head of the FIU, an official

substituting for him or her or an official appointed by him or her.

- (4) Notifications received by fax or post are scanned or transformed into a digital form in some other form by the data processing specialist before registration. Originals are either annexed to the inspection folders or archived.
- (5) The data collected by the FIU independently are registered as notifications in RABIS by recording the official of the FIU as a sender.
- (6) If it becomes evident during inspection that the submitted notification does not conform to the requirements or there are omissions in it, the notification is registered pursuant to general procedure and its sender is notified in writing of the existing omissions which need to be eliminated within the specified term.

#### **§ 6. Information analysis**

- (1) The head of the FIU or an official substituting for him or her shall look through all of the notifications listed in § 1 (3) of the present regulation.
- (2) The notification received from legally obligated persons with the notation “Urgent” and foreign enquiries will be reviewed immediately at the FIU; such notifications are analysed based on the existing information and a decision is made on the use of measures for preserving the assets. Other notifications will be reviewed within a reasonable time by using the special criteria for the allocation of notifications and priority-rating imposed by the head of the FIU.
- (3) When a notification is received, the official stated in subsection 1 of the present section will perform an initial analysis based on the information available at the FIU. If necessary, additional information is gathered from the registers and databases available to the FIU. As a result of the initial analysis the official shall decide whether it could involve a suspicion of money laundering, terrorist financing, offences related thereto or other offences.
- (4) If it appears during the initial analysis that the suspicion based on which the notification was submitted is not confirmed, the notification shall be archived in the RABIS database.
- (5) If it occurs during the review that additional information needs to be collected in order to identify whether the data described in the notification is important for the detection of money laundering or terrorist financing or related offences or whether it is important for the pre-trial procedure, an inspection folder will be opened based on it.
- (6) Each inspection folder shall be assigned a separate number and an official responsible.
- (7) The head of the FIU, an official substituting for him or her or an official appointed by him or her shall assign a deadline of up to three months for reviewing the inspection folder based on the complexity of the case. If the case is particularly complicated or because of the international nature of a case it is possible to prolong the deadline based on a motivated request submitted by the official responsible.
- (8) Based on the content of the enquiry a 1-month deadline shall be established for answering the external enquiries. Urgent requests have to be answered within two workdays.
- (9) Precepts, enquiries, correspondence and other documents are registered in a separate database of FIU and stored in the same inspection folder.

- (10) The FIU will retain the inspection folders usually in an electronic form in RABIS database employing respective security measures to ensure the preservation of the electronic folders and the confidential information contained therein. The documents received on paper will be retained in their original form and scanned into a digital inspection folder.
- (11) If the transactions which are being analysed in an opened inspection folder are connected to notifications which have arrived earlier or arrive later, the decision will be made as regards including them into the already opened folder in RABIS database.
- (12) If it turns out as a result of the analysis that the opened folder concerns the transactions related to the inspection folder opened earlier, the folders will be joined and assigned a common number. If it occurs that the materials in the folder include the elements of another independent offence besides the suspected offence being analysed, these materials may be put separately into another folder.
- (13) The opening, joining, separating of folders and the assignment of responsible officials is in the competence of the head of the FIU, the heads of the FIU offices or an official appointed by the head of the FIU.
- (14) When analysing the notification specified in subsection §1 (3) of the present regulation, the FIU shall use all of the possibilities provided in Money Laundering and Terrorist Financing Prevention Act to obtain additional information.
- (15) The enquiries submitted to foreign competent authorities and the administrative legislation of the FIU shall be signed by the head of the FIU or an official appointed by him or her. Information exchange with foreign competent authorities will take place in the manner provided in this section. Information is exchanged with foreign competent authorities by post or fax on the form of the FIU or electronically via the secured international information exchange system – Egmont Secure Web.
- (16) If the suspicion which formed the basis for the notification was not excluded during processing and based on the existing information there is not sufficient basis for preparing a report of a criminal offence, the FIU may make a notation about the existence of information in the surveillance activity information system by assigning a necessary access category for it.
- (17) The material gathered based on the analysis is submitted with a summary by the responsible official to the head of the FIU, the head of a structural unit or the official substituting him or her for making a decision as to whether to send it to investigative bodies, a competent authority of a foreign country or designate it to be preserved at the FIU.
- (18) The FIU shall not release the notification as regards the suspicion of money laundering, its copy or transcript and data as regards the person who submitted it.
- (19) If information is forwarded to a foreign competent authority, a notation is made concerning the conditions for the use of such information.

### **Chapter 3**

#### **TRANSMISSION AND RELEASE OF DATA**

##### **§ 7. Transmission of materials**

- (1) If elements of money laundering, terrorist financing or related offences or other

- offences occur, the FIU shall immediately send the information to a competent authority. Forwarded materials shall be treated as a report of criminal offence.
- (2) If the collected materials indicate to an offence in the competence of the jurisdiction of another country, the material is sent as a notification to the authority performing the functions of an FIU in the country in question.
  - (3) When forwarding the materials the responsible official shall prepare a consignment note, ensure that a copy of the materials shall be retained by the FIU and forward the material with the consignment note to the head of the FIU or the official of the FIU substituting him or her for signing.
  - (4) If the FIU has applied restrictions for ensuring the retaining of information, it shall submit the materials to the investigative body as soon as possible, but not later than 10 workdays before the end of the restriction period. In such case the investigative body shall decide the question of asset seizure in the manner established in the Code of Criminal Procedure before the expiry of the restriction applied by an administrative act of the FIU.

#### **§ 8. Data release**

- (1) The FIU does not release data unless otherwise provided by law, international agreement or present regulation.
- (2) The FIU forwards important data, including data containing tax secrets and information subject to banking secrecy, to the prosecutor, investigative body or court if it is necessary for the prevention, detection or pre-trial procedure of money laundering, terrorist financing or related offences or other offences.
- (3) The data specified in subsection 2 of the present section are released by the FIU on its own initiative or based on a reasoned request submitted by the agencies specified in subsection 43(3) of Money Laundering and Terrorist Financing Prevention Act.
- (4) The FIU may disclose data collected during administrative proceedings to the investigative bodies for the prevention, detection or pre-trial proceeding of offences.
- (5) The decision as regards the disclosure of data is made and the documents connected to the issue of data shall be signed by the head of FIU, an official substituting for him or her or an official appointed by him or her.
- (6) When data are released from the FIU restrictions may be provided for the use of data.
- (7) Other data exchange shall take place pursuant to the law and inter-agency cooperation agreements.

#### **§ 9. Cooperation with the Security Police Board in the prevention of terrorist financing**

- (1) In the prevention of terrorist financing the FIU cooperates with the Security Police Board pursuant to the provisions of section 45 of the Money Laundering and Terrorist Financing Prevention Act.
- (2) Notifications concerning terrorist financing are forwarded by the head of the FIU, an official substituting for him or her or an official appointed by him or her to the contact person appointed by the commissioner of the Security Police Board in a

digitally signed form and in an encrypted format by e-mail, making a relevant notation in the RABIS database.

- (3) The contact person of the FIU designated by the commissioner of the Security Police Board:
  - 1) shall receive important data specified in subsection 45(2) of the Money Laundering and Terrorist Financing Prevention Act from the FIU;
  - 2) shall analyse the notifications concerning terrorist financing independently or in cooperation with the FIU;
  - 3) shall review the inspection folders opened for the detection of terrorist financing, if necessary;
  - 4) shall submit the notification concerning the suspicion of terrorist financing of the Security Police Board to the FIU for inspection;
  - 5) shall give feedback on a quarterly basis to the FIU as regards the results of the analysis of notifications concerning terrorist financing suspicions inspected by them. If elements of crime are detected and criminal procedure is commenced, it shall notify the FIU immediately;
  - 6) shall be guided by the data protection requirements provided in the law and present regulation.

#### **§ 10. Feedback**

- (1) When fulfilling the requirements specified in clause 2 of subsection 37 (1) of the Money Laundering and Terrorist Financing Prevention Act the FIU shall notify the persons who have submitted notifications to it annually of how the data was used if the notifications were used to commence criminal procedure or if these were annexed to an ongoing criminal matter.
- (2) The assistant at the FIU shall register the notification in the document register of the FIU and shall make a relevant notation in the RABIS database.

### **Chapter 4**

#### **APPLICATION OF RESTRICTIONS**

#### **§ 11. Introduction of restrictions provided in section 40 of the Money Laundering and Terrorist Financing Prevention Act**

- (1) If an obligated person has submitted the notification to the FIU with a notation “urgent” and has suspended the transactions with the assets, the FIU shall review the notification immediately and shall make a decision as regards the introduction of a restriction on the account or the disposal of the assets which are the object of the transaction.
- (2) The decision concerning the suspicion of a transaction or the application of a restriction as regards the disposal of an account or assets which form the basis of the transaction is made by the head of the FIU based on the proposal of the official responsible or of the head of a FIU office.
- (3) If a competent body of another country submits an enquiry and a reasoned request to impose a restriction on the assets to the FIU, the restriction will be applied pursuant to general procedure and the competent body of the other country shall be notified immediately.

- (4) After making a decision as regards the necessity to suspend a transaction or to apply a restriction on the disposal of the account or other assets forming the object of the transaction, the official responsible shall draft a respective precept which shall be signed by the head of the FIU, an official substituting for him or her or an official appointed by him or her
- (5) The precept shall be registered pursuant to the applicable procedure and shall be forwarded to the possessor or owner of the assets or shall be delivered against signature.
- (6) If the possessor or owner of the assets does not submit evidence as regards the legal origin of the assets within 30 working days since the suspension of the transaction or the introduction of the restriction to use the account, the head of the FIU, an official substituting for him or her or an official appointed by him or her shall decide based on the materials of the folder upon the necessity to introduce a second restriction and to impose a deadline. The respective notation shall be entered into the RABIS database.
- (7) If the owner or possessor of assets submits proof as regards the origin of the assets on time, the responsible processing official shall immediately inspect the data by using all of the possibilities provided in the law and shall submit its opinion as regards the cancellation or continuation of restrictions to the head of the FIU or the official substituting him or her.
- (8) If in the course of analysis a need arises to restrict the use of assets or to seize the assets in another country, a respective enquiry and/or reasoned request shall be drafted and it shall be sent to the competent body of the other country.
- (9) If the FIU decides to continue with the introduction of restrictions, it shall notify the possessor or owner of the account or assets immediately. The respective precept shall be registered pursuant to the applicable procedure and shall be forwarded to the possessor or owner of the assets or shall be delivered against signature.
- (10) In order to apply subsection 40(6) of Money Laundering and Terrorist Financing Prevention Act the FIU shall make a respective precept to the possessor of the assets, by showing the reason for introducing a restriction on the disposal of the assets. If the actual owner of assets is determined before one year goes by or new circumstances occur, the procedure provided in the law and present regulation shall be followed.
- (11) If within a year from the introduction of the restriction provided in subsection 10 the actual owner of assets has not become apparent, the head of the FIU, an official substituting for him or her or an official appointed by him or her shall notify the Prosecutor's Office of the restrictions imposed on assets by the FIU and the related circumstances and the Prosecutor's Office shall make a decision as regards the future transactions with the assets.
- (12) If restrictions have been imposed on assets and it occurs during analysis that the origin of assets is legal and the suspicion of terrorist financing has not been confirmed, the assets shall immediately be cleared of restrictions and the possessor shall immediately be notified of the decision.
- (13) The FIU shall maintain records concerning the restrictions imposed on assets, the terms thereof and the list and value of assets. The data shall be retained with

the folder of the RABIS database and as a separate consolidated table. The data shall be entered into the table by the assistant based on the data submitted by the head of the FIU or responsible processing official.

**§ 12. The imposition of restrictions electronically and the technical requirements thereof**

- (1) When a restriction is imposed the head of the FIU or an official substituting for him or her shall forward a respective digitally signed and encrypted precept to the obligated person.
- (2) The representative of the obligated person shall by means of a digitally signed and encrypted e-mail send a confirmation of the receipt of the precept and the application of respective restrictions.
- (3) If it is not possible for technical or other reasons to submit the document digitally, the precept is submitted on paper. The representative of the obligated person shall give a confirmation as regards the receipt of the precept.

**Chapter 5**

**ASSURANCE OF THE ORGANISATIONAL AND TECHNICAL PROTECTION OF DATA**

**§ 13. Assurance of data protection**

- (1) Data protection is ensured in accordance with the requirements provided for the processing of personal data in the Public Information Act and the Personal Data Protection Act and the requirements provided for the protection of information subject to banking secrecy in the Credit Institutions Act.
- (2) The head of the FIU or an official substituting for him or her shall be directly subject to the head of the Central Criminal Police in matters of data protection management. The head of the FIU shall be responsible for the fulfilment of data protection requirements in the FIU.
- (3) The person organising data protection is obliged in the FIU to:
  - 1) to organise data protection and apply measures for ensuring data protection in every way;
  - 2) exercise supervision over the compliance with the requirements arising from the Money Laundering and Terrorist Financing Prevention Act and the legal instruments issued based on it;
  - 3) organise training for its employees in the issues related to data protection;
  - 4) maintain records on data and the persons who have access to it.
- (4) The possessor of data is obliged to notify the head of the FIU immediately if there is reason to believe that data has become known to a person who does not have the access right to it or if the present procedure has in some other way been violated. The possessor of data is in such case obligated to apply measures in order to decrease or prevent the damage which could arise from the disclosure of data.
- (5) The data stored at the FIU may be processed and released only by an official of the FIU who has previously had the guidelines governing the work of the FIU, the present regulation, Money Laundering and Terrorist Financing Prevention Act, Personal Data Protection Act, Public Information Act, Credit Institutions Act and the

provisions of other acts which determine responsibility for violating the abovementioned acts introduced to him or her and who has given a signature confirming that he or she commits to maintain in secrecy the data that has become known to him or her in connection with his or her tasks.

- (6) Professional access to other databases or to the database of the FIU may only be used only for professional purposes. The violation of access rights is considered a disciplinary offence.
- (7) The facilities of the FIU which are used to store and process the collected data must be located in a building with a guarded entry, the entry to the rooms must be guarded with video cameras and be equipped with a signalisation system and a code lock. The rooms may only be equipped with those alarm systems which are not easily neutralised and which are inescapable. The system must operate in such a manner that reacting to an alarm would be as effective as possible.
- (8) The facilities of the FIU have to be inspected immediately after the official working hours. Each employee of the FIU makes sure when leaving the office after working hours that unauthorised person are not in the office, computers are turned off and data media locked in cupboards. When leaving, the employee locks the door. The employee who leaves last shall make sure that the doors of all offices are closed and puts them under surveillance.
- (9) The persons not employed by the FIU may be in the premises of the FIU only with the permission of the head of the FIU and accompanied by an official of the FIU.
- (10) The information technology devices used at the FIU must be equipped with suitable protection means. For the storage of data media used in FIU, the FIU must have locked cupboards.
- (11) The procedure for the use of the RABIS database of FIU is provided in a separate legal instrument.

## **Chapter 6 IMPLEMENTING PROVISIONS**

### **§ 14. Inspection of the compliance with the present regulation**

- (1) Supervisory control over the registration and processing of data is performed by the Central Criminal Police.
- (2) Inspection over the compliance with data protection requirements is performed by the Data Protection Inspectorate.

### **§ 15. Entry into force of the regulation**

**The Regulation shall enter into force on 28 January 2008.**

Jüri Pihl  
Minister

Märt Kraft  
Secretary-General