Issuer:	Minister of the Interior
Type:	regulation
In force from:	12.04.2013
In force until:	26.11.2017
Translation published:	24.09.2014

Procedure for Registration and Processing of Data Collected by Financial Intelligence Unit

Passed 23.01.2008 No. 13
RTL 2008, 8, 96
Entry into force 28.01.2008

Amended by the following acts

Passed	Published	Entry into force
18.12.2009	RTL 2009, 99, 1476	01.01.2010
31.01.2013	RT I, 07.02.2013, 1	10.02.2013, implemented as of1.01.2013
02.04.2013	RT I, 09.04.2013, 1	12.04.2013, implemented as of1.04.2013

The Regulation is established on the basis of subsection 43(6) of the Money Laundering and Terrorist Financing Prevention Act.

Chapter 1
General provisions

§ 1. General provisions

(1) This Regulation regulates the procedure for the registration and processing of data collected by the Financial Intelligence Unit.

(2) The supervisory activities of the Financial Intelligence Unit are regulated by the Code of Supervisory Practice of the Financial Intelligence Unit approved by the head of the Unit.

(3) A notice in the meaning of this Regulation is a written or written reproducible notice concerning a transaction with a suspicion of money laundering or terrorist financing or a transaction set forth in subsection 32(3) of the Money Laundering and Terrorist Financing Prevention Act sent to the Financial Intelligence Unit by the obligated persons specified in section 3 of the Money Laundering and Terrorist Financing Prevention Act (hereinafter *obligated person*) in accordance with the format approved by a regulation of the Minister of the Interior.

(4) RABIS is the electronic database of the Financial Intelligence Unit, in which the notices and other information received from obligated persons are collected, stored and processed.

§ 2. Information of Financial Intelligence Unit

(1) The information of the Financial Intelligence Unit shall be made up of:
1) notices received from the obligated persons of the Money Laundering and Terrorist Financing Prevention Act concerning transactions in regards to which a suspicion of money laundering or terrorist financing has arisen;
2) notices of the application of financial sanctions established in the International Sanctions Act;
3) information obtained as a result of an analysis performed by the Financial Intelligence Unit and additional information concerning the transactions, participants in the transactions and other circumstances related to the transactions, which the Financial Intelligence Unit collects in the cases stipulated by law;
4) any suspicious and unusual transactions, which have otherwise become known to the Financial Intelligence Unit.

(2) The information of the Financial Intelligence Unit also includes the data collected in the performance of supervision stipulated in paragraphs 37(1)4) and 9) and Chapter 5 of the Money Laundering and Terrorist Financing Prevention Act concerning the activities of obligated persons that contain information subject to banking secrecy or proprietary information.

§ 3. Records management of Financial Intelligence Unit

(1) The correspondence of the Financial Intelligence Unit shall generally take place via digitally signed electronic letters. Documents are digitally signed by the head of the Unit or a substituting officer or an officer appointed by the head of the Unit.

(2) Letters and other postal consignments addressed directly to the Financial Intelligence Unit shall be opened only at the Financial Intelligence Unit.

(3) Notices shall be registered in the RABIS database.

(4) The Financial Intelligence Unit has its own stand-alone document register which is located in a local computer connected to the internal network of the Financial Intelligence Unit. Only the officers of the Financial Intelligence Unit shall have access to the said document register. All the letters and postal consignments sent and received by the Financial Intelligence Unit in connection with money laundering and terrorist financing prevention shall be registered in the document register. The outgoing letters shall be sealed in envelopes marked with the address and the sealed envelopes shall be forwarded to the Document Management Unit of the Police and Border Guard Board for dispatch.
[RT I, 09.04.2013, 1 – entry into force 12.04.2013, implemented as of 1.04.2013]

(5) Precepts shall be registered in the stand-alone document register of the Financial Intelligence Unit. Electronic copies of precepts shall be stored in the RABIS database in the file under which the precept was prepared.

(6) Internal police orders, directives and other correspondence related to the position of the Financial Intelligence Unit in the structure of the Police and Border Guard Board and the administrative management of the Unit shall be registered in accordance with the internal records management procedure of the Police and Border Guard Board.
[RTL 2009, 99, 1476 – entry into force 01.01.2010]

Chapter 2
Registration and processing of data

§ 4. Collection of information

(1) Notices shall be sent to the Financial Intelligence Unit using the web-based notice form on the public web page of the Financial Intelligence Unit, electronic mail, fax or ordinary mail.

(2) Enquiries and information received from investigative bodies or foreign institutions fulfilling the tasks of a financial intelligence unit shall be treated as notices.

(3) Notices about suspicious transactions identified in the course of supervisory activities shall be made by the Supervisory Service.

§ 5. Registration of information

(1) A notice received by the Financial Intelligence Unit shall be registered in the stand-alone RABIS database located at the Financial Intelligence Unit, where it is assigned a registration number and the sender of the notice is recorded as well as the number assigned to the notice by the sender, the date of the notice, the details of the customer or the participants in the transaction and other information concerning the transaction. Other materials attached to the notice shall be stored in the RABIS database together with the notice.

(2) Notices sent via the web-based notification environment accessible on the public web page of the Financial Intelligence Unit are located on the web server in encrypted format. Encrypted notices shall be transferred by a data processor of the Financial Intelligence Unit to the RABIS database, where the notices are decrypted.

(3) Notices received by electronic mail shall be opened by the head of the Financial Intelligence Unit or a substituting officer or an officer appointed by the head of the Unit.

(4) A notice received by fax or mail shall be scanned or otherwise digitised by a data processor prior to registration. The original copies shall either be added to a verification file or archived.

(5) Data independently collected by the Financial Intelligence Unit shall be registered as notices in the RABIS database, stating the relevant officer of the Financial Intelligence Unit as the sender of the notice.
[RT I, 09.04.2013, 1 – entry into force 12.04.2013, implemented as of 1.04.2013]

(6) If it is determined upon verification that a submitted notice does not conform to the established requirements or contains deficiencies, the notice shall be registered in accordance with the general procedure and the submitter of the notice shall be informed in writing of the identified deficiencies which have to be eliminated by the indicated term.

§ 6. Analysis of information

(1) The head of the Financial Intelligence Unit or an officer appointed by him or her shall review all the notices specified in subsection 1(3) of this Regulation.

(2) Notices received from obligated persons and marked as 'Urgent' as well as foreign enquiries shall be immediately reviewed at the Financial Intelligence Unit and analysed on the basis of the available information, and the use of measures for the preservation of assets shall be decided. Other notices shall be reviewed within a reasonable period of time on the basis of the criteria for the distribution and determination of priority of notices separately established by the head of the Financial Intelligence Unit.

(3) Upon the receipt of a notice, the officer mentioned in subsection (1) of this section shall perform a primary analysis on the basis of the information contained in the database of the Financial Intelligence Unit. If necessary, additional information shall be collected from registers and databases accessible to the Financial Intelligence Unit. On the basis of the primary analysis, the officer shall decide whether there is a suspicion of money laundering, terrorist financing, related crimes or other crimes.

(4) If it is determined as a result of the primary analysis that the underlying suspicion is not confirmed, the notice shall be archived in the RABIS database.

(5) If it is determined in review of the notice that there is a need to collect additional information in order to determine whether the data described in the notice are relevant for uncovering cases of money laundering or terrorist financing or related crimes or in pre-trial proceedings, a verification file shall be opened on the basis thereof.

(6) Every verification file shall be assigned a separate number and a responsible officer.

(7) The head of the Financial Intelligence Unit or a substituting officer or an officer appointed by the head of the Unit shall assign a term of up to three months for solving the verification file, depending on the complexity of the case. The term may be extended due to the exceptional complexity or international nature of the case on the basis of a justified request of the responsible officer.

(8) A term of up to one month shall be assigned for responding to foreign enquiries, depending on the content of the enquiry. Urgent enquiries shall be responded to within two working days.

(9) Precepts, enquiries, correspondence and other documents shall be registered in the stand-alone database of the Financial Intelligence Unit and stored in the relevant verification file.

(10) The Financial Intelligence Unit shall store the verification files generally in electronic format in the RABIS database, taking all the security measures in order to ensure the preservation of the electronic files and the confidential information contained therein. Documents received in hard copy shall be stored in their original form and scanned into digital verification files.

(11) If transactions analysed under an opened verification file are related to notices received before or after the opening of the verification file, the inclusion of the notices from the RABIS database to the already opened verification file shall be decided.

(12) If it is determined as a result of an analysis that an opened verification file includes transactions related to a previously opened verification file, the files shall be merged and assigned a joint number. If it is determined that in addition to the currently analysed suspicion of crime the file materials also include the attributes of another independent crime, the materials may be assigned to a separate file, if necessary.

(13) The opening, merging and separation of files and the appointment of responsible officers shall be within the competence of the head of the Financial Intelligence Unit, the heads of the services of the Unit or another officer appointed by the head of the Unit.

(14) Upon analysing a notice specified in subsection 1(3) of this Regulation, the Financial Intelligence Unit shall use all the possibilities of obtaining additional information set forth in the Money Laundering and Terrorist Financing Prevention Act.

(15) Enquiries submitted to the competent bodies of a foreign country and the administrative acts of the Financial Intelligence Unit shall be signed by the head of the Financial Intelligence Unit or an officer substituting for him or her. The exchange of information with the competent bodies of a foreign country shall

be performed in accordance with the procedure set forth in this section. Information shall be exchanged with the competent bodies of a foreign country either by letter or fax on the letterhead of the Financial Intelligence Unit or via the international secure electronic information exchange system Egmont Secure Web.

(16) If the suspicion that formed the content of the notice has not been excluded in the course of processing and the available data are not yet sufficient for preparing a report of a criminal offence, the Financial Intelligence Unit may make a note on the existence of the information in the data on surveillance proceedings in the police database 'Polis Information System', assigning it the necessary access category.
[RT I, 07.02.2013, 1 – entry into force 10.02.2013, implemented as of 1.01.2013]

(17) The responsible officer shall submit the materials collected as a result of the analysis together with a summary to the head of the Financial Intelligence Unit, the head of a structural unit or a substituting officer for deciding whether it should be sent to an investigative body or a competent body of a foreign country or assigned for storage at the Financial Intelligence Unit.

(18) The Financial Intelligence Unit shall not release notices of suspicion of money laundering, copies or transcripts thereof and data concerning the person who submitted the notice.

(19) Upon forwarding information to a competent body of a foreign country, a note concerning the terms and conditions of use thereof shall be made.

Chapter 3
Forwarding and release of information

§ 7. Forwarding of materials

(1) Upon the identification of the attributes of money laundering, terrorist financing or related crimes or other crimes, the Financial Intelligence Unit shall immediately forward the material to the competent body. The forwarded materials shall be treated as a report of a criminal offence.

(2) If the collected materials indicate a crime in the competence of the jurisdiction of another country, the materials shall be sent as a notice to the institution fulfilling the functions of a financial intelligence unit in the foreign country.

(3) Upon forwarding materials, the responsible officer shall prepare a cover letter, ensure the preservation of the materials at the Financial Intelligence Unit and forward the materials together with the cover letter to the head of the Financial Intelligence Unit or an officer of the Unit substituting for him or her for signing.

(4) If the Financial Intelligence Unit has imposed restrictions in order to ensure the preservation of assets, it shall submit the materials to the investigative body as soon as possible, but not later than ten working days before the expiry of the restriction term. In such case the investigative body shall decide the seizure of the assets in accordance with the procedure stipulated in the Code of Criminal Procedure before the expiry of the restriction imposed by an administrative act of the Financial Intelligence Unit.

§ 8. Release of data

(1) The Financial Intelligence Unit shall not release data, unless it derives otherwise from the law, international agreements or this Regulation.

(2) The Financial Intelligence Unit shall forward material data, including data containing information subject to taxation and banking secrecy, to the prosecutor, investigative body or court, if the data are necessary for the prevention, identification or pre-trial proceeding of money laundering, terrorist financing, related crimes or other crimes.

(3) The Financial Intelligence Unit shall release the data specified in subsection (2) of this section upon its own initiative or on the basis of the justified requests of the institutions specified in subsection 43(3) of the Money Laundering and Terrorist Financing Prevention Act.

(4) The Financial Intelligence Unit may disclose the data collected in the course of administrative proceedings to an investigative body for the prevention, identification or pre-trial proceeding of crimes.

(5) The decision to release data shall be passed and the documents related to the release of data shall be signed by the head of the Financial Intelligence Unit, a substituting officer or an officer appointed by the head of the Unit.

(6) Upon releasing data from the Financial Intelligence Unit, restrictions on the use of the data may be established.

(7) Other data communication shall take place in accordance with the law and the cooperation agreements between authorities.

§ 9. Cooperation with Estonian Internal Security Service in prevention of terrorist financing

(1) In the prevention of terrorist financing, the Financial Intelligence Unit shall cooperate with the Estonian Internal Security Service in accordance with the provisions of section 45 of the Money Laundering and Terrorist Financing Prevention Act.

(2) The head of the Financial Intelligence Unit, a substituting officer or an officer appointed by the head of the Unit shall forward notices of suspected money laundering to the contact person appointed by the Director General of the Estonian Internal Security Service digitally signed and encrypted by electronic mail, making a relevant note in the RABIS database.

(3) The contact person for the Financial Intelligence Unit appointed by the Director General of the Estonian Internal Security Service shall:
1) receive the material data specified in subsection 45(2) of the Money Laundering and Terrorist Financing Prevention Act from the Financial Intelligence Unit;
2) analyse notices of suspected terrorist financing independently or in cooperation with the Financial Intelligence Unit;
3) if necessary, review the verification files opened for the identification of cases of terrorist financing;
4) if necessary, submit the notice of suspected terrorist financing of the Estonian Internal Security Service to the Financial Intelligence Unit for verification;
5) provide quarterly feedback to the Financial Intelligence Unit on the results of the analyses of the notices of suspected terrorist financing checked by the Internal Security Service, and upon the identification of attributes of a crime and the initiation of criminal proceedings, immediately inform the Financial Intelligence Unit thereof;
6) comply with the data protection requirements stipulated by the law and this Regulation.

§ 10. Feedback

(1) In the case the requirements of paragraph 37(1)2) of the Money Laundering and Terrorist Financing Prevention Act are met, the Financial Intelligence Unit shall inform the person who has submitted data to the Unit once a year of the use of the data, if criminal proceedings have been initiated on the basis of the data or the data were added to already initiated criminal proceedings.

(2) The administrator of the Financial Intelligence Unit shall register notices in the document register of the Unit and make a relevant note in the RABIS database.

Chapter 4
Imposition of restrictions

§ 11. Imposition of restrictions stipulated in section 40 of Money Laundering and Terrorist Financing Prevention Act

(1) If an obligated person has forwarded a notice marked as ‘Urgent’ to the Financial Intelligence Unit and has suspended transactions with the assets, the Financial Intelligence Unit shall immediately review the notice and pass a decision on the imposition of restrictions on the disposal of an account or the assets that form the object of the transaction.

(2) The suspension of a transaction or the imposition of a restriction on the disposal of an account or the assets that form the object of the transaction shall be decided by the head of the Financial Intelligence Unit on the basis of the proposal of the responsible officer or the head of a service of the Financial Intelligence Unit.

(3) If the Financial Intelligence Unit receives an enquiry and a justified request for the imposition of a restriction on assets from a competent body of the foreign country, the restriction shall be applied in accordance with general procedure and the competent body of the foreign country shall be immediately informed thereof.

(4) After deciding on the need to suspend a transaction or impose a restriction on the disposal of an account or the assets that form the object of the transaction, the responsible officer shall prepare a relevant precept which shall be signed by the head of the Financial Intelligence Unit, a substituting officer or an officer appointed by the head of the Unit.

(5) The precept shall be registered in accordance with the applicable procedure and forwarded to the possessor or owner of the assets by registered mail or delivered against signature.

(6) If the possessor or owner of the assets does not submit proof of the lawful origin of the assets to the Financial Intelligence Unit within thirty days from the suspension of the transaction or the imposition of a restriction on the disposal of the account, the head of the Financial Intelligence Unit, a substituting officer or an

officer appointed by the head of the Unit shall decide the need to impose and determine the term of an extended restriction on the basis of the file materials. A relevant note shall be made in the RABIS database.

(7) If the possessor or owner of the assets submits proof of the origin of the assets in a timely manner, the responsible officer shall immediately check the data using all the options provided for that by law, and shall thereafter present his or her opinion on the cancellation or extension of the restrictions to the head of the Financial Intelligence Unit or an officer substituting for the head of the Unit.

(8) If in the course of an analysis a need arises to restrict the disposal of assets or seize assets in another country, a relevant enquiry and/or justified request shall be prepared and sent to a competent body of that country.

(9) If the Financial Intelligence Unit decides to extend the imposition of restrictions, it shall give immediate notice thereof to the possessor or owner of the account or the assets. The relevant precept shall be registered in accordance with the applicable procedure and forwarded to the possessor or owner by registered mail or delivered against signature.

(10) In order to apply subsection 40(6) of the Money Laundering and Terrorist Financing Prevention Act, the Financial Intelligence Unit shall issue a relevant precept to the possessor of the assets, stating the reason for the imposition of the restriction on the disposal of the assets. If the actual owner of the assets is identified within one year or new circumstances are determined, the procedure stipulated in the law and this Regulation shall be complied with.

(11) If the actual owner of the assets is not identified within one year after the imposition of the restriction specified in subsection (10), the head of the Financial Intelligence Unit, a substituting officer or an officer appointed by the head of the Unit shall give notice of the restrictions imposed on the assets by the Financial Intelligence Unit and of the related circumstances to the Prosecutor’s Office who shall decide further procedures with the assets.

(12) If restrictions have been imposed on assets and it is determined in the course of an analysis that the assets are of lawful origin or the suspicion of terrorist financing has not been confirmed, the restrictions on the assets shall be immediately lifted and the possessor of the assets shall be given immediate notice thereof.

(13) The Financial Intelligence Unit shall keep records of the restrictions imposed on assets, the terms thereof and the list and value of the assets. The data shall be stored in the relevant file in the RABIS database and as a separate master table. Data shall be entered in the master table by the administrator on the basis of the data submitted by the head of a service or the responsible person.

§ 12. Procedure and technical restrictions for imposition of restrictions by electronic means

(1) Upon imposing a restriction, the head of the Financial Intelligence Unit or an officer substituting for him or her shall forward a relevant digitally signed and encrypted precept to the obligated person.

(2) The representative of the obligated person shall send a digitally signed and encrypted confirmation by electronic mail concerning the receipt of the precept and the application of the relevant restrictions.

(3) If the document cannot be forwarded digitally due to technical or other reasons, the precept shall be submitted in hard copy. The representative of the obligated person shall provide a confirmation of the receipt of the precept.

Chapter 5
Ensuring organisational and technical protection of data

§ 13. Ensuring data protection

(1) The protection of data shall be ensured in accordance with the personal data processing requirements stipulated in the Public Information Act and the Personal Data Protection Act and the requirements for the protection of information subject to banking secrecy stipulated in the Credit Institutions Act.

(2) In the issues of the organisation of data protection, the head of the Financial Intelligence Unit or an officer substituting for him or her shall be immediately subordinated to the head of the Central Criminal Police of the Police and Border Guard Board. The head of the Financial Intelligence Unit shall be responsible for the fulfilment of data protection requirements in the Financial Intelligence Unit.
[RT I, 07.02.2013, 1 – entry into force 10.02.2013, implemented as of 1.01.2013]

(3) The person organising data protection shall be obligated in the Financial Intelligence Unit:
1) to organise the protection of data and take measures for ensuring the comprehensive protection of data;
2) to perform supervision over compliance with the requirements arising from the Money Laundering and Terrorist Financing Prevention Act and the legal acts issued on the basis thereof;
3) to organise training in the issues of data protection;

[RT I, 09.04.2013, 1 – entry into force. 12.04.2013, implemented as of 1.04.2013]
4) to keep records of the data and the persons authorised to access the data.

(4) The possessor of the data shall be obligated to give immediate notice to the head of the Financial Intelligence Unit, if the there is reason to believe that the data have become known to unauthorised persons or this procedure has been otherwise violated. In such case, the possessor of the data shall be obligated to take measures to limit or prevent the damages that may arise from the disclosure of the data.

(5) The data stored at the Financial Intelligence Unit may be processed and released only by an officer of the Financial Intelligence Unit who has been previously familiarised with the guidelines regulating the work of the Financial Intelligence Unit, this Regulation, the Money Laundering and Terrorist Financing Prevention Act, the Personal Data Protection Act, the Public Information Act, the Credit Institutions Act and the provisions of other legal acts which determine the liability for the violation of the said legal acts, and who have confirmed with their signature that they shall keep confidential the data that become known to them in connection with their work duties.

(6) Official access to other databases or the database of the Financial Intelligence Unit may only be used for work-related purposes. Abuse of access shall be considered as a disciplinary offence.

(7) The premises of the Financial Intelligence Unit, where the collected data are stored and processed, shall be located in a building with a guarded entrance, the entry to the premises shall be under video surveillance and equipped with an alarm system and a code lock. Only such alarm systems which cannot be easily neutralised or bypassed shall be used in the premises. The system shall operate in such a way that it is possible to react to an alarm immediately.

(8) The premises of the Financial Intelligence Unit shall be inspected after the end of official working hours. Upon leaving his or her office after working hours, every officer of the Financial Intelligence Unit shall ascertain that there are no unauthorised persons in the office, the computers are switched off and the information media has been placed in locked cabinets. Officers shall lock the door of the office upon leaving. The officer of the Unit who is the last to leave shall ascertain that the doors of all the offices have been locked and activates the alarm system.
[RT I, 09.04.2013, 1 – entry into force 12.04.2013, implemented as of 1.04.2013]

(9) Persons not employed by the Financial Intelligence Unit may stay in the premises only with the permission of the head of the Financial Intelligence Unit and accompanied by an officer of the Financial Intelligence Unit.

(10) The information technological tools used at the Financial Intelligence Unit shall be equipped with protective devices in accordance with requirements. The Financial Intelligence Unit shall have lockable cabinets for storing the information media used at the Financial Intelligence Unit.

(11) The procedure for the use of the RABIS database of the Financial Intelligence Unit shall be established by a separate legal act.

Chapter 6
IMPLEMENTING PROVISIONS

§ 14. Supervision over compliance with this Regulation

(1) Supervisory control over the registration and processing of the data shall be performed by the Police and Border Guard Board.
[RTL 2009, 99, 1476 – entry into force 01.01.2010]

(2) Supervision over compliance with the data protection requirements shall be performed by the Data Protection Inspectorate.

§ 15. Entry into force of Regulation

The Regulation shall enter into force on 28 January 2008.