Methodological Guideline No 4/2013 of the Financial Market Supervision Unit of Národná banka Slovenska of 4 October 2013 regarding the prevention by insurance companies, branches of insurance companies from other Member States of the European Union and branches of insurance companies from non-Member States of the European Union of money laundering and terrorist financing

The Financial Market Supervision Unit of Národná banka Slovenska (hereinafter the "NBS"), on the basis of Article 1(3)(a) point 3 of Act No 747/2004 Coll. on financial market supervision, as amended, in collaboration with the Financial Intelligence Unit (hereinafter the "FIU"), in order to ensure the uniform procedure for the performance of duties arising from the prevention of money laundering and terrorist financing, has issued this methodological guideline:

Article 1
Purpose

(1) The purpose of this methodological guideline is to provide insurance companies, branches of insurance companies from other Member States of the European Union (hereinafter the "EU") and branches of insurance companies from other than EU Member States that undertake insurance activities in the territory of the Slovak Republic (hereinafter the "insurance company" or the "branch" or the "financial institution") with a more detailed explanation for fulfilling their duties arising from Act No 297/2008 Coll. on the prevention of money laundering and terrorist financing and on the amendment of certain laws, as amended (hereinafter the "Act"), and Act No 8/2008 Coll. on insurance and on amendments to certain laws, as amended (hereinafter the "Insurance Act").

(2) The provisions of this methodological guideline shall apply mutatis mutandis to a financial agent, financial adviser, branch of a financial intermediary from another EU Member State in the insurance or reinsurance sector, or financial adviser from other than EU Member State in the insurance or reinsurance sector.

Article 2
Policy for protecting a financial institution against money laundering and terrorist financing

(1) A financial institution must have its own policy in the field of the prevention and detection of money laundering and terrorist financing (hereinafter the "AML/CFT policy"). The AML/CFT policy must be set so as to ensure effective performance of activities aimed at preventing and detecting money laundering and terrorist financing at the financial institution.

(2) The AML/CFT policy forms a part of risk management, with particular relevance to operational risk management, at the financial institution.

(3) Components of the financial institution's AML/CFT policy are:
(a) an organisational structure ensuring effective and independent performance of activities in the field of the prevention of money laundering and terrorist financing (hereinafter the "AML/CFT"),
(b) a programme of activities pursuant to Article 20 of the Act (hereinafter the "Programme");

(4) In accordance with Article 36(1) of the Insurance Act, the insurance company's Articles of Association shall define in particular the insurance company's organisational structure, powers and responsibilities division, including the field of AML/CFT. The AML/CFT policy in written form shall be adopted by the statutory body which is also responsible for its implementation.

(5) A branch shall, in the framework of the organisational structure, designate a managerial employee as responsible for the AML/CFT area, or shall designate that the head of the branch is responsible for the AML/CFT area (hereinafter the "branch's Responsible Person"). The AML/CFT policy, in written form, shall be adopted by the branch's Responsible Person, who is also responsible for its implementation.

Article 3
Organisational structure of a financial institution ensuring effective and independent performance of activities in the field of the prevention of money laundering and terrorist financing

(1) The statutory body of the insurance company shall be responsible for the insurance company's overall prevention of money laundering and terrorist financing.

(2) A branch's Responsible Person shall be responsible for the overall prevention of money laundering and terrorist financing at the branch.

(3) Responsibility for the practical implementation of activities in the field of AML/CFT, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT policy, the reporting of unusual transactions and for ongoing contact of the financial institution with the FIU lies with the Nominated Officer (hereinafter the "Nominated Officer").

(4) It is not appropriate to outsource the activities of the Nominated Officer.

(5) A financial institution shall ensure full substitutability for the post of the Nominated Officer, by means of a deputy Nominated Officer.

(6) In filling the post of the Nominated Officer and deputy Nominated Officer, the financial institution shall require candidates to demonstrate civic integrity, appropriate education and corresponding professional experience.

(7) The Nominated Officer and deputy Nominated Officer of an insurance company shall be appointed and dismissed by the statutory body. The insurance company's Nominated Officer shall report directly to the insurance company's statutory body.

(8) The Nominated Officer of a branch shall be appointed and dismissed by the branch's Responsible Person or head of the branch. The Nominated Officer of a branch shall report to the branch's Responsible Person or head of the branch.

Where a financial institution has several places of work in the Slovak Republic at which it performs its activities, it may nominate an employee at these places, who need not be a member of the unit responsible for performing activities necessary for ensuring tasks of the prevention system (hereinafter the "Prevention Unit"), and entrust that employee with the performance of selected activities pertaining to the Nominated Officer or Prevention Unit (hereinafter the "Authorised Employee"). The Authorised Employee is in continuous working contact with the Nominated Officer. If a financial institution also establishes a Prevention Unit, the Nominated Officer shall be the manager of that unit.

(9) The job description of the Nominated Officer shall include in particular:

(a) ongoing preparation and updating of the Programme and any other necessary regulations and procedures for the AML/CFT field;
(b) the performance of management and control tasks in the field that he performs and for which he is responsible in the Prevention Unit, if established;
(c) communication, cooperation and maintaining ongoing contacts with the FIU, including the timely reporting of unusual transactions;
(d) organisation and setting of rules for the training of the financial institution's relevant staff, including new staff;
(e) analytical and advisory activity in relation to the assessment and reporting of unusual transactions by the respective staff in connection with the execution of customers' transactions and operations.

(10) The Nominated Officer and his deputy are required to perform their duties with due professional diligence. The Nominated Officer of an insurance company shall submit a report on his activity or on the activity of the Prevention Unit, if established, to the statutory body at least once a year. The Nominated Officer of a branch shall submit a report on his activity, or on the activity of the Prevention Unit, if established, to the branch's Responsible Person and to the head of the branch at least once a year.

The activity report shall contain in particular the following information:
(a) statistics and a brief description of unusual transactions reported by staff;
(b) statistics and a brief description of unusual transactions that were not reported to the FIU, with the reasoning of non-reporting;
(c) statistics and a brief description of unusual transactions reported to the FIU;
(d) overview of identified deficiencies and draft measures and deadlines for their rectification,
(e) information from inspections carried out;
(f) information or overview of staff training conducted.

(11) An important element of AML/CFT policy of a financial institution is to ensure that the Nominated Officer, his deputy and the Prevention Unit have a sufficiently independent status within the structure of managerial staff and organisational units. A Nominated Officer's classification in a financial institution's organisational structure shall contain the following elements guaranteeing an appropriately defined standing of the Nominated Officer, his deputy and, as relevant, the Prevention Unit:
(a) arrangement of powers and duties of the Nominated Officer and his deputy in their job descriptions, with emphasis on the primary area of their operation, which is to ensure the prevention and detection of money laundering and terrorist financing (other activities may not impede them in promoting effective measures in this primary area);
(b) separation from units responsible for executing customers' transactions or trading;
(c) unrestricted access of the Nominated Officer and his deputy to all documents, databases and information at the financial institution;
(d) autonomous and independent decision-making of the Nominated Officer and his deputy in assessing the unusualness of customers' transactions reported by the respective staff in the framework of the internal reporting system;
(e) autonomous and independent decision-making on the sending of unusual transaction reports to the FIU;
(f) control function of the Nominated Officer, his deputy, and the Prevention Unit in relation to units and staff responsible for executing customers' transactions or trading;
(g) separation of the Nominated Officer, his deputy, and the Prevention Unit from the internal audit unit in the organisational structure, whilst preserving follow-up inspection of their activity conducted by the internal audit unit;

(h) in the case of extraordinarily serious circumstances or situations, immediate information to the statutory body or the branch's Responsible Person.

Article 4
Financial institution's Programme of internal activities

(1) A financial institution shall draw up the Programme as an internal regulation, approved by the statutory body of the insurance company or head of the branch. The Programme shall be based on generally binding legal regulations and it shall also take into account the Articles of Association of the insurance company and its AML/CFT policy.

The Programme shall represent a transposition of the AML/CFT policy into practical principles, tasks, procedures, duties and responsibilities in the field of AML/CFT. It shall also contain specific authorisations, duties, responsibilities and tasks of the Nominated Officer, Prevention Unit and relevant staff of the financial institution in the performance of insurance activities (mainly Article 20(2) of the Act), required by the prevention of money laundering and terrorist financing, as well as the control powers of these entities and control powers of the internal audit unit (see Article 11). The Programme shall also define information flows, information systems, control processes and mechanisms in this field.

(2) In creating the Programme, the financial institution shall take into account its own specific characteristics, in particular its size and market share, organisational arrangement and the range of insurance activities. The Programme shall contain not only information on statutory provisions, staff responsibilities, but also all operational procedures and duties of staff at the financial institution in the performance of the relevant type of customers' transactions and trading operations, as well as the most common types of unusual transactions at the given financial institution.

(3) The Programme shall set out in particular**:**
(a) the specification of tasks, duties and responsibilities for the financial institution's comprehensive prevention of money laundering and terrorist financing, at the individual levels of management from the managing board of the financial institution, or from the branch's Responsible Person down to the units of first contact with the customer, including the Prevention Unit;
(b) the designation of the Nominated Officer under Article 20(2)(h) as the holder of a specified office or position;
(c) the nomination of persons at the financial institution who assess whether an intended or ongoing transaction is unusual;
(d) the specification of the time when the assessment is to be performed (where possible, always before execution of a transaction or in the process of its preparation);
(e) the specification of the method of performing assessment pursuant to points (c) and (d), i.e. to state what needs to be performed in an assessment, what aids are to be used (e.g. an overview of the types of unusual transactions, etc.), how and where to record the assessment result;
(f) arrangements for the prevention of money laundering and terrorist financing, the receipt of notifications on identified unusual transactions from organisational units, the evaluation of these notifications and the reporting of unusual transactions to the FIU and arrangements ensuring ongoing working contact with the FIU, or law-enforcement bodies;
(g) the specification of basic tasks of the respective staff at all levels of management, the detection of unusual transactions and the reporting of internal notifications of unusual transactions to the Nominated Officer (possibly also a specimen form for internal notifications of an unusual transaction) and the manner of ensuring the protection of the respective staff in connection with the unusual transactions they identified and reported to the Nominated Officer;
(h) the duty to identify customers and the duty to verify this identification;

(i) the duty to record the identification made and the verification of customer's identification, as well as all trading operations executed for customers;
(j) the duty to retain records on customer identification and on the verification of their identification and on the trading operations conducted by customers, and this for the period set by the Insurance Act;
(k) an overview of known types of unusual transactions, broken down by activity and type of transaction executed;
(l) the evaluation and management of risks associated with money laundering and terrorist financing;
(m) the specification of the nature and extent of the implementation of customer due diligence on the basis of risk evaluation results pursuant to Article 10(4) of the Act;
(n) detailed signs of unusualness by which a customer's unusual transactions can be recognised;
(o) the method and scope of feedback at the financial institution on internal notifications of unusual transactions;
(p) the procedure of the respective staff and Nominated Officer in postponing an unusual transaction under Article 16 of the Act;
(q) the content and timetable of staff training, training staff for ensuring tasks in the field of AML/CFT at the financial institution;
(r) the duty to maintain confidentiality regarding an internal notification of an unusual transaction and its reporting to the FIU and regarding measures performed by the FIU (Article 18 of the Act), primarily in relation to the customer concerned, as well as toward persons having a certain relationship to the customer (e.g. beneficiaries) and toward third parties, other than exceptions stipulated by the Act;
(s) measures and control mechanisms preventing the abuse of position or function by staff to knowingly engage in money laundering or terrorist financing in the exercise of their function;
(t) the method and periods for retaining information and documentation;
(u) an internal control system focused on AML/CFT, consisting of control mechanisms, process controls of managerial staff, including controls by the Nominated Officer and internal audits;
(v) definition of information flows and description of information systems focused on the collection, processing and reporting of information for AML/CFT, including regular reports submitted to the managing board and supervisory board of the financial institution and to the branch's Responsible Person, or head of the branch.

(4) The financial institution shall ensure that the Programme is accessible to all the financial institution's staff, for example via an internal computer network.

(5) It is necessary to update the Programme not only in the case of a change in the relevant generally binding legal regulations, but also in the case of changes concerning the own performance of activities and types of transactions, as well as in the case of changes to the financial institution's organisational arrangement. An appropriate period for updating is once a year.

Article 5
Staff awareness and training

(1) The statutory body of an insurance company or the branch's Responsible Person, jointly with the Nominated Officer, must ensure that staff are aware of the financial institution's responsibility, as well as of the personal responsibility of staff and their protection in the case of identifying unusual transactions in this area.

(2) A financial institution shall publish in appropriate manner information for staff as regards who performs the function of the Nominated Officer and who is his deputy.

(3) A financial institution shall determine in the Programme the optimal regime and method for:
(a) informing its staff about the AML/CFT system, and related procedures, duties and powers;
(b) making the Programme and any other relevant regulations available to the respective staff;
(c) organising regular training and educational activities for staff; where regular training is performed via e-learning, it is recommended in the case of finding the need to raise staff awareness of the Programme, to appropriately supplement e-learning training by personal or other training so that the training system is effective.

(4) The financial institution, in informing and training staff, shall take account of its conditions, in particular its size, organisational arrangement, types of transactions, and trading operations performed for customers, so that all necessary information reaches all staff for whom it is intended.

It is important that the mechanism of providing information to staff from the side of the statutory body, the foreign branch's Responsible Person, the Nominated Officer, and respective managerial staff of the financial institution, as well as the model for performing staff training are effective, flexible and fulfil the expected objective; therefore it is essential that they be updated with regard to changing conditions.

(5) The effectiveness of a financial institution's prevention of money laundering and terrorist financing depends in large part on the level of knowledge on the side of managerial and other staff of the financial institution about the given problem, consisting in familiarisation with basic legal regulations, the Programme and other related internal regulations of the financial institution.

The diversity of trading operations, types of transactions and, in particular, the diversity in the structure of customers give rise to varying degrees of risk and different techniques of money laundering or terrorist financing.

The relevant staff (staff of first contact with the customer) must have all necessary information on the trading operations and types of transactions they will execute for customers and they must learn as soon as possible the criteria (signs of unusualness) for assessing or detecting unusual transactions. These staff must be able to assess the conduct of the financial institution's customers, as well as the content of trading operations performed by customers in terms of their degree of risk, unusualness or suspiciousness. Staff training should significantly contribute to staff acquiring the prerequisites for mastering procedures for applying the Know Your Customer principle (hereinafter referred to as the "KYC") and for recognising the degree of risk from the customer's actions, also with regard to the customer's categorisation into one of the three groups for mandatory customer due diligence:

- basic,
- simplified, and
- enhanced customer due diligence.

The relevant staff are an important element for preventing the misuse of the financial institution for money laundering or terrorist financing. Likewise, however, they can also be its weakest element, if they do not fulfil the set duties, or if they knowingly or unwittingly participate in the execution of a customer's unusual transactions.

(6) Before an employee enters employment at the financial institution in a post or function where they will, in direct contact with customers, ensure the execution of trading operations, the financial institution shall check a copy of the potential employee's excerpt from the Criminal Register to establish that they have not been convicted of any property, economic or other serious crime. The financial institution may require from the potential employee information also beyond the framework of an excerpt from the Criminal Register, in so doing though, it should take account of the fact that pursuant to Act No 300/2005 Coll., the Criminal Code, as amended, if the conviction of a person has been expunged, this person is to be viewed as having a clean criminal record. The

financial institution should require from a potential employee also a sufficiently satisfactory reference, or assessment of their prior work integrity, issued by their previous employer.

(7) In the framework of training, the financial institution shall ensure that staff are familiarised with the consequences of negligence or negligent fulfilment of their work duties and of any knowing or unwitting participation in money laundering or terrorist financing, as well as the consequences of a breach of the prohibition of providing a customer with information to which the duty of confidentiality applies (Article 18 of the Act); as well as with the manner of their protection in the case of detecting an unusual transaction.

(8) The financial institution must have a project or plan of staff training, taking into account the employee's work classification (own categorisation according to job positions, taking account of the employee's exposure to opportunities for and attempts at misuse for the purposes of money laundering and terrorist financing) and the resulting responsibilities, duties and the level and frequency of training pertaining thereto. In determining the appropriate frequency of training, the financial institution shall observe the provisions of Article 20(3) of the Act (once per calendar year and always before employees are assigned to work in which they perform tasks under the Act). The training plan, or its basic principles, should form a part of the Programme and should determine the basic outline, periodicity and content of staff training, in particular the provisions of the respective acts, internal regulations and rules of the financial institution or group to which the financial institution belongs, as well as an analysis of the content and circumstances of the most frequently occurring types of internal notifications of unusual transactions within the financial institution, or within the group.

(9) The financial institution is required under Article 20(3) of the Act to ensure staff training focused on familiarisation with the Programme at least once per calendar year and always before employees are assigned to work in which they will perform tasks set by the Act and by the Programme. Each employee concerned who performs tasks under the Act must be familiarised with the applicable Programme governing procedures in assessing customers and their financial operations, and concurrently the financial institution is required to ensure that each employee has permanent access to this Programme.

Staff training shall include in particular:

(a) familiarisation with the Programme;

(b) knowledge arising from the Nominated Officer's activity, from the activity of other financial institutions, as well as available knowledge arising from the activity of the FIU or supervisory authority.

A financial institution shall repeat and supplement training with new knowledge, where necessary, also more frequently than in a 12-month cycle (e.g. in the case of a change in the Programme), so as to ensure that the relevant staff are able to continuously perform their duties and exercise their powers. Forms of training (classic lecture, electronic, or other) should be regularly alternated. It is appropriate that the relevant staff be tested on the knowledge acquired.

(10) A financial institution shall ensure that records are drawn on staff training conducted, containing the date at which the respective staff participated in the training, the content and form of the training, and, where relevant, an evaluation of the test completed, as well as the employees' signatures or other electronic confirmation. In addition to this, it is necessary to obtain from the respective staff a written or electronic confirmation that they have been familiarised with the Programme and related regulations governing AML/CFT procedures.

Article 6
Information system at a financial institution

(1) A systematic approach to the financial institution's risk management and AML/CFT requires the creation of appropriate information flows for ensuring the smooth, timely and regular flow of information between individual levels of management at the financial institution, including its statutory body, the Nominated Officer, his deputy and the Prevention Unit, internal audit unit and the relevant staff. A systematic approach for ensuring information flows also requires support in the form of application software, i.e. a specialised information system, or systems. In broad terms this means a system of acquiring, processing, evaluating, transferring and also using information concerning this area. This shall include flows of AML/CFT information in the processes of the financial institution's individual activities and types of transactions performed. For effective prevention it is essential to ensure that it is regularly updated.

(2) The financial institution is required to ensure information flows for:
(a) the transmission of information to staff on AML/CFT principles, procedures, duties and powers and the related performance of day-to-day tasks;
(b) making the Programme and other relevant internal regulations available to employees;
(c) transmission of necessary information between the Responsible Person and Nominated Officer;
(d) transmission of information between staff and the Nominated Officer and vice versa, including the internal reporting of unusual transactions;
(e) record-keeping, i.e. the recording, processing and updating of information on customers and the recording and monitoring of customers' transactions;
(f) communicating to the statutory body or Responsible Person the results of control performed by the Nominated Officer and the internal audit unit, as well as informing staff of these results;
(g) transfer of information between the Nominated Officer and FIU, including the reporting of unusual transactions and provision of other necessary information and source documentation to the FIU, as well as the provision of feedback from the FIU to the financial institution;
(h) searching for unusual transactions in the financial institution's relevant information systems that contain information on customers and their operations.

(3) The form, content and rules of information flows should be set by the financial institution depending on its size, focus, scope and the complexity of its activities and on the types of transactions and services offered, as well as on the characteristics of its customers and their transactions.

The information system(s) shall conform to the specific conditions of the financial institution and, from the technical aspect, have parameters so that the financial institution is capable of fulfilling the duties arising to it under the Act (in particular Article 24(4) of the Act) as an obliged entity.

(4) An essential component of a financial institution's information system is an electronic information system (hereinafter referred to as an "EIS") that complies with statutory requirements, with the aim of ensuring sufficient quality in the prevention of money laundering and terrorist financing. An EIS, recording and processing information on customers and their transactions must take account of the requirements provided for in Article 9(e) of the Act:
(a) in the case of a natural-person customer, the EIS must contain records of the first name, last name, date of birth or birth registration number, and in the case of a sole proprietorship also the identification number, if assigned;
(b) in the case of a legal-person customer, the EIS must contain records containing the customer's name (business name) and identification number.

The EIS must also contain information or records on the nature of the customer's business relationship. The nature of a business relationship is given by the type of transaction pursuant to Article 9(i) of the Act or solely by a transaction pursuant to Article 9(h) of the Act, whilst the nature of the business relationship is primarily predetermined by the actual product or service that the customer uses. The EIS and the manner of using it should make it possible to identify unusual transactions performed by customers, and, as relevant, monitor also their course or development, as

well as the connections between the transactions of a certain customer and, where possible, also the unusual transactions of different customers.

A special part of information recorded and monitored by the EIS consists in information on politically exposed persons (Article 6 of the Act), which the respective staff received in performing their work tasks.

The EIS should enable the financial institution to immediately provide the FIU, upon its request, with information as to whether it has had a business relationship with a specified person in the past five years, as well as on the nature of that business relationship (Article 24(4) of the Act).

The EIS should also be capable of providing, in cases specified by law and in a timely manner and sufficient scope, information to the FIU, the NBS Financial Market Supervision Unit as the supervisory authority, and to law enforcement authorities.

The EIS shall also satisfy requirements of the financial institution and the FIU (Article 30 of the Act) for the purposes of control, and for statistical purposes.

Article 7
Customer identification and customer acceptance; customer risk profile; basic, simplified, and enhanced customer due diligence; performance by third parties

(1) The basic obligations of financial institutions in these areas are laid down in particular in the provisions of Articles 7, 8 and 10 to 13 of the Act and Article 47 of the Insurance Act.

(2) Pursuant to Article 47(1) and (2) of the Insurance Act, a financial institution is entitled, for the purposes of identifying customers and their representatives and enabling subsequent verification of this identification, for concluding insurance contracts and for insurance administration, as well as for other purposes referred to under (3) of this Act, to require from customers and their representatives the information defined in (1)(a) and to obtain it by the means defined in (1)(b); and the customer shall provide this information upon request.

Under Article 10(3), however, financial institutions are required to perform identification and verification when concluding a **non-life insurance** contract if the amount of the premium for a calendar year is equal to at least EUR 2,000 and if, based on information about the customer or transaction, it is not necessary to perform basic customer due diligence under Article 10(2); this obligation shall also apply where the amount of the premium is increased to EUR 2,000 or more. Financial institutions shall perform basic due diligence under Article 10(1) of the Act where the amount of the insurance premium for a calendar year is equal to at least EUR 15,000, or when performing a so-called occasional transaction worth at least EUR 15,000 outside a business relationship, i.e. an insurance contract, whether or not the transaction is executed at once or sequentially through transactions that are or can be interlinked.

Where a non-life insurance contract is concluded through a financial agent or financial adviser, identity may also be verified by the financial agent or financial adviser.

(3) Basic customer due diligence under Article 10(1) of the Act shall include the following acts:

(a) identification of the customer and verification of the customer's identification (including determining whether the customer is acting on their own behalf; where the customer is not acting on their own behalf, the customer shall provide a binding written declaration stating the first name, last name, birth registration number or date of birth of the natural person; or the business name, registered office and identification number of the legal person, on whose behalf of the customer is executing the transaction; the same shall apply to cases where doubts exists as to whether the customer is acting on their own behalf);

(b) depending on the risk of money laundering or terrorist financing, identification of the beneficiary and adoption of appropriate measures for verification of the identity of the beneficiary,

including measures to determine the ownership and management structure of the customer who is a legal person or an asset pool;
(c) acquiring information on the purpose and intended nature of the business relationship;
(d) continuous monitoring of the business relationship, including scrutiny of specific transactions executed during the business relationship in order to determine whether such transactions are consistent with what the obliged entity knows about the customer, including the customer's business profile and risk profile; and, depending on the risk of money laundering and terrorist financing, identification of the provenance of funds and action to ensure that the customer's documentation, data and other information available to the obliged entity are kept updated.

(4) When concluding a **life insurance** contract, financial institutions shall, pursuant to Article 47(6) of the Insurance Act, request the customer to prove their identity and the customer shall comply with such request. Where a life insurance contract is concluded through a financial agent or financial adviser, identity may also be verified by the financial agent or financial adviser. Financial institutions, financial agents and financial advisers shall refuse to conclude a life insurance contract in which customer anonymity would be maintained.
Under Article 11(2) of the Act, with regard to life insurance contracts, financial institutions shall perform basic customer due diligence if the premium for a calendar year exceeds EUR 1,000 or single premium exceeds the amount of EUR 2,500. Pursuant to Article 47(8) of the Insurance Act, for life insurance contracts in which the standard premium for a calendar year exceeds EUR 1,000 or a single premium exceeds EUR 2,500, financial institutions shall determine the ownership of funds used by the customer to conclude the insurance contract; this obligation shall also apply where the amount of the premium is increased to EUR 1,000 or more. For the purpose of this provision, the customer shall confirm the ownership of the funds by providing a binding written declaration stating whether the funds belong to the customer and whether the customer is concluding the insurance contract for their own account. If the funds belong to another person or if the insurance contract is concluded for the account of other person, the customer shall state in the declaration the first name, last name, birth registration number or date of birth, and address of permanent residence of the natural person, or the business name, registered office and identification number, if assigned, of the legal person, to whom the funds belong and for whose account the insurance contract is concluded; in this case the customer shall submit to the financial institution also the written consent of that natural or legal person to using that person's funds for concluding the insurance contract and to concluding this contract for the account of that person. In the case that the customer fails to meet these obligations, the financial institution shall refuse to conclude the insurance contract.
Verification of identification of the beneficiary of the life insurance contract,
(a) where the financial institution was obliged to perform basic due diligence when concluding the contract, or
(b) where the amount of insurance benefit is equal to at least EUR 2,000,
must be completed not later than when the beneficiary applies their rights arising from the life insurance or when the insurance benefit is paid.

(5) The process of determining and, to an appropriate extent, also verifying the beneficiary, shall be primarily governed by the provisions of Articles 9 and 10 of the Act. Verification of information acquired on the beneficiary in accordance with the Act shall be performed to an appropriate extent, e.g. by requesting a written declaration on the beneficiary and subsequent verification of this information from available sources. Where the customer's risk profile so allows, the financial institution, in applying basic customer due diligence, may determine the beneficiary on the basis of information from available sources, without the need to contact the customer or verify this information with the customer.

(6) The importance of the provisions of Article 10(1)(a) to (c) and Article 10(10) of the Act is highlighted in the provisions of Article 15 and Article 24(2) of the Act, which impose on the

financial institution the duty to refuse new customers, terminate an existing business relationship with customers, or refuse to perform a specific transaction in the case where it is not possible to perform basic customer due diligence or where the customers refuse to demonstrate on whose behalf they are acting.

The obligation of financial institutions, financial agents or financial advisers to refuse to conclude a life insurance contract in which customer anonymity would be maintained also follows from Article 47(6) of the Insurance Act. Pursuant to Article 17(1), financial institutions shall promptly report such cases to the FIU.

In this context, it is necessary to respect the guideline of the FIU published on the website (http://www.minv.sk/swift_data/source/policia/finpol/usmernenie_paragraf_15.pdf).

(7) In the case of new customers, the customer acceptance process should include basic customer due diligence, as well as the customer's categorisation into a certain risk group, accompanied by thorough application of the KYC principle, meaning the acquisition of sufficient information on the nature of the customer's expected transactions and any foreseeable scheme of operations to be performed by the customer. Based on this, it is possible to create the customer's risk profile.

In applying basic customer due diligence, a financial institution may not enter into a business relationship with a customer without reliably ascertaining all relevant circumstances concerning the customer.

The main criteria to be considered when composing a customer's risk profile shall be:

- the customer's aim in concluding the insurance contract,
- the type and origin of customer and beneficiary,
- the location of the residence/registered office of the customer and beneficiary,
- the location of the business activities of the customer and beneficiary,
- the main field of business,
- the provenance of the customer's funds,
- the provenance of the customer's wealth,
- the frequency and scope of activities,
- the type and complexity of the customer's business activities,
- whether the insurance benefit will be paid to a third party,
- whether the customer's business relationships are dormant,
- any suspicion or knowledge of money laundering, terrorist financing or other crimes.

The financial institution shall continuously update the customer's risk profile according to the risk group to which the customer is assigned; for this purpose it shall require from the customer the updating of information that the customer originally provided it, and this in appropriate time intervals and depending on changes concerning the customer's person, or their commercial or other activities with which the customer's transactions performed by the financial institution are connected. Updating may be performed also by way of requesting the customer to complete the relevant form, for example once a year, unless more frequent updating is necessary, or by agreeing a contractual condition with the customer on the duty to notify the financial institution of relevant changes.

(8) By means of categorising customers according to their risk profile the financial institution can then in practice apply Article 10(1)(d) of the Act, namely ongoing monitoring of the business relationship, which leads to recognition and also reporting of unusual transactions. In connection with the risk categorisation of customers, the financial institution should also consider Article 10(1)(d) and Article 10(8) of the Act, which establish the duty to continuously update the customer risk profile on the basis of a permanent monitoring of the business relationship. The

appropriate frequency for updating depends on the financial institution's assessment and decision; in each case this duty should be included in the internal regulation governing the Programme.

In connection with the consideration of risk in assessing a financial institution's customers, it is appropriate to use materials prepared by experts of the Financial Action Task Force (the intergovernmental body is the lead institution in setting international standards in the fight against money laundering and terrorist financing on a global scale; hereinafter referred to as the "FATF") and the MONEYVAL Committee of the Council of Europe, regularly published (updated three times a year) conclusions from the ongoing monitoring of countries that have significant shortcomings in the enforcement of AML/CFT measures, e.g.:
(a) the FATF Public Statement available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement-19october2012.html); i.e. the "black list";
(b) Improving Global AMLCFT Compliance: ongoing process available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/improvingglobalamlcftcomplianceon-goingprocess-19october2012.html); i.e. the "grey list";
(c) valid conclusions from FATF monitoring available on the website of the FIU (http://www.minv.sk/?vyhlasenia-fatf);
(d) the Public Statement on a member state, confirming that the country fails to comply with the basic reference documents for appropriate prevention of money laundering and terrorist financing, available on the website (http://www.coe.int/t/dghl/monitoring/moneyval/);
(e) currently valid conclusions from monitoring are published also on the website of the financial police intelligence (http://www.minv.sk/?moneyval-vyhlasenia);
(f) detailed evaluation reports on each member state and its system of prevention and repression in the field of money laundering and terrorist financing (in the form of a "Mutual Evaluation Report"), available in English on the website (http://www.fatf-gafi.org/topics/mutualevaluations/ and http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp);
(g) the list of equivalent third countries, which was created on the basis of agreement of the EU Member States in the European Commission committee ("CPMLTF" – Committee on Prevention of Money Laundering and Terrorist Financing), available on the Committee's website (http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf) as well as on the website of the FIU (http://www.minv.sk/?ekvivalent).

(9) In accordance with the implemented EU directives, the Act defines only the basic situations that pose an increased risk of money laundering and terrorist financing. However, the financial institution must apply a more stringent procedure for the identification and verification of facts ascertained and subsequent monitoring of the business relationship with a customer also in other situations, according to the customer's risk profile or according to the degree of risk inherent in the service or type of transaction provided to the customer.

(10) Enforcement and compliance of all these procedures and rules (identification, verification, KYC) provides, besides the recognition of unusual transactions and minimisation of the risk of money laundering and terrorist financing, also protection against fraud. At the same time it enables the financial institution to select and offer from the range of transaction types those that are suitable for particular customers according to the content and scope of their activities. This helps the financial institution retain customers not connected with money laundering and fraud and concurrently eliminate the risk of financial loss and reputational risk.

(11) Where the customer poses a high risk, this requires more detailed assessment of the customer and the customer's behaviour. It is then necessary to take measures to eliminate the risk to an acceptable level.

The financial institution shall exercise enhanced customer due diligence in situations that, with regard to their nature, may pose a high risk of money laundering or terrorist financing. The

financial institution shall pay particular attention to selected groups of subjects, e.g. politically exposed persons (Article 6 of the Act).

In the case of identifying politically exposed persons, financial institutions are recommended, in accordance with the new FATF international standards published in February 2012 on the website (http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html) to exercise enhanced customer due diligence not just to the sphere of persons referred to in Article 6(1) of the Act, but also to persons with permanent residence in the Slovak Republic.

In the process of the identification and verification of politically exposed persons it is recommended to use the existing commercial databases of high-risk customers, e.g.: World-Check database of high risk individuals and companies; website (http://www.world-check.com/).

In monitoring existing customers it is essential to focus also on the ongoing monitoring and verification as to whether the customer has become a politically exposed person; in such a case the consent of a managing employee, meaning an employee one or more management levels higher must be required for continuing the business relationship. Where a politically exposed person owns or works in the managing structure of a customer – legal person, or is a beneficiary, in such a case this constitutes a situation requiring the application of enhanced customer due diligence towards the customer – legal person.

In this regard it is necessary to respect the guideline of the FIU (in particular its second part) as published on the website (http://www.minv.sk/swift_data/source/policia/finpol/PEPS-usmernenie-20052011.pdf) .

(12) The Act in Article 13 allows the use of basic customer due diligence - other than the ongoing monitoring of a business relationship under Article 10(1)(d) of the Act - that has already been performed by another credit or financial institution in applying customer due diligence procedures, i.e. performance by third parties. This means that, as regards compliance with the conditions referred to in this provision of the Act, it is possible to rely on already-performed identification and verification of the customer and beneficiary and to receive or provide information on this identification and verification from/to a credit or financial institution (under Article 5(1)(b) points 1 to 10 of the Act) operating in the territory of an EU Member State (i.e. a third party), including those institutions operating in the territory of the Slovak Republic. Exchange offices and payment institutions are outside the sphere of obliged entities from which it is possible to accept identification and verification of a customer and beneficiary. Responsibility for the fact that information thus acquired meet the requirements for exercising customer due diligence under the provisions of the Act, nonetheless remains with the financial institution that decided to rely on the third-party performance approach. In such cases, in accordance with the practice in EU Member States, it is not necessary to specifically require the customer's consent to the provision of information to a third party.

Under Article 13(4) of the Act, the business relationships of a financial institution with entities that perform activities for the institution on the basis of an outsourcing contract shall not be deemed performance by third parties within the meaning of the said Article. Likewise, where a financial agent or financial adviser as an obliged entity performs identification, verification or due diligence in respect of a customer in accordance with the Act, this shall not be deemed as performance by third parties. These acts are considered as acts performed by the financial institution itself.

(13) Article 11 of the Act defines the scope and conditions for exercising simplified customer due diligence, i.e. a less demanding procedure in customer identification. The financial institution may use this option after careful consideration with the use of a risk-based procedure in the case of such situations and customers where it is possible to obtain and verify basic information from publicly available and reliable sources – as referred to in Article 11(1) of the Act.

Article 11(2) of the Act lays down the types of products in which simplified customer due diligence approaches may be used. It is important that before deciding to use simplified customer

due diligence the financial institution first obtain information about the customer or type of transaction that justifies the application of simplified customer due diligence. The use of simplified customer due diligence in no way represents an exemption from the duty to monitor the business relationship on an ongoing basis (Article 10(1)(d) of the Act), or from other duties defined by the Act, so that it is possible to comply with the provisions of Articles 14 and 17 of the Act, as well as others, including the duties to process and archive data according to the provisions of Articles 19 and 21 of the Act. In connection with the use of simplified customer due diligence there comes into consideration also the possibility to use a list of equivalent third countries, as created by agreement of the EU Member States, and published in English on the CPMLTF website, and on the FIU website. The fact that a country is included in the list, however, does not preclude that a particular customer from the country may be included in a higher risk category. Indeed, it is always necessary to consistently fulfil duties under the provisions of Article 10(1)(d), Article 10(4) and (8) of the Act.

Article 8
Detection, reporting and postponement of unusual transactions

(1) For identifying unusual transactions it is crucial that a financial institution apply the provisions of Articles 2 to 4, Articles 10 to 12 and Articles 14 and 20 of the Act. Under Article 14(1) of the Act a financial institution is required to assess whether an intended or ongoing transaction is unusual. Under Article 20(1) and (2)(d) of the Act a financial institution must regulate this part of the procedures in its Programme. Duties referred to in Article 14(1) and (2)(a) and (b) of the Act must be fulfilled demonstrably so that the financial institution can, in accordance with Article 30(3), in the case of an inspection, provide information and written documents on the fulfilment of these duties. Article 14(3) of the Act also emphasises the duty to draw up records on transactions under Article 14(2)(a) of the Act (i.e. internal reporting of unusual transactions), which must be archived in accordance with Article 30(3) of the Act for a period of five years.

(2) Under Article 4 of the Act an unusual transaction is a legal act or other act that indicates that its execution may lead to money laundering or terrorist financing. Article 4(2) of the Act provides a demonstrative presentation of unusual transactions. In each unusual transaction listed in this provision there are, however, several indicators of unusualness (e.g. an unusually high volume of funds with regard to the type of transaction, an unusually high volume of funds without clear economic or legal purpose, etc.) that the financial institution is required to assess and concurrently apply the KYC principle (the Act does not define any KYC principles, though where an obliged entity applies them in practice, it is necessary to thus define them in the Programme). Only by such action can it competently assess whether a customer's intended or ongoing transaction is unusual or not. The Act in Article 4 does not stipulate any criteria, e.g. in the form of threshold amounts of funds that would lead to the automatic finding in the case of a certain type of financial operation that it undoubtedly constitutes an unusual transaction. The decisive element for assessing a customer's transactions is the application of the KYC principle and the proper recognition of indicators of unusualness, as well as other signs or criteria that the financial institution is required to determine for itself, depending on the subject of its activity, when drawing up an overview of the types of unusual transactions (Article 20(2)(a) of the Act).

(3) The conditions for the proper application of the KYC principle derive from the duties of the financial institution and customer, as set out in the provisions of Articles 10 to 12 of the Act. The crucial provisions are those of Article 10(1), (4) and (5) and Article 11(3) of the Act. The procedure under the provisions of Article 10(1) and Article 11(3) of the Act enables a financial institution to satisfy itself as to the actual identity of each customer and identify the purpose and planned nature of business activities that a customer will probably conduct. This procedure is also the starting point for a financial institution in determining the customer's risk profile, subsequent determining the degree of customer due diligence pursuant to Article 10(4) of the Act and accepting

a customer. A financial institution then, depending on the result, shall apply procedures in the framework of basic customer due diligence under Article 10 of the Act or simplified customer due diligence under Article 11 of the Act or enhanced customer due diligence under Article 12 of the Act.

(4) Irrespective of whether a financial institution proceeds under Article 10, 11 or 12 of the Act No 297/2008, it is required always to also proceed in accordance with Article 14 of the Act. A financial institution is required, in applying each type of customer due diligence, to assess whether an intended or ongoing transaction is unusual (Article 14(1) of the Act) and to pay particular attention to all complicated, unusually large transactions and all transactions of an unusual nature that do not have a clear economic purpose or clear legal purpose and to make an appropriate record on them in accordance with Article 14(3) of the Act (i.e. internal reporting of an unusual transaction); it is also necessary to archive these records in accordance with the period referred to in Article 19 of the Act.

(5) A financial institution shall perform skilled assessment of intended and ongoing transactions under Article 14 of the Act at various time intervals and at various levels. The assessment process takes place:
(a) on the frontline, where the financial institution's staff are in contact with an existing or potential customer;
(b) in the framework of ongoing monitoring of an existing business relationship;
(c) in the framework of subsequent (retrospective) assessment of a customer's transactions.

(a) Assessment of transactions at initial contact with the customer before and during execution of a transaction

The assessment of a customer's transactions is performed by employees of the financial institution who, in fulfilling their duties, are in contact with the customer. The assessment of a transaction by an employee of the financial institution is thus performed largely at the place of executing the transaction and prior to its conduct, or at an attempt to execute a transaction so that an unusual transaction can be postponed and promptly reported. The assessment of transactions is dependent on the staff's expertise and knowledge that they have acquired in the framework of mandatory training (Article 20(3) of the Act).

Each of the relevant staff is required to have the Programme permanently available, either in paper or electronic form and is required to learn it and proceed according to it. An employee of a financial institution shall in this stage primarily follow Article 10(1) as well as Article 11(3) of the Act, which enables the employee to ascertain to an appropriate degree the real identity of the customer and to know the purpose and planned nature of the business activities that the customer will probably perform. This procedure is also the starting point for the financial institution in accepting a customer, determining the customer's risk profile and then determining the degree of customer due diligence pursuant to Article 10(4) of the Act.

A crucial element for assessing customers' transactions is the appropriate application of the KYC principle and its procedures and skilled identification of signs of unusualness. This procedure enables the employee to assess customers' intended or ongoing transactions by comparing them against an overview of types of unusual transactions (Article 20(2)(a) of the Act), as well as against forms referred to in Article 4(2) of the Act and to detect those that are unusual in relation to the customers and their otherwise usual transactions.

If an employee assesses an intended or ongoing transaction to be unusual, they shall make a written record on this transaction in accordance with Article 14(3) of the Act and promptly notify this finding to the Nominated Officer (hereinafter the "notification of unusual transaction").

(b) Assessment of transactions in the framework of ongoing monitoring of a business relationship

Depending on whether this concerns:

1. contracting of a business relationship (Article 10(2)(a) of the Act) or
2. an occasional transaction (Article 10(2)(b) and (c) of the Act),

the competent staff of the financial institution shall assess the customer's transactions also in the framework of ongoing monitoring of the business relationship.

The assessment of intended or ongoing transactions in the framework of ongoing monitoring of the business relationship is specific in that the business relationship has already started and still continues (Article 10(2)(a) of the Act). The customer may also be known to the financial institution where the customer has already executed several occasional transactions (Article 10(2)(b) or (c) of the Act). Therefore, this is not the first contact with the customer and the financial institution may take account of the customer's existing risk profile and history of transactions performed by the customer.

The procedure according to Article 10(1)(d) of the Act, including verification of the completeness and validity of identification data and information under Article 10(8) of the Act and the customer's duty under Article 10(5) of the Act form the basis for ongoing monitoring of the business relationship. This type of monitoring requires the creation of customer risk profiles and their classification with regard to the possible risk of money laundering and terrorist financing under Article 10(4) of the Act. Ongoing monitoring of the business relationship requires the use of an appropriate EIS that enables the financial institution, in accordance with risk-based prevention, to create financial or other criteria or limits as indicators of unusualness in customers' transactions so as to allow their differentiation into certain levels of the monitoring process, corresponding to the degree of risk inherent in the operations performed by customers. The criteria or limits defined by the institution for this purpose must be regularly verified so that it is possible to determine their adequacy in regard to the identified levels of risk. The financial institution is required also to regularly review the adequacy of the existing system and individual processes of protection and prevention.

For assessing transactions, importance shall be given, in the framework of ongoing monitoring of the business relationship, to intended or ongoing transactions of a customer that do not correspond to the customer's known or expected activity or that correspond to types of unusual transactions referred to in the Programme or in Article 4(2) of the Act. Such transactions of a customer shall form the subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record of them (Article 14(3) of the Act); these records must be archived in accordance with the period referred to in Article 19 of the Act.

The Nominated Officer may, on the basis of results from the assessment of the various circumstances of a transaction and with regard to the overview of types of unusual transactions (Article 20(2)(a) and Article 4(2) of the Act), reach the conclusion that in the given case it does not constitute an unusual transaction. If the conclusion cannot be reached solely on the basis of information on the customer that the financial institution already has available, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the Act.

In cases where the Nominated Officer is unable, even through this procedure, to identify the reason for the customer's transactions that do not correspond to the customer's risk profile or known or expected activities, it is sufficient that these operations merely indicate the fact that their execution may constitute money laundering or terrorist financing, and the Nominated Officer is required to proceed according to Article 17 of the Act, i.e. to report the unusual transaction to the FIU.

The assessment of transactions in the framework of ongoing monitoring of the business relationship is performed, depending on the transaction, by staff as well as the Nominated Officer.

(c) Assessment of transactions in the framework of subsequent or retrospective assessment of a customer's transactions

A means of subsequent monitoring of customers' transactions is, for example ex-post

random selection of executed transactions in the framework of an inspection from the side of a manager superior to the employee who executed the customer's operations, as well as in the framework of an inspection performed by the Nominated Officer and the internal audit unit.

(6) The recommended procedure in the processing and handling of internal notifications of unusual transactions and unusual transaction reports is as follows:
(a) All internal notifications of unusual transactions sent by competent staff to the Nominated Officer must be documented according to Article 14(3) of the Act and must be available for the purposes of inspection according to Article 29 of the Act.
(b) The sending of internal notifications and reports to the Nominated Officer may not be subject to the prior consent of any person.
(c) The Nominated Officer shall register and archive notifications on internal notifications of unusual transactions, including the position, first name, last name, workplace or unit of the financial institution and all data on the given customer and transaction in accordance with Article 19 of the Act.
(d) The Nominated Officer, as well as staff of the financial institution, including its managers (and members of the statutory body) involved in assessing transactions under Article 14 of the Act are required to maintain confidentiality on reported unusual transactions and on measures taken by the FIU (Article 18 of the Act), including the fulfilment of duties under the provisions of Article 17(5) and Article 21 of the Act; the financial institution may not, however, cite toward Národná banka Slovenska and the Slovak Ministry of Finance the duty to maintain confidentiality in connection with the performance of supervision and inspection under Article 29 of the Act (Article 18(5) of the Act). Provided that information given is used exclusively for the purposes of preventing money laundering or terrorist financing, the duty of confidentiality shall not apply to the provision of information between credit or financial institutions under the conditions set out in Article 18(8)(a) and (c) of the Act.
(e) The financial institution is required to draw up a procedure covering the period from the moment of detecting an unusual transaction through to prompt reporting of the unusual transaction, including the procedure and responsibility of staff who assess the transaction.
(f) The Nominated Officer, after receiving an internal notification of an unusual transaction, may confirm receipt of the notification on the unusual transaction to the employee who sent the notification. The confirmation should contain an instruction on the duty to maintain confidentiality under Article 18 of the Act. Where the financial institution has an electronic system of gathering internal reports that enables the competent employee to monitor the status or receipt of a submitted internal report of an unusual transaction by the Nominated Officer, or by the Prevention Unit, no individual confirmation of receipt of such a notification is needed.
(g) The internal notification of an unusual transaction, including the conduct of a customer or the transaction specified in the notification, shall be assessed by the Nominated Officer, who may, on the basis of results from further assessment of the various circumstances of the transaction, with regard to the overview of types of unusual transactions (Article 20(2)(a) of the Act) and with regard to Article 4(2) of the Act, decide whether it does or does not constitute an unusual transaction. This internal notification shall contain information on the economic or lawful purpose of the transactions and, in the case that the transaction is usual, also sufficient reasoning or statement of information and reasons regarding its usual nature. Otherwise the process of such assessment cannot be considered trustworthy and objective. If it is not possible to reach a decision solely on the basis of information on the customer that the financial institution already has available, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the Act. Where the Nominated Officer reaches the justified conclusion that in the case of an internally notified unusual transaction it does not actually constitute an unusual transaction, the Nominated Officer is required to document this decision in writing and to archive all related information, written documentation and electronic documentation in accordance with the period referred to in Article 19 of the Act.
(h) In cases where the Nominated Officer cannot even through this procedure reach the conclusion

that it is not an unusual transaction, it is sufficient that the transaction indicates that its execution may constitute money laundering or terrorist financing, and the Nominated Officer is required to proceed according to Article 17 of the Act, i.e. to report the unusual transaction to the FIU.

According to Article 17(1) of the Act, an unusual transaction or attempt to execute an unusual transaction must be promptly reported to the FIU. It is always necessary to take into consideration the particular circumstances of the situation in which the finding of the unusual transaction is made, whilst a financial institution is required to report an unusual transaction as soon as possible. The decision of the Nominated Officer to report an unusual transaction may not be subject to the consent or approval of any other person. A report of an unusual transaction shall contain information specified in Article 17(3) and may not contain information referred to in Article 17(4) of the Act. The reference number of each report of an unusual transaction should take the form: serial number / year / character code of the financial institution.

An unusual transaction may be reported in writing, electronically or by telephone (in this case it is necessary to report the unusual transaction also in person, in writing or by e-mail). The specimen form for reporting an unusual transaction, issued by the FIU, is given on the website (http://www.minv.sk/?vzory).

An unusual transaction report may be supplemented at the financial institution's own initiative within 30 days. After this period it is necessary to additionally report information and documentation acquired as another unusual transaction. In this subsequent unusual transaction the financial institution shall state the unusual transaction to which the additionally acquired information and documentation relate.

In connection with the reporting of unusual transactions and sending of further supplementary information, as well as the overall communication and exchange of information with the FIU, it is recommended in the interest of compatibility and streamlining of the procedure in the reporting process, as well as in the interest of streamlining control processes, that financial institutions communicate with the FIU by electronic means via the electronic registry, while complying with the conditions for protection of transmitted information and for clear identification and verification. Only in this way is it possible to avoid security risks connected with the reporting of unusual transactions by post, fax and e-mail,

(i) Article 18(8)(a) of the Act allows financial institutions, under defined conditions, to exchange information where this is reasonable and related to the threat of money laundering or terrorist financing, and where it helps obliged entities to more effectively assess a customer's transactions, as well as to alert other obliged entities to identified risks. An exchange of information may not contain the full scope of the reported unusual transaction as a whole, but only specific information relating to the risk of money laundering or terrorist financing. Information provided may, pursuant to the Act, be used exclusively for the purposes of preventing money laundering or terrorist financing.

(7) The recommended procedure in the postponement of an unusual transaction is as follows:

(a) According to Article 16 of the Act, a financial institution shall postpone an unusual transaction, i.e. a particular transaction (Article 9(h) of the Act) that would otherwise be executed.

(b) The financial institution is required under Article 16(1) of the Act to postpone an unusual transaction until the time of its reporting to the FIU, whilst account shall always be taken of the operating and technical possibilities, as well as the moment when the transaction was or should have been assessed as unusual; e.g. a customer's transaction assessed in the framework of ex-post or retrospective assessment of the customer's transactions can no longer be postponed.

(c) The financial institution is required under Article 16(2) of the Act to postpone an unusual transaction in the following two cases:

1. the financial institution shall postpone an unusual transaction at its own discretion if execution of the unusual transaction poses the risk that there may be frustrated or substantially impeded the seizure of proceeds from crime or seizure of funds intended for financing terrorism; in such a case

the financial institution is required to immediately inform the FIU of the postponement of the unusual transaction;
2. the financial institution shall postpone an unusual transaction if the FIU requests it to do so in writing; the reason for postponing an unusual transaction from the side of the FIU shall always be stated in the written request.
(d) The financial institution shall not postpone an unusual transaction if it is unable to do so for operating or technical reasons (it shall immediately notify the FIU of this fact) or if postponing the unusual transaction could, according to a previous notice from the FIU, frustrate the processing of the unusual transaction.
(e) The period of postponement of an operation pursuant to Article 16 of the Act shall be no more than 48 hours; therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to the law enforcement authority, the financial institution is required to extend the period of postponement, though no more than by a further 24 hours.

Therefore, the total duration of postponement of an unusual transaction is no more than 72 hours. If during the period of postponement of an operation the financial institution receives no instruction to seize funds from the side of a judge or prosecutor pursuant to Article 95 or 96 of Act No 301/2005 Coll. the Code of Criminal Procedure, as amended (hereinafter referred to as the "Code of Criminal Procedure"), the financial institution shall execute the postponed operation following the expiry of the set period. Prior to the expiry of the postponement period, the financial institution may execute the operation only in the case that the FIU notifies it in writing that from the aspect of processing the unusual transaction, its further postponement is not necessary. Weekends and bank holidays shall not be counted in the period of postponement of an unusual transaction.

The period of postponement of an operation pursuant to Article 16 of the Act shall be deemed to begin at the moment when the customer expresses the intention (will) to use the funds on their account. If the financial institution presumes that the customer will express an intention to execute an unusual transaction (use funds) in the future, it is required to take personnel, organisational and technical measures so that in the case that the customer does give such instruction, it is not executed and thereby any potential postponement of the unusual transaction is not frustrated.

The period of postponement of an operation pursuant to Article 16 of the Act may not be deemed to begin as of when the financial institution evaluated the executed transactions as unusual, or learnt of the customer's executed operations.

Article 9
Measures against terrorist financing

Terrorism represents one of the most serious forms of breaching values such as human dignity, freedom, equality and solidarity and respect for human rights and fundamental freedoms on which the European Union is founded. It also represents one of the most serious attacks on the principle of democracy and the principle of the rule of law, which are common to Member States and on which the European Union is founded. The Act prohibits the financing of terrorism and requires financial institutions to pay attention to transactions that may be related to terrorist financing.

(1) Definitions of terrorism and terrorist financing:

Act No 126/2011 Coll. on the implementation of international sanctions, as amended (hereinafter the "International Sanctions Act"), defines an international sanction as a restriction, instruction or prohibition issued for the purpose of maintaining or restoring international peace and security, the protection of fundamental human rights and the fight against terrorism. At the same time it specifically defines international sanctions in the field of trade and non-financial services, in the field of financial services and financial markets, money transfers, the use of other means of payment, the purchase and sale of securities and investment coupons, in the field of transport, posts,

postal services and electronic communications, in the field of technical infrastructure, in the field of scientific and technical relations, in the field of cultural and sports contacts.

The aim of sanctions is to maintain or restore international peace and security according to the principles of the UN Charter and Common Foreign & Security Policy. This primarily concerns changing the policy of a government, state, individual or group that does not respect the fundamental principles of the rule of law, that breaches human rights, international law or threatens security.

(2) Procedure in fulfilling the reporting duty:

(a) financial institutions shall, in the framework of CFT, apply toward customers procedures analogous to those applied in AML, including the reporting of unusual transactions connected with terrorist financing to the FIU;

(b) financial institutions are required to promptly report unusual transactions to the FIU (Article 17(1) of the Act); the Act defines unusual transactions as, inter alia, a transaction in which there is a justified assumption that the customer or beneficiary is a person against whom international sanctions have been imposed, or is a transaction in which there is a reasonable assumption that the subject of it is or should be a thing or service that may relate to a thing or service against which sanctions are imposed under the International Sanctions Act.

(3) Permission for funds transfer

Under Article 4(2) of the International Sanctions Act in conjunction with the respective EU Council Regulation on restrictive measures (e.g. EU Council Regulation No 267/2012 on restrictive measures against Iran) the Slovak Ministry of Finance is competent for the official procedure; e.g. to issue permits for a funds transfer following approval by other state authorities referred to in Article 14(5) and (6) of the International Sanctions Act. The requested authority is required to send an opinion within the term set by the Slovak Ministry of Finance, and this term may not be shorter than 10 days from the delivery date of the request. A shorter period may be set only in exceptional cases and must be thoroughly justified.

The competent unit is the **Financial Market Section of the Ministry of Finance of the Slovak Republic.**

(4) Consolidated list of persons subject to sanctions

Lists of persons subject to sanctions (natural persons and legal persons) form a part of the annexes to individual regulations and decisions of the EU, which obligate all financial institutions of Member States to immediately freeze financial and economic resources of persons subject to sanctions from states listed in the annexes to the individual regulations and decisions of the EU.

The regulations and decisions of the EU concerning exclusively persons subject to sanctions and comprehensive restrictive measures, including the consolidated list, which contains the names and identification data of all persons, groups and entities subject to financial restrictions of the EU Common Foreign & Security Policy (in the framework of enforcing the Common Foreign & Security Policy) are listed on the website (http://eeas.europa.eu/cfsp/sanctions/index_en.htm). In this regard, the EU sanctions are listed on the website of the Ministry of Foreign Affairs of the Slovak Republic, (http://www.foreign.gov.sk/sk/zahranicna__politika/europske_zalezitosti-sankcie_eu, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).

(5) Adoption of sanctions (restrictive measures):

(a) through the transposition of sanction resolutions of the Security Council of the United Nations (hereinafter referred to as the “UN Security Council”);

(b) in the case of autonomous sanctions adopted only by the EU, the sanctions are adopted through common positions of the EU and implemented at the EU level; in the case of autonomous sanctions, the EU may adopt also more stringent and broader sanctions than those of a sanction resolution;

(c) sanctions concerning persons against whom they were declared pursuant to a regulation of the Government of the Slovak Republic.

Restrictive measures are adopted in several forms. This concerns, for example, diplomatic sanctions, suspension of cooperation with a third country, boycott of sporting or cultural events, trade sanctions, arms embargoes, financial sanctions, flight bans, restrictions on entry to the territory of a member state. UN sanction measures concerning an arms embargo or visa bans are implemented directly by the member state.

Sanction measures concerning economic relations with third countries, for example freezing of financial assets and economic resources, are implemented by an EU regulation (approved by the Council) and are directly binding and applicable in the EU. Regulations have general application and are directly applicable in all Member States. As legally binding acts they take precedence over acts of the Slovak Republic, and financial institutions in Slovakia are required to directly apply sanctions declared in EU regulations. They are also the subject of legal assessment by European courts.

(a) Sanction resolutions of the UN Security Council

The UN Security Council Resolution against Terrorism is a document that provides the basis for criminalisation of incitement to terrorist acts and recruitment of persons for such acts. Resolutions call on states to adopt necessary and appropriate measures and, in accordance with their obligations arising under international law, prohibit by law the incitement to commit terrorist acts and to prevent such activity.

With regard to the above, sanctions are adopted through the transposition of sanction resolutions of the UN Security Council. This means that following the issuance of a UN Security Council resolution, it is necessary to implement the resolution in the shortest possible time in an EU regulation or in a common position of the EU.

An overview of comprehensive resolutions, sanction committees and UN policy against terrorism is published in English on the UN Security Council website (http://www.un.org/Docs/sc/).

(b) Autonomous sanctions adopted by the EU

The EU Common Position 2001/931/CFSP as amended by Common Position 2008/586/CFSP published a list of persons subject to sanctions (natural persons and legal persons) associated with terrorism and against whom it is necessary to apply sanctions in the fight against terrorism. Persons listed in EU Common Position 2001/931/CFSP are broken down into external terrorists and internal terrorists (in this case persons marked with an "*", who are EU citizens or are domiciled in the EU, e.g. members of the Basque organisation ETA and extremist groups, in particular from Spain and Northern Ireland).

Financial sanctions are applied against the group of external terrorists under Article 3 of EU Common Position 2001/931/CFSP. Implementation of these sanctions is governed by EU Council Decision 2005/428/CFSP and Council Regulation No 2580/2001, which in practice means that, on the basis of directly applicable EU legislation, sanctions are binding for everybody in all EU Member States and are directly enforceable.

Financial sanctions shall not apply against internal terrorists, since this is not permitted under the EU Treaty, which establishes a mandate for implementation of restrictive measures within the single market and financial services only towards third countries (Articles 60 and 301 of the EU Treaty, i.e. there is no mandate for imposing financial sanctions at the Community level against the EU's own citizens). Against internal terrorists, only enhanced judicial and police cooperation applies at the EU level on the basis of Article 4 of the EU Common Position 2001/931/CFSNP and in accordance with Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

(c) Procedure in the case of persons against whom sanctions have been declared under a regulation of the Government of the Slovak Republic

Persons included in the list of the EU Common Position 2008/586/CFSP, marked with an "*" are, however, terrorists and, on the basis of UN Security Council Resolution 1373/2001 on the

suppression of terrorist financing, as well as on the basis of Article 2 of the EU Common Position 2001/930/CFSP, all countries have the duty to freeze economic and financial assets of all persons designated as terrorists or who provide assistance thereto, or who are in any way linked to terrorist structures.

With regard to the above, the Slovak Republic has not been able to declare sanctions against internal terrorists of the EU; therefore, it has been necessary to codify the freezing of terrorist assets of such persons at the level of national legislation. The Slovak Republic declares international sanctions through a Government Decree, unless these result directly from the applicable law of the EU Act in accordance with Article 3 of the International Sanctions Act. Under Article 288 of the Consolidated Text of the EU Treaty, such an act is a regulation with general application. It is binding in its entirety and is directly applicable in all EU Member States. In Slovak law, international sanctions are declared by Slovak Government Regulation No 397/2005 Coll. declaring international sanctions ensuring international peace and security, as amended by Government Regulation No 209/2006 Coll., No 484/2006 Coll., No 488/2007 Coll. and No 239/2008 Coll., 168/2009 Coll. and Decree No 442/2009 Coll. (hereinafter referred to as "Decree No 397/2005 Coll."). Decree No 397/2005 Coll. and relevant EU regulations laying down restrictive measures include a list of those persons subject to sanctions whose activity is confined to the territory of EU Member States, or who are EU citizens. Financial institutions are required to immediately freeze all financial and economic assets of persons subject to sanctions included in the list published in the annex to Slovak Government Regulation No 397/2005 Coll. or in the relevant EU regulations governing restrictive measures.

Article 10
Archiving of data and documentation

(1) The financial institution is entitled, for the purposes of performing customer due diligence (Articles 10 to 12 of the Act) and without the customer's consent and without informing the customer concerned, to ascertain, acquire, record, store, use and otherwise process the customer's personal data and other information in the scope of Article 10(1) and Article 12 of the Act.

(2) The financial institution is entitled to acquire the necessary personal data also by copying, scanning or by other recording of official documents on information media, as well as to process birth registration numbers and other information and documents without the customer's consent and in the scope set out in the mentioned provisions of the Act.

(3) The financial institution shall store (archive) information on the identification of customers and on the verification of identification, records on customers' transactions and records on ascertaining beneficiaries, including photocopies of relevant documents.

(4) Within the meaning of Article 19(1) and (2) of the Act, the financial institution is required to archive for the period of five years:
(a) from the end of the contractual relationship with a customer, information and written documents acquired by way of the procedure under the provisions of Articles 10 to 12 of the Act,
(b) from the execution of a transaction, all data and written documents on the customer.

The financial institution shall archive this data and written documents for longer than five years if the FIU requests it to do so by way of a written request containing the period and scope of archiving data and written documents. This duty shall also apply to a financial institution that ceases business, up until the expiry of the period during which it is required to archive these data and written documents.

Whereas the Act lays down a five-year period, Article 47(9) of the Insurance Act requires financial institutions to store insurance contracts (including amendments thereto and related

documents), information and copies of documents proving the customer's identity, and documents on the determination of the ownership of funds used by the customer to conclude the insurance contract, for the duration of the insurance period and thereafter until the expiry of the statute of limitations for exercising rights arising from the insurance contract, but for at least ten years after the termination of the contractual relationship with the customer.

Národná banka Slovenska, for the purpose of exercising supervision, requires financial institutions to retain the information and documents defined under Article 47(9) of the Insurance Act for at least ten years after the termination of the contractual relationship, whereas other data and documents prescribed by law (e.g. records on internal notifications of unusual transactions and unusual transaction reports, records on staff education and training, etc.) shall be retained during the period stipulated under Article 19 of the Act, i.e. the five-year period, unless the FIU requests a longer period for data retention by a way of procedure under Article 19(3) of the Act.

(5) In view of the importance of information acquired by financial institutions in fulfilling AML/CFT duties under Article 14(2)(a) of the Act, it is recommended that written records referred to in paragraph 3 of that provision be archived for the statutory period (five years from the written record being made).

(6) The financial institution's procedure in archiving data and documentation, and records related to AML/CFT shall be governed by the financial institution's Programme, which should, in accordance with the Act, specify in more detail the following:

(a) the records that need to be archived (at least information on customer identification and records on the customer's transactions, including written records under Article 14(3) of the Act and information on identification of the beneficiary),

(b) the form of records (paper, electronic),

(c) the place, method and period for which records are to be archived, taking account of

1. the end of the contractual relationship with the customer,
2. the execution of a transaction with the customer, and
3. any written request of the FIU and the period specified (Article 19(3) of the Act).

(a) Records that need to be archived

1. records on customers' risk rating

Documents and information related to customers' assignment to risk groups must be archived. The financial institution shall record and archive any important information confirming circumstances justifying a customer's reassignment to a different risk group (and therefore a change of their risk profile) together with other information on the customer.

2. records on transactions

Internal regulations of the financial institution shall establish the duty to record all transactions executed for customers in the financial institution's accounting and reporting.

3. records on internal notifications of unusual transactions and unusual transaction reports

The financial institution shall archive all reports on customers' suspicious activities, namely internal notifications of unusual transactions intended for the Nominated Officer, as well as unusual transaction reports sent by the Nominated Officer to the FIU.

If the Nominated Officer, after assessing the relevant information and knowledge concerning a customer's suspicious activity, decides that the activity does not constitute an unusual transaction and does not report it to the FIU, the reasons for that decision must also be recorded and archived together with the records on the particular transaction.

4. records on implemented education and training

The financial institution shall archive records on staff training, containing the date and content of the training and the confirmation that the respective employee attended the training and was familiarised with the financial institution's AML/CFT Programme, as well as related internal regulations of the financial institution.

5. Programme

The financial institution shall archive the Programme, which shall contain information on statutory provisions, staff responsibilities, and mainly on any operational procedures and duties of staff at the financial institution in the performance of relevant types of customers' transactions and trading operations, including the most common types of unusual transactions at the given financial institution.

6. records on inspections performed

The financial institution shall archive records on inspections performed in accordance with Article 11.

(b) and (c) Form of records as well as place, method and period for which records must be archived

Originals or photocopies of paper documents and documentation, as well as data stored in personal computers and on mechanical media for electronic data must be archived. Archiving periods are the same, regardless of the form in which the data is archived.

After the expiry of the statutory period or period stipulated by the Insurance Act, the financial institution shall archive such information and documents which relate to those customers and their transactions in the case of which an investigation has been started by law enforcement authorities or a criminal prosecution begun, and which are useful for the purposes of investigation and criminal prosecution; archiving shall be maintained on the basis of a written request by the FIU pursuant to Article 19(3) of the Act, in the scope and for the period stated in the request.

In this context, the FIU's instruction published on the website (http://www.minv.sk/swift_data/source/policia/finpol/Par19ods-2-pism-b-usmernenie.pdf) shall be respected.

(7) Records prepared and archived by the financial institution shall satisfy statutory requirements for record keeping on customer data and also enable:
(a) an independent party to evaluate the efficiency of compliance with basic principles, as well as the financial institution's AML/CFT procedures,
(b) reconstruction of the course of transactions made by the financial institution for a customer,
(c) identification and location of each customer,
(d) identification of all internal notifications of unusual transactions and external unusual transaction reports,
(e) fulfilment, within a reasonable time, of statutory requirements of the FIU, supervisory authority and law enforcement authorities concerning a customer and a transaction.

Article 11
Securing the system and ensuring performance of internal control

The financial institution must have in place a reliably functioning system of control focused in part on the fulfilment of AML/CFT measures.

(1) The system of control shall comprise a specification of control responsibilities at all levels of the management as well as the performance of control activity itself by:
(a) supervisory board,

(b) insurance company's statutory body,
(c) Nominated Officer (his deputy and the Prevention Unit),
(d) managerial staff,
(e) staff involved in the processing of customers' transactions,
(f) staff coming into contact with customers in entering into transactions,
(g) internal audit unit responsible for controlling all units, including the Nominated Officer, Prevention Unit, and relevant staff.

(a) and (b) Control performed by the insurance company's statutory body and supervisory board

Control shall be based on generally binding legal regulations and internal regulations of the financial institution and derive from the position in the hierarchy of the financial institution's management system. The statutory body of an insurance company and the branch's Responsible Person shall regularly, at least once a year, evaluate the effectiveness of the existing system – the financial institution's AML/CFT policy, the Programme and specific measures, including the activity of the relevant units and staff.

(c) and (d) Control activity performed by the Nominated Officer and managerial staff

Control activity shall be based on powers, duties and responsibilities of the Nominated Officer and all managerial staff of the financial institution and shall be performed as a regular and ongoing control of the performance of work duties, consisting in the verification and approval of the quality, level or state of the performance of subordinate staff's work activities in the field of AML/CFT.

(e) and (f) Control performed by staff

This represents an ongoing control process at various units of the financial institution performed on a daily basis. It comprises control mechanisms that are a direct component of staff's working procedures as well as their work duties, tasks and responsibilities in the first contact with customers, as arise from AML/CFT.

(g) Internal audit

The internal audit unit controls compliance with the Programme and internal regulations and verifies adopted AML/CFT procedures, as well as the performance of duties by staff, managerial staff and the Nominated Officer (his deputy and the Prevention Unit).

The performance of control shall be focused primarily on controlling:
1. the performance of the relevant degrees (levels) of customer due diligence,
2. procedures for ensuring that customer information received is up-to-date (verification),
3. the assessment of specific transactions, monitoring of customers and business relationships,
4. risk evaluation and management,
5. internal notification of unusual transactions and reporting of unusual transactions to the FIU,
6. the implementation of staff training, and
7. records archiving.

The financial institution's AML/CFT system and processes should regularly be subject to internal audit within which the functionality, effectiveness and efficiency of all elements, tools, procedures, management and control mechanisms applied in this area should be evaluated.

(2) The internal audit should be performed in compliance with the work program of the internal audit unit in such periodicity which will arise from evaluation of the degree of risk inherent in individual areas of financial institution's activity, at least once per calendar year. Members of the

statutory body of the insurance company and head of a branch should be regularly informed of the results of audits performed.

Article 12
Final provision

This methodological guideline shall become effective on the day of its publication in the Journal of Národná banka Slovenska.

Ing. Vladimír Dvořáček, m.p.
Executive Director
Financial Market Supervision Unit

ANNEX
(source: FIU)

General methods of recognising unusual transactions

1. A transaction which by virtue of its complexity, unusually high volume of funds or other characteristics clearly deviates from the ordinary framework or nature of a transaction of that type or particular customer, or which has no clear economic or lawful purpose.
2. A transaction in which the business partner refuses to provide information on the intended transaction or seeks to provide as little information as possible or provides only such information that the obliged entity can check with great difficulty or at high cost.
3. A transaction in which the business partner requests the establishment of a contractual relationship or execution of a transaction with the obliged entity on the basis of an unclear project.
4. A transaction in which a request was submitted from the side of customer to arrange a transaction or intermediate a contract and where it may be assumed that the customer, in view of their standing, employment or other characteristic, is not or cannot be the true owner of funds.
5. A transaction in which the volume of funds that the customer possesses is clearly not commensurate with the nature or scope of the customer's business activity or declared financial circumstances.
6. A transaction whose relationship to the ordinary business activities of the customer is not evident and which is atypical for the customer.
7. A refusal to prove identity when concluding a business relationship.
8. A transaction in which the business partner submits documents issued by an unknown financial institution.
9. A transaction in which the business partner lacks documentation expected in legitimate transactions.
10. A transaction in which the customer uses or tries to use fake or stolen identification documents.

Specific methods of recognising unusual transactions in insurance activities

1. Concluding a transaction which exceeds the nature and scope of business activities of the policyholder.
2. Multiple repeated changes in the policyholder’s account over a year with respect to payment or refund of the premium.
3. The customer requires the insurance contract to be transferred to another person prior to the expiry of its maturity.
4. The customer pays in advance for many years ahead.
5. The customer asks to insure an item which bears signs of having been stolen.
6. The customer concluded several life insurance contracts at the same time and for each of them the premium was paid in cash.
7. Concluding an insurance contract with an annual premium exceeding EUR 15,000.
8. The customer pays the premium exclusively in lower denomination banknotes.
9. Cash payment of life insurance instalments exceeding EUR 2,000 for one insurance contract.
10. Payment by bank transfer from several banks, mainly from abroad.
11. Repetitive concluding of (three or more) insurance contracts for unusually high amounts.
12. Very short time (less than 3 months) between the conclusion of the contract and its cancellation, where the premium exceeds EUR 15,000.
13. The customer pays funds in cash or by credit transfer to the account of the insurance company and subsequently announces to the insurance company that they did so by mistake and requests to

have the money returned to them, but to a different account, or requests to have it returned by postal order.
14. A refusal to state on whose behalf the insurance contract is concluded.
15. For investment products, three and more repeated deposits made by credit transfer to an account, including premiums of less than EUR 15,000.
16. The customer makes a payment of two instalments and then asks for a refund to another account.