Methodological Guideline
of the Financial Market Supervision Units of Národná banka Slovenska
No 5/2019 of 9 May 2019
on the prevention of money laundering and terrorist financing at life insurance undertakings, branches of life insurance undertakings from other EU Member States and branches of life insurance undertakings from other than EU Member States

Národná banka Slovenska, Financial Market Supervision Units, on the basis of Article 1(3)(a), point 3 of Act No 747/2004 on financial market supervision, as amended, has issued this Methodological Guideline:

Article 1
Purpose

The purpose of this Methodological Guideline is to provide life insurance undertakings, branches of life insurance undertakings from other EU Member States and branches of life insurance undertakings from other than EU Member States in the territory of the Slovak Republic (hereinafter 'insurance undertaking', 'branch' or 'financial institution') a more detailed explanation of their obligations arising from Act No 297/2008 on the prevention of money laundering and terrorist financing (and amending certain laws), as amended (hereinafter 'the Act'), and Act No 39/2015 on insurance (and amending certain laws), as amended (hereinafter 'the Insurance Act').

Article 2
Organisational structure of a financial institution ensuring effective and independent performance of activities in the anti-money laundering and counter-terrorist financing field

(1) Under Article 23(2) of the Insurance Act, insurance undertakings shall have in place an effective system of governance which provides for sound and prudent management of the business. The system shall at least include an adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities, including in the anti-money laundering (hereinafter 'AML') and countering financing of terrorism (hereinafter 'CFT') field.

(2) Within the organisational structure, a branch shall designate a senior manager as the person responsible for the AML/CFT field, or it shall determine that the head of the branch is responsible for the AML/CFT area (hereinafter the 'branch's Responsible Person').

(3) The overall AML/CFT responsibility of an insurance undertaking lies with the statutory body of the insurance undertaking.

(4) The overall AML/CFT responsibility of a branch lies with the branch's Responsible Person.

(5) Responsibility for the practical implementation of AML/CFT measures, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT policy, the reporting of unusual transactions (hereinafter 'UT') and for the financial institution's ongoing contact with the Financial Intelligence Unit (hereinafter 'the FIU') lies with the Nominated Officer under Article 20(2)(h) of the Act (hereinafter 'NO').

(6) It is not appropriate to outsource the activities of the NO.

(7) Financial institutions shall ensure full substitutability of the NO by means of their deputy.

(8) In filling the posts of the NO and deputy NO, financial institutions shall require candidates to demonstrate civic integrity, an appropriate level of education and corresponding professional experience.

(9) Only a senior manager directly reporting to the statutory body or a member of the statutory body may be appointed the insurance undertaking's NO. The NO of a financial institution shall comply with the fit and proper requirements laid down in Article 24 of the Insurance Act. Where the NO is not a member of the statutory body, the NO and deputy NO shall be appointed and dismissed by the statutory body of the insurance undertaking. The NO must be able to communicate directly with the statutory and supervisory body of the insurance undertaking and must have access to the information and documents acquired by the obliged entity while performing customer due diligence.

(10) The NO of a branch shall be appointed and dismissed by the branch's Responsible Person or by the head of the branch. The NO of a branch shall report to the branch's Responsible Person or to the 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 such places, who need not be a member of the unit responsible for the performance of activities of the prevention system (hereinafter 'the Prevention Unit'), and entrust that employee with the performance of selected activities pertaining to the NO or to the Prevention Unit (hereinafter the 'Authorised Employee'). The Authorised Employee maintains an ongoing working contact with the NO. Where financial institutions also establish a Prevention Unit, the NO shall be the manager of that unit.

(11) The NO's job description shall include in particular:
(a) ongoing preparation and updating of the Programme and any other necessary AML/CFT regulations and procedures;
(b) the performance of management and control tasks in the field within the Prevention Unit, if established, for which they are responsible;
(c) communication, cooperation and ongoing maintenance of contact with the FIU, including the timely reporting of UTs;
(d) organisation and setting of rules for the training of the financial institution's relevant staff, including new employees;
(e) analytical and advisory activity in relation to the assessment and reporting of UTs by the relevant staff in connection with the execution of customers' products, services and transactions.

(12) The NO and their deputy shall perform their duties with due professional diligence. The NO of an insurance undertaking shall submit a report on their activity or on the activity of the Prevention Unit, if established, to the statutory body at least once a year. The NO of a branch shall submit a report on their 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 UTs reported by the staff;
(b) statistics and a brief description of UTs that have not been reported to the FIU, specifying the underlying rationale;
(c) statistics and a brief description of UTs reported to the FIU;
(d) an 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.

(13) An important element of the financial institution's AML/CFT policy is to ensure that the NO, their deputy and the Prevention Unit have a sufficiently independent status within the structure of senior management and organisational units. The classification of the NO within the financial institution's organisational structure shall meet the following criteria that guarantee an adequate definition of the NO's position, as well as that of their deputy and, if relevant, of the Prevention Unit:
(a) powers and duties of the NO and their deputy in their job descriptions, with emphasis on their primary area of 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 the execution of customers' products, services and transactions;
(c) unlimited access for the NO and their deputy to all documents, databases and information at the financial institution;
(d) autonomous and independent decision-making of the NO and their deputy when assessing the unusualness of customer transactions reported by the respective staff within the framework of the internal reporting system;
(e) autonomous and independent decision-making regarding the reporting of UTs to the FIU;
(f) control function of the NO, their deputy and the Prevention Unit in relation to units and staff responsible for the execution of customer's products, services and transactions;
(g) separation of the NO, their deputy and the Prevention Unit from the internal audit unit within 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 a member of the statutory body or the branch's Responsible Person.

Article 3
Financial institution's anti-money laundering and countering financing of terrorism policy

(1) Financial institutions shall prepare their own policy concerning the prevention and detection of money laundering and terrorist financing (hereinafter 'the AML/CFT policy'). The AML/CFT policy shall ensure effective performance of the financial institution's AML/CFT activities.

(2) The AML/CFT policy forms a part of the financial institution's risk management system, and operational risk management in particular.

(3) The AML/CFT policy shall include in particular the following components:
(a) an organisational structure which ensures effective and independent implementation of AML/CFT measures;
(b) a programme of own activity under Article 20 of the Act (hereinafter 'the Programme').

(4) The AML/CFT policy of an insurance undertaking shall be approved in writing by its statutory body, which is responsible for its implementation. The AML/CFT policy of a branch shall be approved by the branch's Responsible Person, who is also responsible for its implementation.

Article 4
Financial institution's programme of own activity

(1) Financial institutions shall prepare the Programme as an internal regulation, approved by the statutory body of the insurance undertaking or by the head of the branch. The Programme shall be based on legislation of general application and it shall take into account the insurance

undertaking's Articles of Association and its AML/CFT policy. The Programme represents a transposition of the AML/CFT policy into practical principles, tasks, procedures, obligations and responsibilities in the AML/CFT field. It also contains specific powers, obligations, responsibilities and tasks of the NO, Prevention Unit and relevant staff of the financial institution in the performance of insurance activities (mainly Article 20(2) of the Act) relating to AML/CFT, as well as the control powers of these entities and control powers of the internal audit unit. In addition, the Programme defines information flows, information systems, as well as control processes and mechanisms in this field.

(2) In creating the Programme, financial institutions shall take into account their own specificities, in particular their size and market share, organisational arrangement and the range of insurance activities. The Programme shall contain not only information on statutory provisions and staff responsibilities, but in particular all operational procedures and duties of staff at the financial institution in the execution of relevant types of customers' products, services or transactions, as well as the most common forms of UTs recorded at the financial institution.

(3) The Programme shall set out in particular:
(a) the tasks, duties and responsibilities for the comprehensive protection of the financial institution in the AML/CFT field at the individual levels of management, from the financial institution's management board or the branch's Responsible Person down to front office units, including the Prevention Unit;
(B) the NO under Article 20(2)(h) of the Act, specifying their full name and employment position;
(c) the persons at the financial institution who assess whether an intended or ongoing transaction is unusual;
(d) the time when such assessment is to be carried out (where possible, always before executing a transaction or in the process of its preparation);
(e) the method of performing the assessment under points (c) and (d), i.e. what needs to be done during such assessment, what aids are to be used, and how and where the assessment result are to be recorded;
(f) the arrangements for the AML/CFT measures, the receipt of notifications of identified UTs from organisational units, the evaluation of these notifications and the reporting of UTs to the FIU, as well as arrangements for the ongoing working contact with the FIU or with law-enforcement authorities;
(g) the basic tasks of the relevant staff at all levels of management, the detection of UTs and the submission of internal notifications of UTs to the NO (possibly also a specimen form for internal notifications of UTs) and the manner of ensuring protection of the relevant staff in connection with UTs they identified and reported to the NO;
(h) the obligation to perform identification and verification of the customer's identity;
(i) the obligation to record the identification and verification of the customer's identity, as well as all transactions executed for the customers;
(j) the obligation to store the records of identification and verification of the customer's identity, and of transactions executed by the customers, and this for the period set out in the Insurance Act;
(k) an overview of specific forms of UTs that the obliged entity may be exposed to within its business activity;
(l) the assessment and management of the money laundering (ML) and terrorist financing (TF) risks under Article 20a of the Act, including procedures for customer evaluation on a risk-sensitive basis, taking into account own risk factors and risk factors set out in Annex 1 hereto;
(m) the specification of method and extent of customer due diligence on the basis of the risk assessment under Article 10(4) of the Act, as well as other measures based on the level of ML/TF risk under Article 12(2) of the Act;
(n) detailed signs of unusualness by which the customer's UTs can be recognised;
(o) the method and extent of feedback at the financial institution regarding internal notifications of UTs;

(p) the procedure to be followed by the relevant staff and NO in delaying UTs under Article 16 of the Act and in declining transactions under Article 15 of the Act;
(q) the content and timetable of staff training, the training of the financial institution's relevant staff for performing AML/CFT tasks;
(r) the obligation to maintain confidentiality in respect of internal notifications on UTs and their reporting to the FIU, and in respect of measures adopted by the FIU (Article 18 of the Act), primarily in relation to the customer concerned, as well as to persons with certain links to the customer (e.g. beneficiaries) and to third parties, other than exceptions laid down by the Act;
(s) measures and control mechanisms preventing the abuse of position or function by the relevant staff to deliberately engage in ML and TF while performing their tasks;
(t) the method and time periods for storing data and documentation;
(u) an internal AML/CFT control system which includes control mechanisms, process controls of senior managers, including controls by the NO and internal audits;
(v) the definition of information flows and description of information systems used to collect, process and report relevant AML/CFT information, including regular reports submitted to the financial institution's management and supervisory board and to the branch's Responsible Person or head of the branch;
(x) the description and use of the Know Your Customer principle (hereinafter 'the KYC principle').

(4) Financial institutions shall make the Programme accessible to all staff, for example via an internal computer network.

(5) The Programme needs to be updated in particular with any change in the financial institution's business scope or before the institution starts providing new products where the change in business scope or provision of new products could potentially lead to higher ML/TF risks. The appropriate period for updating is once a year.

Article 5
Good repute of staff

Before accepting an employee to a position or function where they will be in direct contact with customers executing their transactions, financial institutions shall verify by means of the potential employee's criminal record check certificate that they have not been lawfully convicted of any property-related criminal offence, criminal offence committed in a managerial position or another deliberate criminal offence. Financial institution should also require potential employees to provide an assessment issued by their previous employer.

Article 6
Staff awareness and training

(1) The statutory body of an insurance undertaking or the branch's Responsible Person, together with the NO, shall ensure that the staff are aware of the financial institution's responsibility, as well as of personal responsibility of the staff and their protection in case of identifying UTs.

(2) Financial institutions shall inform their staff in an appropriate manner who performs the function of the NO and who is their deputy.

(3) In their Programmes, financial institutions shall determine the optimal regime and method for:
(a) informing their staff about the AML/CFT system and related procedures, obligations and powers;
(b) making the Programme and any other relevant regulations accessible to the relevant staff;

(c) organising regular training and educational activities for staff; where regular training is conducted 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 with personal or other training methods so that the training system is effective.

(4) In informing and training their staff, financial institutions shall take account of their specific circumstances, in particular their size, organisational arrangement, types of products, services or transactions executed for their customers, so that all the necessary information reaches the 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 NO and relevant senior managers of the financial institution, as well as the model for performing staff training is effective, flexible and fulfils the desired objective; therefore it is essential that it be updated in response to changing conditions.

(5) The effectiveness of a financial institution's AML/CFT measures depends largely on the level of knowledge of its senior managers and other staff about the subject matter, i.e. to what extent do they familiarise themselves with basic legal regulations, the Programme and other related internal regulations of the financial institution.

The diverse typology of products, services or transactions executed, and the diversity in the structure of customers in particular, gives rise to varying levels of risk and different techniques of ML/TF.

The relevant staff (front office staff) must have all the necessary information on financial operations and types of products, services or transactions they will execute for customers and they must familiarise themselves as soon as possible with the criteria (signs of unusualness) for assessing or detecting UTs. They must be able to assess the conduct of the financial institution's customers and to evaluate the content of transactions executed by the customers in terms of their riskiness, unusualness or suspiciousness. Training of staff should significantly contribute to the staff acquiring prerequisites for mastering the procedures for applying the KYC principle and for recognising the level of risk associated with the actions of the financial institution's customers, also with regard to customers' categorisation into one of three groups of customer due diligence:

- basic;
- simplified; and
- enhanced.

(6) Within the training framework, financial institutions shall ensure that their staff are familiarised with the consequences of negligence or negligent fulfilment of their work duties and of any knowing or unwitting participation in ML/TF, and with the consequences of a breach of the prohibition of providing customers with information that are subject to confidentiality (Article 18 of the Act), as well as with the manner of their protection if they detect a UT.

(7) Financial institutions must have a project or plan of staff training which takes into account the work classification of their employees (own categorisation according to job positions, taking account of the exposure of employees to opportunities for and attempts at misuse for the purposes of ML/TF) and the resulting responsibilities, obligations, and the level and frequency of corresponding training. In determining the appropriate frequency of training, financial institutions shall proceed in line with the provisions of Article 20(3) of the Act (once per calendar year and always before an employee is assigned to work in which they perform tasks under the Act). The training plan, or its basic principles, should be 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 UTs within the financial institution or within the group.

(8) Under Article 20(3) of the Act, financial institutions shall ensure staff training focused on familiarisation with the Programme at least once per calendar year and always before an employee is assigned to work in which they will perform tasks set out in the Act and in the Programme. Each employee who performs tasks under the Act shall be familiar with the applicable Programme governing procedures for assessing customers and their financial operations; financial institutions shall ensure that the Programme is accessible to the entire staff at all times.

Staff training shall include in particular:

(a) familiarisation with the Programme;

(b) knowledge arising from the activity of the NO and that of other financial institutions, and available knowledge arising from the activity of the FIU or supervisory authority;

(c) practical examples of the assessment of customers' products, services and transactions or risks associated with customers;

Where necessary, financial institutions shall repeat and supplement the training with new knowledge 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 (lectures, electronic, etc.) should be regularly alternated. The acquired knowledge of relevant staff should be verified by means of tests.

(9) Given the difference of approach of financial institutions to staff training and to verification of their knowledge, the following harmonisation is required:

- knowledge of all staff shall be verified once a year;
- in addition to theory (programme of own activity, legislation), the training shall also focus on practical aspects of assessing customers and their products, services and transactions, performing customer due diligence (e.g. establishing the source of funds, repeated basic and enhanced customer due diligence), reporting potential UTs, etc.;
- special training shall be organised for selected staff and tied financial agents who may be more heavily exposed to opportunities for and attempts at misuse for the purposes of ML/TF;

(10) Financial institutions shall draw up records of staff training sessions conducted, containing the participation date of the relevant staff, the content and form of the training, and, where relevant, an evaluation of the tests completed, as well as the employees' signatures or other electronic confirmation of their participation. In addition to this, financial institutions shall obtain a written or electronic confirmation from the relevant members of staff that they have familiarised themselves with the Programme and related regulations governing the AML/CFT procedures.

Article 7
Information system at a financial institution

(1) As part of a systemic approach to risk management and AML/CFT activities, financial institutions shall establish appropriate information flows to ensure smooth, timely and regular flow of information between individual levels of management at the financial institution, including its statutory body, the NO and their deputy, Prevention Unit, internal audit unit and the relevant staff. A systemic approach to ensuring information flows also requires support in the form of application software, i.e. a specialised information system or systems. In broader terms this means a system of acquiring, processing, evaluating, transferring, as well as using information concerning this field. The system includes flows of AML/CFT information in the processes of the financial institution's individual activities and types of products, services or transactions executed. For the prevention of ML/TF to be effective, it is essential that the system is regularly updated.

(2) Financial institutions shall establish information flows for:

(a) the transmission of information to staff on AML/CFT principles, relevant procedures, duties and powers, and the related performance of day-to-day tasks;
(b) making the Programme and other relevant internal regulations available to staff;
(c) the transmission of necessary information between the Responsible Person and the NO;
(d) the transmission of information between staff and the NO and vice versa, including internal notification of UTs;
(e) the record-keeping, i.e. the recording, processing and updating of information on customers, and the recording and monitoring of customer transactions;
(f) notifying the statutory body or Responsible Person of the results of controls performed by the NO and the internal audit unit, as well as informing staff of these results;
(g) the transmission of information between the NO and the FIU, including the reporting of UTs and provision of other necessary information and documentation to the FIU, and the provision of feedback from the FIU to the financial institution;
(h) searching for UTs in the financial institution's relevant information systems which contain information on customers and their transactions.

(3) Financial institutions should set the form, content and rules of their information flows proportionately to their size, focus, the scope and complexity of activities performed and types of products, services or transactions offered, and the characteristics of their customers.

(4) An essential component of a financial institution's information system is an electronic information system (hereinafter 'EIS') which complies with statutory requirements and ensures sufficient level of protection against ML/TF. The EIS, which records and processes information on customers and their transactions, shall take into account the identification data set out in Article 7 of the Act. The EIS shall also contain information or records on the nature of the customer's business relationship. The nature of a business relationship is determined by the type of products, services or transactions under Article 9(h) of the Act or solely by the transaction under Article 9(g) of the Act; the nature of the business relationship is primarily predetermined by the actual product or service that the customer uses. The EIS and the way how it is used should make it possible to identify UTs executed 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, between unusual transactions of different customers.

(5) A special type of information recorded and monitored by the EIS is information on politically exposed persons under Article 6 of the Act obtained by the relevant staff while performing their work tasks.

(6) The EIS shall enable financial institutions to provide to the FIU, upon request and without undue delay, information as to whether they have or have had a business relationship with a specific person in the past five years, as well as information on the nature of that business relationship (Article 21(1) of the Act).

(7) In cases specified by the Act, the EIS shall also be capable of providing timely and sufficient information to the FIU, Národná banka Slovenska and law enforcement authorities. The EIS shall comply with the requirements for the purposes of control for the financial institution's own needs and for the needs of the FIU (Article 30 of the Act), as well as for statistical purposes.

Article 8
Customer identification and customer acceptance, customer risk profile; basic, simplified, enhanced customer due diligence, performance by third parties

(1) Basic obligations of financial institutions in these areas are governed in particular by the provisions of Articles 7, 8, and 10 to 13 of the Act, and Article 78 of the Insurance Act.

(2) Under Article 78(1) and (2) of the Insurance Act, financial institutions are entitled, for the purposes of identification and verification of identity of the customer and their representatives, conclusion of insurance policies and management of insurance, as well as for other purposes stated in Article 78(3) thereof, to request from the customers and their representatives the information defined in Article 78(1)(a) thereof and to obtain it by the means defined in Article 78(1)(b) thereof, and the customers shall meet that request. Under Article 11(2) of the Act, financial institutions shall perform basic customer due diligence when concluding a **life insurance policy** with an insurance premium for a calendar year exceeding EUR 1,000 or a single premium exceeding EUR 2,500. Where the insurance premium in a life insurance policy does not exceed EUR 1,000 or the single premium does not exceed EUR 2,500, financial institutions may perform only simplified customer due diligence. When concluding **non-life insurance policies**, basic customer due diligence under Article 10(1) of the Act is not performed; in these cases, financial institutions may perform identification and verification of the customer's identity pursuant to Article 78(1) and (2) of the Insurance Act.

(3) Basic customer due diligence under Article 10(1) of the Act shall include the following:
(a) identification and verification of the customer's identity;
(b) identification of the beneficial owner and adoption of appropriate measures for verification of their identity, including measures to determine the ownership and management structure of the customer who is a legal person or a trust; when identifying the beneficial owner, obliged entities shall not rely exclusively on data from the register of legal persons, entrepreneurs, and public sector entities;
(c) acquiring information on the purpose and intended nature of the product, service or transaction, or those of the business relationship;
(d) ascertaining whether the customer or their beneficial owner is a politically exposed or a sanctioned person;
(e) depending on the ML/TF risk, ascertaining the origin of funds or assets used in a transaction or business relationship;
(f) determining whether the customer is acting on their own behalf;
(g) ongoing monitoring of the business relationship, including scrutiny of specific products, services or 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 potential risk profile and ensuring that the customer's documentation, data and other information available to the obliged entity are kept up to date.

(4) Where financial institutions were obliged to perform basic customer due diligence when concluding an insurance policy or where the payout is at least EUR 1,000, the verification of identity of the beneficiary of the insurance policy shall be completed not later than when the beneficiary claims their rights arising from the life insurance policy or during the payout of the insurance benefits. If the identity of the beneficiary of a life insurance policy has already been verified, the financial institution does not need to verify this person's identity again during the payout of the insurance benefits. Under Article 10(6) of the Act, financial institutions shall verify, depending on the level of ML/TF risk, the validity and completeness of identification data and information submitted also during a business relationship and record any changes.

(5) Financial institutions shall perform the identification and verification of the beneficial owner's identity in accordance with Articles 6a, 7, 8 and 10 of the Act.

(6) Under Article 10(1)(b) of the Act, financial institutions shall identify the beneficial owner and adopt appropriate measures to verify their identity, including measures for determining the

ownership and management structures of the customer who is a legal person or a trust; when identifying the beneficial owner, obliged entities shall not rely exclusively on data from a register of legal persons, entrepreneurs and public sector entities. If any reasonable doubt arises about the correctness or completeness of the information on the beneficial owner obtained, financial institutions shall repeat basic customer due diligence under Article 10(2)(d) of the Act.

(7) The importance of Article 10(1)(a) to (c) and Article 10(7) of the Act is highlighted in the provisions of Article 15 and Article 24(2) of the Act which impose on financial institutions the obligation to reject a new customer, terminate an existing business relationship with a customer, or refuse to execute a specific transaction where it is impossible to perform basic customer due diligence or where the customer refuses 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 policy in which customer anonymity would be maintained is also set out in Article 78(6) of the Insurance Act. Under Article 17(1) of the Act, financial institutions shall report such cases to the FIU without undue delay.

(8) When establishing a business relationship, financial institutions shall perform basic customer due diligence and assign the customer into a risk category based on the set risk factors. In assigning the customer into a risk category, financial institutions shall take into account the information on risk factors stated in Annex 1 hereto, while duly applying the KYC principle, i.e., obtaining sufficient information on the nature of the expected products or services of the customer and any foreseeable scheme of transactions to be performed by the customer.

(9) Financial institutions shall continuously update the customer's risk profile according to the risk category to which the customer has been assigned; for this purpose, they shall require the customer to update the information they originally provided, and this in appropriate time intervals and depending on changes concerning the customer's person, or their commercial and other activities with which the customer's transactions performed by the financial institution are connected. The information may also be updated by requesting the customer to fill out the corresponding form at least once per calendar year.

(10) Categorisation of customers according to their risk profile allows financial institutions to apply in practice the provisions of Article 10(1)(g) of the Act, i.e. ongoing monitoring of the business relationship which leads to identification and subsequent reporting of UTs. In connection with risk categorisation of customers, it is necessary that financial institutions consider also Article 10(1)(g) and Article 10(6) of the Act, which establish the obligation to continuously update the customer's risk profile on the basis of a permanent monitoring of the business relationship. The appropriate update frequency depends on the financial institution's assessment and decision; in any case, this obligation shall be included in the internal regulation governing the Programme.

(11) When applying customer due diligence measures, Article 13 of the Act allows the use of customer due diligence already performed by another credit or financial institution, the so-called performance by third parties; this does not apply to ongoing monitoring of a business relationship under Article 10(1)(g) of the Act. After meeting the requirements stated in Article 13, financial institutions may use the already performed identification and verification of the customer's or beneficial owner's identity, i.e. receive data and documentation under Article 10(1)(a) to (c) necessary to perform customer due diligence from a bank or financial institution under Article 5(1)(b), points 1 to 10, which operates in the territory of a Member State that obliges it to perform measures equivalent to those relating to customer due diligence under Articles 10, 11 and 12, and to archiving of data under Article 19 and in line with the requirements of EU law, and which is subject to supervision at levels corresponding to EU law. Responsibility for the information thus acquired meeting the requirements for performing customer due diligence in accordance with the provisions

of the Act nonetheless remains with the financial institution that decided to rely on the 'third-party performance' approach.

(12) Financial institutions shall perform simplified customer due diligence in the scope and under the conditions set out in Article 11 of the Act. After considering the risk-based procedure, financial institutions may perform simplified customer due diligence in such situations and with respect to such customers where it is possible to obtain relevant basic information from publicly available and reliable sources and where this information justifies the application of simplified customer due diligence measures. A more detailed procedure for applying simplified customer due diligence measures is set out in Annex 1 hereto.

(13) The application of simplified customer due diligence measures does not exempt financial institutions from the obligation to conduct ongoing monitoring of business relationships pursuant to Article 10(1)(g) of the Act or other obligations laid down in Articles 14, 17, 19 and 21 of the Act.

(14) Financial institutions shall perform enhanced customer due diligence in the scope and under the conditions set out in Article 12 of the Act. A more detailed procedure for applying enhanced customer due diligence measures is set out in Annex 1 hereto.

(15) Financial institutions shall perform enhanced customer due diligence in particular with respect to products, services or transactions that, given their nature, pose a higher ML/TF risk and to customers who pose a higher ML/TF risk.

Article 9
Detecting, reporting and delaying of UTs

(1) The identification of UTs by financial institutions is governed by 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, financial institutions are required to assess whether an intended or ongoing transaction is unusual. Under Article 20(1) and (2)(d) of the Act, financial institutions must regulate this part of the procedures in its Programme. Obligations stated in Article 14(1) and (2)(a) and (b) of the Act shall be fulfilled demonstrably so that financial institutions can, in accordance with Article 30(3), provide information and written documents on the fulfilment of these obligations in case of an inspection. Article 14(3) of the Act also emphasises the obligation to draw up records on products, services and transactions under Article 14(2)(a) of the Act (the so-called internal notifications of potential UTs which contain information justifying the results of as assessment of the transaction); these records shall be archived in accordance with Article 30(3) of the Act for a period of five years.

(2) Under Article 4 of the Act, a UT is a legal or other act indicating that its execution may lead to ML/TF. Article 4(2) of the Act gives a non-exhaustive typology of UTs. Each of the UTs listed in this provision bears several indicators of unusualness (e.g. an unusually high volume of funds given the type of transaction, an unusually high volume of funds without clear economic or legal purpose, etc.) that financial institutions are required to assess and concurrently apply the KYC principle (while the Act does not define any KYC principles, if an obliged entity applies them in practice, that is how they should be defined in the Programme). Only by so doing can financial institutions competently assess whether a customer's intended or ongoing transaction is unusual or not. Article 4 of the Act does not stipulate any criteria – e.g. threshold amounts for funds – that would lead to an automatic finding that a certain type of financial operation undoubtedly constitutes a UT. The decisive element for assessing customer transactions is the application of the KYC principle and proper recognition of indicators of unusualness, as well as other signs or criteria that financial institutions are required to determine for themselves, depending on the subject of its activity, when drawing up an overview of the types of UTs (Article 20(2)(a) of the Act).

(3) The conditions for a proper application of the KYC principle derive from the obligations of financial institutions and customers, 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 Article 10(1) and Article 11(3) of the Act enables financial institutions to satisfy themselves about the real identity of each customer and identify the purpose and intended nature of business activities that the customer will probably conduct. This procedure is also the starting point for financial institutions in creating risk profiles for their customers, determining the appropriate level of customer due diligence under Article 10(4) of the Act, and accepting the customers. Depending on the results, financial institutions shall apply measures of basic customer due diligence under Article 10 of the Act, 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 financial institutions proceed under Article 10, 11 or 12 of the Act, they shall also always proceed in accordance with Article 14 of the Act. Financial institutions shall assess whether an intended or ongoing transaction is unusual (Article 14(1) of the Act) and pay particular attention to all complex, unusually large transactions and all transactions of an unusual nature that do not have a clear economic or legal purpose; all such transactions must be appropriately recorded in accordance with Article 14(3) of the Act (the so-called internal notification of UTs) and these records shall be archived for the period set out in Article 19 of the Act.

(5) Financial institutions shall carry out a qualified 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) at the front office, where the financial institution's staff members are in contact with existing or potential customers;
(b) as part of ongoing monitoring of existing business relationships;
(c) during follow-up (retrospective) assessment of customers products, services and transactions.

(a) Assessment of transactions at first contact with customers before and during the execution of a transaction

The assessment of customer transactions is performed by employees of the financial institution who, in fulfilling their duties, are in contact with the customers. The assessment of a transaction by an employee of the financial institution is, thus, performed largely at the place where the transaction is executed and before its execution or during the attempt to execute it, so that a potential UT can be identified, delayed and reported without delay. The assessment of transactions is dependent on the staff members' expertise and knowledge which they have acquired during mandatory training (Article 20 (3) of the Act).

Each relevant staff member shall have permanent access to the Programme, be it in written or electronic form, is required to be familiar with it and adhere to it. At this stage, employees of financial institutions shall primarily follow Article 10(1) and Article 11(3) of the Act in order to be able to adequately satisfy themselves about the real identity of the customer and to know the purpose and planned nature of business activities that the customer will probably perform. This procedure is also the starting point for financial institutions in accepting a customer, creating their risk profile and determining the appropriate level of customer due diligence under Article 10(4) of the Act.

A crucial element of assessing a customer's transactions is the appropriate application of the KYC principle and the related procedures, as well as a qualified evaluation of signs of unusualness. This procedure enables employees to assess the customer's intended or ongoing transactions by comparing them against an overview of types of UTs (Article 20(2)(a) of the Act), as well as against forms stated in Article 4(2) of the Act, and to detect those that are unusual with regards to the customers and their otherwise usual transactions.

If an employee assesses an intended or ongoing transaction as unusual, they shall make a written record of this transaction in accordance with Article 14(3) of the Act and promptly notify the NO (hereinafter 'notification of a UT').

(b) Assessment of transactions as part of ongoing monitoring of a business relationship

Relevant employees of financial institutions assess customer transactions also as part of ongoing monitoring of the business relationship. The assessment of intended or ongoing transactions as part of ongoing monitoring of the business relationship is specific in that the business relationship has already been established and still continues (Article 10(2)(a) of the Act). Also, financial institutions may already know the customer, provided that they have already executed several occasional transactions (Article 10(2)(b) or (c) of the Act). Hence, as this is not the first contact with the customer, financial institutions may take account of the customer's existing risk profile and their transaction history.

The procedure under Article 10(1)(g) of the Act, including the verification of the completeness and validity of identification data and information under Article 10(6) of the Act and the customer's obligation under Article 10(5) of the Act form the basis for ongoing monitoring of the business relationship. This type of monitoring requires customer risk profiles to be created and customers to be categorised with regard to the possible ML/TF risk under Article 10(4) of the Act. In creating customer risk profiles, financial institutions make use of the overview of risk factors as set out in Annex 1 hereto.

Ongoing monitoring of the business relationship requires financial institutions to use an appropriate EIS that would enable them, in line with the risk-based approach, to create financial or other criteria or limits as indicators of unusualness in customer 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 the customers. The criteria or limits defined by financial institutions for this purpose shall be regularly reviewed so that it is possible to determine their adequacy in regard to the identified levels of risk. Financial institutions shall also regularly review the adequacy of the existing system and individual processes of protection and prevention.

With regard to the assessment of transactions within the ongoing monitoring of business relationships, importance shall be given to those intended or ongoing customer transactions that do not correspond to the customer's known or expected activity or that correspond to the types of UTs referred to in the Programme or in Article 4(2) of the Act. Such customer transactions form subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record of them containing the rationale behind the results of the assessment (Article 14(3) of the Act); these records shall be archived for the period set out in Article 19 of the Act.

The NO may, based on the results of the assessment of the various circumstances of a transaction and with regard to the overview of types of UTs (Article 20(2)(a) and Article 4(2) of the Act), reach the conclusion that in the given case it does not constitute a UT. Where the conclusion cannot be reached solely on the basis of information on the customer already available to the financial institution, it may, based on the circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the Act.

In cases where the NO is unable, even by applying this procedure, to justify customer 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 ML/TF; the NO shall then proceed in accordance with Article 17 of the Act and report the UT to the FIU.

Depending on the transaction, the assessment of transactions in the framework of ongoing monitoring of the business relationship is performed by staff and/or by the NO.

(c) Assessment of transactions during follow-up (retrospective) assessment of customer transactions

A means of subsequent monitoring of customer 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 NO and the internal audit unit.

(6) The recommended procedure for processing and handling internal notifications of UTs and UT reports is as follows:
(a) all internal notifications of UTs sent by the relevant staff to the NO must be documented in line with Article 14(3) of the Act and must be available for the purposes of inspection under Article 29 of the Act;
(b) the sending of internal notifications and reports to the NO must not be subject to prior consent of any person;
(c) the NO shall register and archive internal notifications of UTs, including the position, full 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 NO, as well as the staff of the financial institution, including its managers (and members of the statutory body) involved in the assessment of transactions under Article 14 of the Act are required to maintain confidentiality on reported UTs and on measures taken by the FIU (Article 18 of the Act), including the fulfilment of obligations under Article 17(5) and Article 21 of the Act; financial institutions may not, however, cite toward Národná banka Slovenska and the Ministry of Finance of the Slovak Republic the obligation 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 the information provided is used exclusively for AML/CFT purposes, the obligation to maintain confidentiality does 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) financial institutions shall draw up a procedure covering the period from the moment of detecting a UT until its prompt reporting, including the corresponding procedure and responsibility of employees who assess the transaction;
f) the NO, after receiving an internal notification of UT, can confirm the receipt of the notification to the employee who sent the notification. The confirmation should contain the information on the obligation to maintain confidentiality under Article 18 of the Act. Where financial institutions collect internal notifications by means of an electronic system that enables the competent employee to monitor the status or receipt of submitted internal notifications of UT by the NO or by the Prevention Unit, no individual confirmation of receipt of such notification is necessary;
(g) the internal notification of UT, including the conduct of the customer or the transaction specified in the notification, shall be subjected to an assessment by the NO, who may, on the basis of results from further assessment of various circumstances of the transaction, with regard to the overview of types of UTs (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 a UT. This internal notification shall contain information on the transaction's economic or lawful purpose and, where the transaction is considered usual, also sufficient reasoning, information or justification regarding its usualness. Otherwise, such assessment process cannot be considered trustworthy and objective. If the decision cannot be reached solely on the basis of information on the customer already available to the financial institution, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the Act. Where the NO reaches a justified conclusion that an internally notified UT is not unusual after all, they shall make a written record of this decision and archive all related information, as well as written and electronic documentation for the period laid down in Article 19 of the Act;
(h) where the NO in unable, even by applying this procedure, to reach a conclusion that this transaction does not constitute a UT, it is sufficient that the transaction indicates that its execution may constitute ML/TF; the NO shall proceed in accordance with Article 17 of the Act and report the UT to the FIU, stating the reason for classifying this transaction as unusual.

Under Article 17(1) of the Act, UTs or attempts to execute unusual transactions must be reported to the FIU without undue delay. It is always necessary to take into consideration the particular circumstances of the situation in which the finding of the UT is made; financial institutions are required to report UTs as soon as possible. The decision of the NO to report a UT must not be subject to prior consent or approval of any other person. The UT report shall contain data stated in Article 17(3) of the Act and may not contain data referred to in Article 17(4) of the Act. The reference number of each UT report should take the form: serial number/year/character code of the financial institution.

UTs may be reported in person, in writing, by email or by telephone (in which case, the UT shall also be reported in person, in writing or by email within three days). The specimen form for reporting UTs, issued by the FIU, is available on the FIU's website (https://www.minv.sk/?vzory-hlaseni-o-noo).

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

In connection with the reporting of UTs 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 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. It is the only way how to avoid security risks connected with the reporting of UTs by post, fax or email;

(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 ML/TF, and where it helps obliged entities to assess customer transactions more effectively, and alert other obliged entities to identified risks. An exchange of information shall not contain the full scope of the reported UT as a whole, but only specific information relating to the ML/TF risk. In accordance with the Act, information provided may be used exclusively for AML/CFT purposes.

(7) Recommended procedure for the delaying of UTs:

(a) under Article 16 of the Act, financial institutions shall delay UTs, i.e. particular transactions (Article 9(g) of the Act) that would otherwise be executed;

(b) under Article 16(1), financial institutions shall delay UTs until they are reported 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. transactions assessed in the framework of ex-post or retrospective assessment of customer transactions can no longer be delayed;

(c) under Article 16(2), financial institutions shall delay UTs in the following two cases:

1. financial institutions shall delay a UT at its own discretion if the execution of the transaction poses the risk of frustrating or substantially impeding the seizure of proceeds from crime or seizure of funds intended for financing of terrorism; in such case, financial institutions shall immediately inform the FIU of the delaying of the UT;
2. financial institutions shall delay a UT if the FIU requests them to do so in writing; the FIU's written request shall always state the reason for delaying the UT;

(d) financial institutions shall not delay UTs if they are unable to do so for operating or technical reasons (they shall immediately notify the FIU) or if the delaying of a UT could, according to a previous notice from the FIU, frustrate the processing of the UT;

(e) the period for delaying a transaction under Article 16 of the Act shall be no more than 120 hours; therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to law enforcement authorities, the financial institution is required to extend the period of delaying, though not more than by a further 72 hours.

Therefore, UTs may be delayed for a maximum of 192 hours. If during the period of delaying an operation financial institutions receive no instructions from the judge or prosecutor to seize funds pursuant to Article 95 or 96 of Act No 301/2005 the Code of Criminal Procedure, as amended (hereinafter 'the Code of Criminal Procedure'), they shall execute the delayed transaction upon the lapsing of the set period. Prior to the lapsing of the delay period, financial institutions may execute a transaction only when the FIU notifies them in writing that no further delaying is necessary with regard to the processing of the UT. Saturdays and bank holidays are not counted in the period of delaying a UT.

The period of delaying a transaction under Article 16 of the Act is deemed to begin at the moment when the customer expresses their intention (will) to use the funds in their account. Where financial institutions expect that their customer will express an intention to execute a UT (use funds) in the future, they are obliged to take such personnel, organisational and technical measures which would prevent its execution should the customer give such instruction and not frustrate any potential delay of the UT.

The beginning of the period of delaying a transaction under Article 16 of the Act may not be deemed the moment when the financial institution evaluated the already-executed transactions as unusual or learnt of the customer's executed operations.

(8) In connection with the reporting of UTs it is important that insurance undertakings:

a) assign their customers to relevant risk categories;
b) duly apply customer due diligence;
c) establish the source of funds entering the system as part of the transaction assessment;
d) do not limit the reporting of UTs to funds leaving the system (buy-in, termination of insurance policy) within the insurance sector;
e) include in the UT reports also information on customer due diligence already performed, including repeated customer due diligence under Article 10(2)(c) and (d) of the Act.

Article 10
Counter-terrorist financing measures

(1) Terrorism represents one of the most serious violations of values such as human dignity, freedom, equality, 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 the Member States and on which the European Union is founded. The Act prohibits financing of terrorism and requires financial institutions to pay attention to transactions that may be related to terrorist financing.

(2) The issue of terrorist financing is also addressed by the recommendations of the Financial Action Task Force (FATF). Further information and reports concerning terrorist financing are available on the FATF website:
(http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html).

(3) Act No 289/2016 on the implementation of international sanctions (and amending Act No 566/2001 on securities and investment services (and amending certain laws) (the Securities Act), as amended)) (hereinafter 'the International Sanctions Act) defines an international sanction as a restriction, instruction or prohibition issued for the purpose of ensuring, maintaining or restoring international peace and security, protecting fundamental human rights, combating terrorism and proliferation, and accomplishing the objectives of the EU's Common Foreign and Security Policy and those of the United Nations Charter. The aim of sanctions is to ensure, maintain or restore international peace and security, combat terrorism and proliferation according to the principles of the UN Charter and the EU's Common Foreign and Security Policy.

(4) Procedure to be used in fulfilling the reporting obligation:
(a) financial institutions shall, within the CFT framework, apply toward their customers procedures analogous to those applied in the AML field, including the reporting of UTs connected with terrorist financing to the FIU;
(b) financial institutions shall report UTs to the FIU without undue delay (Article 17(1) of the Act); the Act defines a UT as, inter alia, a product, service or transaction in which there is a justified assumption that the customer or beneficial owner is a person against whom international sanctions have been imposed, or a person with links to that person, or as a product, service or transaction in which there is a reasonable belief 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 applied under the International Sanctions Act;
(c) financial institutions shall, under Article 91(8) of the Banking Act, provide the Ministry of Finance of the Slovak Republic, within the time limits set by it, with a list of customer who are subject to international sanctions under the International Sanctions Act and the relevant decrees; the list shall also contain account numbers and account balances of these customers (hereinafter 'sanctioned persons').

(5) A sanctioned person is a natural or legal person to which international sanctions apply, including:
(a) a state against which an international sanction has been imposed;
(b) a citizen of a state against which an international sanction has been imposed;
(c) a member or representative of a person against which an international sanction has been imposed;
(d) other natural person staying in the territory against which an international sanction has been imposed, except for a citizen of the Slovak Republic;
(e) a legal person with registered office in the territory against which an international sanction has been imposed; or
(f) a person included in the lists of sanctioned persons issued by Sanctions Committees of the United Nations Security Council, or a person stated in decisions taken in accordance with Title V of the Treaty of the European Union and in other EU legal acts.

(6) A list of sanctioned persons is a list of natural and legal persons against which international sanctions have been imposed in regulations on international sanctions published in the Official Journal of the European Union or in the Collection of Laws of the Slovak Republic. Lists of sanctioned persons form 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 sanctioned persons from states listed in the annexes to the individual regulations and decisions of the EU.

The regulations and decisions of the EU concerning exclusively sanctioned persons and comprehensive restrictive measures, including the consolidated list which contains the names and identification data of all persons, groups and entities that are 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 (https://eeas.europa.eu/topics/sanctions-policy_en).

In this regard, the EU sanctions are listed on the website of the Ministry of Foreign Affairs of the Slovak Republic (https://www.mzv.sk/zahranicna-politika/medzinarodne-sankcie, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).

A consolidated list of sanctions is published on the UN website (https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list).

(7) The inclusion of a person in the list of sanctioned persons, the removal of a person from that list, and the rights and obligations of sanctioned persons in the conditions of the Slovak Republic are regulated by the provisions of Articles 16 to 18 of the International Sanctions Act.

(8) Financial institutions shall act in accordance with the procedures for efficient implementation in practice of the rules of financial assets freezing of sanctioned persons in Slovakia, which are published on the website of the Ministry of Finance of the Slovak Republic (https://www.finance.gov.sk/sk/financie/financny-trh/bankovnictvo/sankcie-eu/).

Article 11
Archiving of data and documentation

(1) Financial institutions are entitled, for the purposes of performing customer due diligence (Articles 10, 11, 12 and 14 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 the provisions of Article 10(1) and Article 12 of the Act.

(2) Financial institutions are entitled to acquire the necessary personal data also by copying, scanning or other means of recording 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 aforementioned provisions of the Act.

(3) Financial institutions shall store (archive) information on the identification and verification of the customer's identity, records on the customer's products, services and transactions, and records on the identification of beneficial owners, including photocopies of relevant documents.

(4) Under the provisions of Article 19(1) and (2) of the Act, financial institutions shall archive for the period of five years:
(a) from the date of terminating contractual relationship with the customer information and written documents acquired by means of applying the procedure laid down by the provisions of Articles 10, 11, 12 and 14 of the Act;
(b) from the date of execution of a transaction all information and written documents on the customer.

Financial institutions shall archive such data and written documents also for longer than five years if the FIU requests it do so by way of a written request specifying the relevant period, which must not exceed another five years, and the scope of data and written documents to be archived. This obligations also applies to financial institutions that ceases business, up until the expiry of the period during which it is required to archive these data and written documents.

(5) The procedure followed by a financial institution for archiving data and documentation, and records relating to AML/CFT activities shall be governed by the financial institution's Programme, which should, in accordance with the Act, set out in detail:
(a) 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 the identification of the beneficial owner);
(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 the customers' risk rating

Documents and information concerning the customer's assignment to risk categories must be stored. Financial institutions shall record and store any important information confirming

circumstances justifying a customer's reassignment to a different risk category (and therefore a change of their risk profile) together with other information on the customer.

2. records on transactions

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

3. records on internal notifications of UTs and UT reports

Financial institutions shall archive all reports on customers' suspicious activities, namely internal notifications of UTs intended for the NO, as well as UT reports sent by the NO to the FIU.

If the NO, after assessing relevant information and knowledge concerning the customer's suspicious activity, decides that the activity does not constitute a UT 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 staff training conducted

Financial institutions shall store records on staff training, containing the date and content of the training, and a confirmation that relevant employees attended the training and were familiarised with the financial institution's AML/CFT Programme and related internal regulations of the financial institution.

5. the Programme

Financial institutions shall archive their Programmes, which shall contain information on statutory provisions, staff responsibilities, and mainly on any operational procedures and duties of the staff at the financial institution in the execution of relevant types of customers' products, services or transactions, including the most common types of UTs at the given financial institution.

6. records on inspections carried out

Financial institutions shall archive records on inspections carried out in accordance with Article 11.

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

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

Financial institutions shall continue to archive such information and documents on customers and their transactions also after the lapsing of the statutory archiving period or period laid down in the Insurance Act in cases where an investigation has been started by the competent law enforcement authorities, or a criminal prosecution has begun, for the purposes of investigation and criminal prosecution, on the basis of a written request of the FIU pursuant to Article 19(3) of the Act; the scope and the additional period required must be stated in the request.

(7) The records prepared and archived by financial institutions shall satisfy statutory requirements for record keeping with respect to 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 localisation of each customer;

(d) identification of all internal notifications of UTs and external UT reports;

(e) compliance, within a reasonable time, with statutory requirements of the FIU, supervisory authority and law enforcement authorities concerning a customer and a transaction.

Article 12
Securing the control system and ensuring the performance of internal control

Financial institutions shall have in place a reliably functioning control system focused on, inter alia, the implementation of AML/CFT measures.

(1) The control system shall comprise a specification of control responsibilities at all levels of management, as well as the performance of internal control by:
(a) the insurance undertaking's supervisory board;
(b) members of the insurance undertaking's statutory body;
(c) the Nominated Officer (their deputy and the Prevention Unit);
(d) managers;
(e) the staff involved in the processing of customer transactions;
(f) the staff coming into contact with customers in executing transactions.

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

Control is based on legislation of general application and the financial institution's internal regulations, and derives from the position in the hierarchy of the financial institution's management system. The statutory body of an insurance undertaking 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 of the NO and that of managers

Control activity shall be based on powers, duties and responsibilities of the NO and those of all managers 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 AML/CFT field.

(e) and (f) Control performed by the staff

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 the staff's work procedures, as well as their work duties, tasks and responsibilities as front office staff arising from the AML/CFT policy.

Article 13
Internal audit

(1) The internal audit unit assesses the adequacy and efficiency of the internal control system from the AML/CFT perspective, compliance with the Programme and internal regulations, and the performance of duties by employees of individual units, the Prevention Unit and managers, including the NO and their deputy.

(2) The internal audit unit's primary areas of focus:
1. performance of the relevant degrees (levels) of customer due diligence;
2. procedures for ensuring that the customer information obtained is up-to-date (verification);
3. assessment of specific transactions, monitoring of customers and business relationships;
4. risk management;

5. internal notification of UTs and reporting of UTs to the FIU;
6. conduct of staff training; and
7. record-keeping.

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

(4) The internal audit should be performed in compliance with the work programme of the internal audit unit at frequency determined by an evaluation of the degree of risk inherent to individual areas of financial institution's activity, at least once per calendar year. Members of the statutory body of the insurance undertaking and heads of branches should be regularly informed about the results of the audits performed.

Article 14
Final provisions

This Methodological Guideline replaces in full 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.

Vladimír Dvořáček
Member of the Bank Board
and Executive Director of
the Prudential Supervision Division
of the Financial Market Supervision Unit
of Národná banka Slovenska

Júlia Čillíková
Executive Director of the
Financial Consumer Protection and
Regulation Division
of the Financial Market Supervision Unit
of Národná banka Slovenska

ANNEX 1

Guidelines on risk factors relating to customer relationships and occasional transactions

This annex is based on Annex 2 to the Act and provides more detailed guidance on risk factors financial institutions should consider when performing customer due diligence for AML/CFT purposes.

These guidelines have been prepared in accordance with Joint Guidelines under articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (JC 2017 13) (hereinafter the 'joint guidelines').

In relation to risk factors, financial institutions should also adjust the extent of their customer due diligence measures in a way that is commensurate to the identified money laundering and terrorist financing risks.

The joint guidelines are available also in Slovak: https://esas-jointcommittee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SK_04-01-2018.pdf

A) GENERAL GUIDELINES

Part 1
General guidelines on assessing and managing risk

'Risk factors' means variables that, either on their own or in combination, may increase or decrease the money laundering and terrorist financing (hereinafter 'ML/TF') risk posed by an individual business relationship or occasional transaction.

Financial institutions should perform a business-wide assessment of ML/TF risks to understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the mitigation of these risks. In line with Annex 2 to the Act and Article 8 of Directive (EU) 2015/849, financial institutions should identify and assess the ML/TF risks associated with their products and services, customers, and transactions and delivery channels used to service their customers. The steps taken by the financial institutions to identify and mitigate the ML/TF risks shall be proportionate to their nature and size.

Financial institutions should adjust the extent of initial obligatory customer due diligence measures on a risk-sensitive basis. Where the risk associated with a business relationship has been assessed as low, financial institutions shall apply simplified customer due diligence measures.

Where the risk associated with a business relationship has been assessed as higher, financial institutions shall apply enhanced customer due diligence measures.

Financial institutions should collect adequate information in order to establish that they identified and assessed all risk factors with the objective of conducting a comprehensive assessment of risks associated with a particular business relationship or occasional transaction.

When assessing and managing risks, financial institutions should always consider the following sources of information:
(a) the European Commission's supranational risk assessment (under Article 6 of Directive (EU) 2015/849);
(b) information from the national risk assessment (under Article 7 of Directive (EU) 2015/849), policy statements, alerts and explanatory memorandums to relevant legislation;
(c) information from regulators, such as guidance, statements, etc.;
(d) information from the FIU, such as threat reports, alerts and typologies;
(e) information obtained as part of the customer due diligence process.

In addition to the sources mentioned above, financial institutions should consider, among others, the following sources of information:
(a) own knowledge and expertise acquired during the provision of services to their customers;
(b) information from industry bodies, such as typologies and information on emerging risks;
(c) information from civil society, such as corruption indices, country reports, etc.;
(d) information from international standard-setting bodies in the field of AML/CFT (FATF, MONEYVAL), such as reports on mutual evaluation of ML/TF risks;
(e) information from other credible and reliable open sources, such as media, the Internet, etc.;
(f) information from statistical organisations and academia.

Part 2
Risk assessment

A risk assessment conducted by a financial institution should consist of two distinct but related steps:
2.1. the identification of ML/TF risks;
2.2. the assessment of ML/TF risks.

2.1. Identification of ML/TF risks

When identifying ML/TF risks associated with a business relationship or occasional transactions, financial institutions should consider relevant risk factors related to:
(a) their customers;
(b) products, services and transactions requested by their customers;
(c) the countries or geographical areas their customers operate in;
(d) the delivery channels used by the financial institutions to deliver products, services and transactions.

Information about these ML/TF risk factors should come from a variety of sources. Financial institutions should determine the number of these sources on a risk-sensitive basis.

2.1.1. Customer risk factors

When identifying the risks associated with their customers, including their customer's beneficial owners, financial institutions should consider the risks related to:

a) the customer's and the customer's beneficial owner's business or professional activity;
Risk factors that may be relevant when considering the customer's business or professional activity include:
(a) Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk (such as construction, healthcare, the arms trade and defence, the extractive industries, public procurement, etc.)?
(b) Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk (such as casinos, gambling venues or dealers in precious metals)?
(c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
(d) Does the customer have political connections (for example, are they a politically exposed person or is their beneficial owner a politically exposed person, do they have any links to a politically exposed person)?
(e) Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain (for example, are they members of local or regional decision-making bodies with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers)?
(f) Based on publicly available sources, is there evidence that the customer has been subject to sanctions for failure to comply with AML/CFT obligations?

b) the customer's and the customer's beneficial owner's good repute;
When considering the risks associated with the customer's good repute, financial institutions should consider the following factors:
(a) Are there adverse media reports or other relevant sources of information about the customer (for example, are there any allegations of criminality or terrorism against the customer)?
(b) Has the customer, beneficial owner or anyone known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?
(c) Does the financial institution know if the customer or beneficial owner has been the subject of an unusual transactions report in the past?

c) the customer's and the customer's beneficial owner's nature and behaviour;
When considering the behaviour of their customers, financial institutions should note that not all of the risk factors below will be apparent at the outset of a business relationship and that they may emerge only once a business relationship has been established:
(a) Is the customer's ownership and control structure transparent and does it make sense? If not, is there an obvious lawful or economic rationale to this?

(b) Is there a sound reason for changes in the customer's ownership and control structure (such as sale or transfer of the company or a part thereof to other beneficial owners, etc.)?
(c) Does the customer request transactions that are complex, unusually large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale (for example, is the customer trying to evade specific thresholds set out for occasional transactions)?
(d) Does the customer request unnecessary or unreasonable levels of secrecy? Is the customer reluctant to share customer due diligence information, or does the customer appear to want to disguise the true nature of their business (for example when the customer requests private banking services)?
(e) Does the customer issue bearer shares as part of their business activity?
(f) Is the customer able to plausibly explain the source of their wealth or the source of funds (for example through their occupation, business activity, inheritance, donation or investments)?
(g) Does the customer use the products and services they have taken out when the business relationship was first established as expected and in line with the information obtained by the financial institution regarding the purpose and intended nature of the relationship?
(h) Are there indications that the customer might seek to avoid the establishment of a business relationship (for example by requesting only one transaction or several one-off transactions even where the establishment of a business relationship might make more economic sense)?

2.1.2. Products, services and transactions risk factors

When identifying the risks associated with their products, services or transactions, financial institutions should consider the risks related to the level of transparency the product, service or transaction affords, as well as the overall complexity, value or size of the product, service or transaction.

a) risks related to the level of transparency the product, service or transaction affords:
The products, services and transactions allow the customer or beneficial owner to remain anonymous, or facilitate hiding their identity (such as bearer shares or activities of legal persons that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies).

b) risks related to the complexity of the product, service or transaction:
Third party that is not part of the business relationship is able to give instructions for the execution of a transaction, product or service (for example in the case of certain correspondent banking relationships).
The transaction is complex and involves multiple parties or multiple jurisdictions (for example in the case of certain trade finance transactions). There are risks associated with financial institution's new products or services, in particular where this involves the use of new technologies (such as remote identification and verification of the customer without the customer being physically present).

c) risks related to the value or size of the product or service:
The products or services are cash intensive (such as payment services), they facilitate high-value transactions and/or there are no caps on cross-border and cash/cashless transactions.

2.1.3. Customer's geographical area risk factors

When identifying risk associated with countries and geographical areas, financial institutions should consider the risks related to countries in which the customer or beneficial owner are based, which are their main places of business, and to which they have relevant personal links.

When identifying the geographical risk factors, financial institutions should also consider the overall effectiveness of a country's AML/CFT regime. This includes the following risk factors:

The country has been identified by the European Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of Directive (EU) 2015/849. Where financial institutions deal with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, they must always apply enhanced customer due diligence measures.

There is information from a credible and reliable source about the quality of the country's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and financial sector oversight. Examples of possible sources include the FATF mutual evaluation reports, the FATF's list of high-risk and non-cooperative countries, International Monetary Fund (IMF) assessments, etc. When assessing the risks, financial institutions should note that the country's membership in the FATF or FSRB (e.g. MoneyVal) does not, of itself, mean that the country's AML/CFT regime is adequate and effective.

There is information from credible and reliable public sources about the level of predicate offences to money laundering, for example corruption, organised crime, tax crime, etc. Examples include corruption perceptions indices, OECD country reports on the implementation of the OECD's anti-bribery convention, and the United Nations Office on Drugs and Crime World Drug Report.

There is information suggesting that the country provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country.

The country is subject to financial sanctions or embargoes that are related to terrorism, financing of terrorism or proliferation issued by the United Nations or the European Union.

2.1.4. Delivery channel risk factors

When identifying the risks associated with the way in which the customer establishes business relationships, financial institutions should consider the following risk factors:

The customer is not physically present for identification and verification purposes. For this type of establishment of a business relationship, financial institutions should have a procedure in place for a reliable form of non-face-to-face obligatory customer due diligence.

The customer has been introduced by another institution of the same financial group. The financial institution should consider to what extent can it rely on this introduction as reassurance

that the customer will not expose the financial institution to excessive ML/TF risk? The financial institution should verify whether the other institution of the same financial group applies customer due diligence measures to EU standards in line with Article 21(4) and (5) of the Act.

The customer has been introduced by a third party, for example by a bank that is not part of the same group, and the third party is a financial institution (the financial institution should verify how does the third party apply customer due diligence measures, how does it keep records and whether it is supervised for compliance with comparable AML/CFT obligations).

The customer has been introduced through a tied agent, that is, without direct financial institution contact (the financial institution should verify whether the agent has obtained enough information so that the financial institution knows its customer and the level of risk associated with the business relationship).

The financial institution cooperates with an intermediary whose level of compliance with applicable AML/CFT legislation might be inadequate.

2.2. Assessment of ML/TF risks

Financial institutions should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship or occasional transactions. As part of this assessment, financial institutions may decide to weigh factors differently depending on their importance.

When weighting risk factors, financial institutions should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction.

When weighting risk factors, financial institutions should ensure that:
(a) weighting is not unduly influenced by just one factor identified;
(b) economic or profit considerations do not influence their risk rating;
(c) weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
(d) they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

During the assessment process, financial institutions should assign higher weight to material risk factors and lower weight to non-material risk factors.

Following their risk assessments, financial institutions should categorise their business relationships and occasional transactions according to the perceived level of ML/TF risk.

Financial institutions should decide on the most appropriate way to categorise risk. This will depend on the complexity and size of the financial institution and the types of ML/TF risk it is exposed to. Financial institutions are recommended to use the following three risk categories:

(a) High;
(b) Medium;

(c) Low.

Financial institutions may use a more detailed categorisation, for example by splitting the "Medium risk" category into "Medium low risk" and "Medium high risk".

Part 3
ML/TF risk management, simplified and enhanced customer due diligence, risk monitoring and review

Risk assessment should help financial institutions determine their risk management priorities in the AML/CFT field. Financial institutions should set their basic customer due diligence measures to a level that is appropriate considering the identified ML/TF risks.

3.1. Simplified customer due diligence

To the extent laid down by the Act, financial institutions may apply simplified customer due diligence measures in situations where the ML/TF risk associated with a business relationship has been assessed as low. Simplified customer due diligence is not an exemption from any of the customer due diligence measures. Financial institutions may adjust the amount, timing or type of each or all of the customer due diligence measures in a way that is commensurate to the low risk they have identified.

Simplified customer due diligence measures financial institutions may apply include:

3.1.1. adjusting the timing of customer due diligence, for example where the product, service or transaction sought has features that limit its use for ML/TF purposes, for example by:
1) verifying the customer's or beneficial owner's identity during the establishment of the business relationship;
2) verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed.

Financial institutions must make sure that:
(a) the situations in points 1 and 2 do not result in an exemption from customer due diligence, that is, financial institutions must ensure that the customer's or beneficial owner's identity will ultimately be verified;
(b) the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, financial institutions should note that a low threshold alone may not be enough to reduce risk);
(c) they have systems in place to detect when the threshold or time limit mentioned in point 2 has been reached;
(d) they do not defer customer due diligence or delay obtaining relevant information about the customer needed.

3.1.2. adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:

1) verifying identity on the basis of information obtained from one reliable, credible and independent document only; or
2) assuming the nature and purpose of the business relationship.

3.1.3. adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:
1) accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; or
2) where the risk associated with all aspects of the relationship is low, relying on the source of funds to meet some of the obligatory customer due diligence requirements (for example where the funds are state benefit payments).

3.1.4. adjusting the frequency of customer due diligence updates and reviews of the business relationship (for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached). If statutory thresholds are exceeded, financial institutions must perform basic customer due diligence.

3.1.5. adjusting the frequency and intensity of transaction monitoring (for example by monitoring transactions above a certain threshold only). Where financial institutions choose to do this, they must ensure that the threshold is set at a statutory level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

Financial institutions should ensure that the information they obtain when applying simplified customer due diligence measures are sufficient to justify the low risk. It must also be sufficient to give the financial institutions enough information about the nature of the business relationship to identify any unusual or suspicious transactions. Simplified customer due diligence does not exempt a financial institution from reporting unusual transactions to the FIU.

3.2. Enhanced customer due diligence

Financial institutions must apply enhanced customer due diligence in higher risk situations to manage and mitigate those risks appropriately. Enhanced customer due diligence measures cannot be substituted for regular customer due diligence measures but must be applied in addition to regular customer due diligence measures.

Under Article 12 of the Act, financial institutions are obliged to perform enhanced customer due diligence where risk assessment under Article 10(4) of the Act indicates that a customer, transaction type or individual transaction poses a higher ML/TF risk. Financial institutions must **always** perform enhanced customer due diligence:
3.2.1. where the customer is a politically exposed person;
3.2.2. with respect to cross-border correspondent relationship of a bank and financial institution with respondents from third countries;
3.2.3. where they deal with natural or legal persons established in countries that the European Commission has identified as presenting a high risk.

3.2.1. Enhanced due diligence with respect to politically exposed persons

Financial institutions that have identified that a customer or beneficial owner is a politically exposed person **must always**:

(a) Take adequate measures to establish the source of wealth and the source of funds in order to allow them to satisfy themselves that it does not handle the proceeds from criminal activity. The measures financial institutions should take to establish the politically exposed person's source of wealth and the source of funds will depend on the degree of risk associated with the business relationship. Financial institutions should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information.

(b) Obtain approval of the statutory body or Nominated Officer under Article 20(2)(h) of the Act for establishing, or continuing, a business relationship with a politically exposed person. The appropriate level of seniority for sign-off should be determined by the level of increased risk associated with the business relationship, and the senior manager approving a business relationship with a politically exposed person should have sufficient seniority and oversight to take informed decisions on issues that directly impact the financial institution's risk profile. When considering whether to approve a relationship with a politically exposed person, statutory body or the Nominated Officer should base their decision on the level of ML/TF risk the financial institution would be exposed to if it entered into that business relationship. The financial institution should also consider how well equipped it is to manage and mitigate that risk effectively.

(c) Apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship. Financial institutions should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of risk associated with the relationship.

Financial institutions must apply all of these measures to politically exposed persons, their family members and known close associates. They should adjust the extent of these measures on a risk-sensitive basis. Financial institutions should apply these measures for a period of at least 12 months after the termination of the term of significant public office that the politically exposed person held, at minimum, however, until the financial institution does not rule out the risk specific for politically exposed persons.

3.2.2. Enhanced customer due diligence with respect to correspondent relationships

Financial institutions must take specific enhanced customer due diligence measures where they have a cross-border correspondent relationship with a respondent who is based in a third country.

Financial institutions must make sure that they:
(a) collect information on the partner institution in order to determine the nature of their business and their good repute and to ascertain the level of effectiveness of supervision using information from public sources;
(b) assess the partner institution's AML/CFT controls;
(c) obtain approval of the statutory body or Nominated Officer under Article 20(2)(h) of the AML Act for establishing a new correspondent relationship;
(d) verify that the partner institution is authorised to perform its business activities;

(e) establish, in the case of account-based payments, whether the partner institution verified the identity of the customer who has direct access to the partner institution's account and performed basic customer due diligence, and whether the partner institution is able, if requested, to provide the information in the extent of basic customer due diligence.

3.2.3. Enhanced customer due diligence with respect to high-risk third countries and high-risk situations

High-risk third countries:

When dealing with customers established or residing in a high-risk third country identified by the Commission in Commission Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, and in all other high-risk situations, financial institutions should take an informed decision about which enhanced customer due diligence measures are appropriate for each high-risk situation.

Financial institutions are not required to apply all the enhanced customer due diligence measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring of the business relationship. During supervision, the obliged entity shall demonstrate that the extent of performed customer due diligence is commensurate with the identified level of ML/TF risk.

Complex and unusually large transactions:

Financial institutions should put in place adequate procedures to detect unusual transactions or patterns of transactions. Where a financial institution detects transactions that are unusual because:

(a) they are larger than what the financial institution would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
(b) they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers or deals; or
(c) they are very complex compared with other, similar, transactions associated with similar customer types, products or services, and the financial institution is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply enhanced customer due diligence measures.

These enhanced customer due diligence measures should be sufficient to help the financial institution determine whether these transactions give rise to suspicion of money laundering and must at least include:

(a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
(b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A financial institution may decide to monitor individual transactions where this is commensurate to the risk it has identified.

Enhanced customer due diligence measures should in particular include:

(a) **Increasing the quantity of information** obtained for customer due diligence purposes, for example:

1) identifying the customer using additional documents, obtaining information about the customer's ownership and control structure, obtaining information about the customer's family members and close business partners, and obtaining information about the customer's or beneficial owner's past and present business activities;

2) obtaining more detailed information about the purpose and intended nature of the business relationship with the customer, for example information about the number, size and frequency of transactions that are likely to pass through the payment account, and information about the nature of the customer's or beneficial owner's business, to enable the financial institution to better understand the nature of the business relationship;

(b) **Increasing the quality of information** obtained for customer due diligence purposes, for example:

1) requiring the first payment to be carried out through an account verifiably in the customer's name, where the customer presented a document proving the existence of such account;

2) establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the financial institution's knowledge of the customer and the nature of the business relationship;

(c) **Increasing the frequency of reviews** to be satisfied that the financial institution continues to be able to manage the risk associated with the individual business relationship, for example by:

1) increasing the frequency of regular reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable for the financial institution;

2) conducting more frequent and in-depth transaction monitoring to identify any unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions;

3) obtaining the approval of the statutory body or a senior manager or the Nominated Officer to establish or continue the business relationship to ensure that senior management are aware of the risk their financial institution may be exposed to.

Other considerations with respect to enhanced due diligence

Financial institutions should not enter into a business relationship if they are unable to comply with their customer due diligence requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage and mitigate the risk that they may be used for ML/TF purposes. Where such a business relationship already exists, financial institutions shall terminate it or suspend transactions of the customer until it can be terminated.

Financial institutions should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one risk category.

Where financial institutions have reasonable grounds to suspect that ML/TF is being attempted, they must report this to their FIU.

3.3. Risk monitoring and review

Financial institutions should keep their assessments of the ML/TF risks associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant.

Financial institutions should also ensure that they have systems (including a system to set a date on which the next risk assessment will take place) and controls in place to identify emerging ML/TF risks. They should also be able to assess these risks and incorporate them into their risk assessment. Any update to a risk assessment and adjustment of accompanying customer due diligence measures should be proportionate to the identified ML/TF risk.

Systems and controls to monitor and review risks that financial institutions should put in place include:

(a) processes to ensure that internal risk information is reviewed regularly to identify trends and emerging issues, in relation to both individual business relationships and the financial institution's business;

(b) processes to ensure that the financial institution regularly reviews information sources (such as the national risk assessment report, EU supranational risk assessment report, report of the Financial Intelligence Unit, other national regulators, own knowledge and analysis, etc.);

(c) processes to ensure careful recording of issues that could have a bearing on risk assessment (such as internal suspicious transaction reports, past compliance failures of employees and intelligence from front office staff).

Financial institutions should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews and monitoring, to ensure that they can demonstrate to the competent authorities that their risk assessments and associated measures to manage and mitigate risks are adequate.

B) SECTORAL GUIDELINES FOR THE FIELD OF LIFE INSURANCE – RISK FACTORS

Most life insurance products are designed for the long term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime.

Part 1
Risk factors associated with life insurance

1.1. Product, service and transaction risk factors

The following factors may contribute to increasing risk:
(a) flexibility of payments, for example if the product allows payments from unidentified third parties, high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments, or cash payments;
(b) ease of access to accumulated funds, for example if the product allows partial withdrawals or early surrender at any time, with limited charges or fees;
(c) negotiability, for example if the product can be traded on a secondary market or if the product can be used as collateral for a loan.

There are factors that may contribute to reducing risk, for example if the product:

(a) only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
(b) has no surrender value;
(c) has no investment element;
(d) has no third party payment facility;
(e) requires that total investment is curtailed at a low value;
(f) is a life insurance policy where the premium is low;
(g) only allows small-value regular premium payments, for example no overpayment;
(h) is accessible only through employers, for example a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
(i) cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option;
(j) cannot be used as collateral;
(k) does not allow cash withdrawals;
(l) has conditions that must be met to benefit from tax relief.

1.2. Customer and beneficiary risk factors

The following factors may contribute to increasing risk:

(a) the nature of the customer, for example:
- legal persons structure of which makes it difficult to identify the beneficial owner;
- the customer or the beneficial owner of the customer is a politically exposed person;
- the beneficiary of the policy or the beneficial owner of this beneficiary is a politically exposed person;
- the customer's age is unusual for the type of product sought (for example, the customer is very young or very old);
- the contract does not match the customer's wealth situation;
- the customer's profession or activities are regarded as particularly likely to be related to money laundering, for example because they are known to be very cash intensive or exposed to a high risk of corruption;
- the contract is subscribed by a 'gatekeeper', such as a fiduciary company, acting on behalf of the customer;

the policy holder and/or the beneficiary of the policy are companies with nominee shareholders and/or shares in bearer form;
(b) the customer's behaviour:

- *in relation to the contract*, for example the customer frequently transfers the contract to another insurer; frequent and unexplained surrenders, especially when the refund is done to different bank accounts; the customer makes frequent or unexpected use of 'free look' provisions; the customer incurs a high cost by seeking early termination of a product; the customer transfers the contract to an apparently unrelated third party; the customer requests to change or increase the sum insured and/or requests premium payment that are unusual or excessive;

- *in relation to the beneficiary of the policy*, for example the insurer is made aware of a change in beneficiary only when the claim is made; the customer changes the beneficiary clause and nominates an apparently unrelated third party; the insurer, the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner are in different jurisdictions;

- *in relation to payments*, for example the customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity; payments from different bank accounts without explanation; payments from banks that are not established in the customer's country of residence; the customer makes frequent or high-value overpayments where this was not expected; payments received from unrelated third parties; catch-up contribution to a retirement plan close to retirement date.

The following factors may contribute to reducing risk:

In the case of corporate-owned life insurance, the customer is:
(a) a credit or financial institution that is subject to requirements to combat money laundering and the financing of terrorism and supervised for compliance with these requirements in a manner that is consistent with Directive (EU) 2015/849;
(b) a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) that impose requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company;
(c) a public administration or a public enterprise from an EEA jurisdiction.

1.3. Delivery channel risk factors

The following factors may contribute to increasing risk:

(a) non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents that comply with Regulation (EU) No 910/2014;
(b) long chains of intermediaries;
(c) an insurance intermediary is used in unusual circumstances (such as unexplained geographical distance).

The following factors may contribute to reducing risk:

(a) insurance intermediaries are well known to the insurer, who is satisfied that the insurance intermediary applies CDD measures commensurate to the risk associated with the relationship and in line with those required under Directive (EU) 2015/849;
(b) the product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

1.4. Geographical risk factors

The following factors may contribute to increasing risk:

(a) the insurer, the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner are based in, or associated with, jurisdictions associated with higher ML/TF risk; companies should pay particular attention to jurisdictions without effective AML/CFT supervision;
(b) premiums are paid through accounts held with financial institutions established in jurisdictions associated with higher ML/TF risk; companies should pay particular attention to jurisdictions without effective AML/CFT supervision;
(c) the insurance intermediary is based in, or associated with, jurisdictions associated with higher ML/TF risk; companies should pay particular attention to jurisdictions without effective AML/CFT supervision.

The following factors may contribute to reducing risk:

(a) countries are identified by credible sources, such as mutual evaluations or detailed assessment reports, as having effective AML/CFT systems;
(b) countries are identified by credible sources as having a low level of corruption and other criminal activity.

Part 2
Measures in the field of life insurance

Financial institutions must apply customer due diligence measures not only to the customer and beneficial owner but also to the beneficiaries as soon as they are identified or designated. This means that financial institutions must:
(a) obtain the name of the beneficiary where either a natural or legal person or an arrangement is identified as the beneficiary; or
(b) obtain sufficient information to be satisfied that the identities of the beneficiaries can be established at the time of payout where the beneficiaries are a class of persons or designated by certain characteristics (for example, where the beneficiary is 'my future grandchildren', the insurer could obtain information about the policy holder's children).

Financial institutions must verify the beneficiaries' identities at the latest at the time of payout.

2.1. The following enhanced customer due diligence measures may be appropriate in a high-risk situation:

(a) Where the customer makes use of the 'free look' provisions/'cooling-off' period, the premium should be refunded to the customer's bank account from which the funds were paid. Companies

should ensure that they have verified the customer's identity in line with Article 13 of Directive (EU) 2015/849 before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Companies should also consider whether the cancellation gives rise to suspicion about the transaction and whether submitting a suspicious activity report would be appropriate.
(b) Additional steps may be taken to strengthen the company's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, the third party payers and payees. Examples include:
- not using the derogation in Article 14(2) of Directive (EU) 2015/849, which provides for an exemption from upfront customer due diligence;
- verifying the identity of other relevant parties, including third-party payers and payees, before the beginning of the business relationship;
- obtaining additional information to establish the intended nature of the business relationship;
- obtaining additional information on the customer and updating more regularly the identification data of the customer and beneficial owner;
- if the payer is different from the customer, establishing the reason why;
- verifying identities on the basis of more than one reliable and independent source;
- establishing the customer's source of wealth and source of funds, for example employment and salary details, inheritance or divorce settlements;
- where possible, identifying the beneficiary at the beginning of the business relationship, rather than waiting until they are identified or designated, bearing in mind that the beneficiary can change over the term of the policy;
- identifying and verifying the identity of the beneficiary's beneficial owner;
- in line with Articles 20 and 21 of Directive (EU) 2015/849, taking measures to determine whether the customer is a politically exposed person and taking reasonable measures to determine whether the beneficiary or the beneficiary's beneficial owner is a politically exposed person at the time of assignment, in whole or in part, of the policy or, at the latest, at the time of payout;
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to customer due diligence standards that are not less robust than those required under Directive (EU) 2015/849.

Article 20 of Directive (EU) 2015/849 requires that, where the risk associated with a relationship involving a politically exposed person is high, companies must not only apply customer due diligence measures in line with Article 13 of the Directive but also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and decide on the most appropriate measures to mitigate that risk. In addition, companies must conduct enhanced customer due diligence on the entire business relationship. More frequent and more in-depth monitoring of transactions may be required (including where necessary, establishing the source of funds).

2.2. The following simplified customer due diligence measures may be appropriate in a low-risk situation:

(a) Financial institutions may be able to assume that the verification of the identity of the customer is fulfilled on the basis of a payment drawn on an account that the company is satisfied is in the sole or joint name of the customer with an EEA-regulated credit institution.

(b) Financial institutions may be able to assume that the verification of the identity of the beneficiary of the contract is fulfilled on the basis of a payment made to an account in the beneficiary's name at an EEA-regulated credit institution.

ANNEX 2
(source: FIU)

General methods of recognising unusual transactions

1. A transaction which by virtue of its complexity, unusually high volume of funds or other characteristic 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 the customer requests to arrange a transaction or intermediate a contract, 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 uses is clearly not commensurate with the nature or scope of the customer's business activity or declared financial circumstances.
6. A transaction whose relation 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 customary in legitimate transactions.
10. A transaction in which the customer uses or tries to use false or stolen identification documents.

Specific methods of recognising unusual transactions in insurance activities

1. A refusal to state on whose behalf the insurance contract is concluded.
2. The customer asks for insurance of an item which bears signs of having been stolen.
3. The customer wants to enter into an insurance contract for such amount which seems to be disproportionate to the customer's insurance needs.
4. The customer accepts insurance conditions which are unfavourable and do not relate to the customer's health and/or age, and is ready to pay high premium which is obviously beyond their means.
5. Repetitive conclusion of (three or more) insurance contracts for unusually high amounts.
6. The customer changes authorised persons specified in the contract; these persons frequently do not have any obvious relations with the policyholder.
7. The customer, when concluding contract, is not interested in meeting the contract terms but rather in its early termination; the customer may seem to have insurance contracts concluded with more insurance companies.
8. The customer requires an extreme increase of the insured sum and premium.

9. The customer makes multiple changes to accounts used for the payment or repayment of premiums.
10. The customer concluded several life insurance contracts at the same time and for each of them the premium was paid in cash.
11. Very short time (less than 3 months) between the conclusion and cancellation of the contract where the premium is very high.
12. Concluding an insurance contract with an unusually high annual premium.
13. The customer pays very high insurance amounts in cash or by postal order.
14. The customer credits funds to the insurance company's account and subsequently announces to the company that they did so by mistake and requests to have the money returned to them, but to a different account or by postal order.
15. The customer makes a payment of approximately two instalments and then asks for a refund to another account.
16. After regular instalment payments, the customer suddenly makes a lump-sum payment of the full premium and/or transfers the funds from several banks, mainly from abroad.
17. For investment products, the customer makes three or more repetitive deposits by credit transfer to an account.