VÚB AML Guidelines

FOR THE FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING AND THE HANDLING OF THE EMBARGOES

VÚB Bank
Date: March, 1st 2019
CONTENTS

1. KEY TERMS DEFINITION / INTRODUCTION ................................................................................. 3
   1.1 Regulatory framework of prevention of money laundering and fight against terrorism financing ... 3
   1.2. Regulations on dealing with embargoes .................................................................................. 5
2. OBJECTIVES, DEFINITIONS AND PRINCIPLES ................................................................. 7
   2.1. Objectives .......................................................................................................................... 7
   2.2. Definitions ......................................................................................................................... 7
   2.3. General governance model principles ................................................................................. 8
3. ROLES AND RESPONSIBILITIES ......................................................................................... 8
   3.1. Supervisory Board ............................................................................................................. 9
   3.2. Management Board .......................................................................................................... 9
   3.3. Audit Committee ............................................................................................................. 10
   3.4. Anti-Money Laundering Department ................................................................................. 10
   3.5. AML Officer ..................................................................................................................... 11
   3.6. Legal Services Department ............................................................................................... 12
   3.7. Operations and IT Division ............................................................................................... 12
   3.8. Risk Management Division .............................................................................................. 12
   3.9. Human Resources & Organization Department ................................................................. 13
   3.10. Retail and Corporate Banking Divisions ......................................................................... 13
   3.11. Internal Audit and Control Department ........................................................................... 13
4. TOPICS COVERED IN MACRO PROCESSES FOR FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING .......................................................... 14
   4.1 Definition of the guidelines and methodological rules ..................................................... 14
   4.2 Risk Assessment and Risk Appetite Framework .............................................................. 14
   4.3 Regulatory alignment ....................................................................................................... 15
   4.4 Consultation and clearing ................................................................................................ 15
   4.5. Assurance ....................................................................................................................... 15
   4.5.1. Interactions with the other control functions and information flows ....................... 16
   4.6. Spreading the culture of anti-money laundering, combating terrorist financing and embargoes ......................................................................................................................... 16
   4.7. Interaction with the Supervisory Authorities and management of non-compliance events ......................................................................................................................... 17
   4.8 Customer awareness and profiling ................................................................................. 17
   In order to make sure a customer due diligence is performed, the following activities should be undertaken: ......................................................................................................................... 17
   4.9. Data retention .................................................................................................................. 17
   4.10. Transaction monitoring ................................................................................................. 17
   4.11. Reporting and information management across the Bank ......................................... 18
5. FINAL PROVISIONS ............................................................................................................. 18
1. KEY TERMS DEFINITION / INTRODUCTION

<table>
<thead>
<tr>
<th>Expression</th>
<th>Acronym</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AML</td>
<td></td>
<td>Anti Money Laundering means protecting the bank from legalizing the proceeds of crime (anti-money laundering and terrorist financing)</td>
</tr>
<tr>
<td>2. Bank</td>
<td></td>
<td>Všeobecná úverová banka, a.s.</td>
</tr>
<tr>
<td>3. FIU</td>
<td></td>
<td>Financial Intelligence Unit</td>
</tr>
</tbody>
</table>

1.1 Regulatory framework of prevention of money laundering and fight against terrorism financing

Basic measures and activities aimed at preventing and detecting money laundering and terrorism financing have been stipulated by the following legislations:

- Methodological Guideline No 9/2012 of the Financial Market Supervision Unit of National Bank of Slovakia of 20 November 2012 regarding the prevention by banks and foreign bank branches of money laundering and terrorist financing;
- Act 297/2008 of 2 July 2008 on the Prevention of Legalization of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended (further also “AML Act”);

Main regulations at the Group level are the following:

- Intesa Sanpaolo – Guidelines for the Fight against Money Laundering and Terrorist Financing and for the Handling Embargoes (May 2018);
- Intesa Sanpaolo – Sanctions Management Rules (October 2015)
- Intesa Sanpaolo – Rules on Transactions in the Armament Sector for Foreign Banks (June 2017);

Main best practices at international level are the following:

- Sound management of risks related to money laundering and financing of terrorism (Basel Committee on Banking Supervision – February 2016);

The regulations issued by US Authorities, included in the following main provisions, are also of particular significance in view of the Intesa Sanpaolo Group operations in the United States:

- Bank Secrecy Act – “BSA” (1970), designed to identify the source, volume and currency of financial instruments that flow into and out of the United States or are deposited in their financial institutions;
- US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tool to Intercept and Obstruct Terrorism - 2001) which was issued following the terrorist attacks of 11 September 2001, extending the BSA requirements, and requiring financial institutions to prepare due
diligence procedures and improve the sharing of information between the financial institutions and the US government;

- Law 302 - Section 504 (NY DFS Rule on Transaction Monitoring and Filtering - 2017) which establishes minimum standards for monitoring transactions and sanctions on Banks subject to New York laws, including the jurisdiction of the Department Financial Service;

- Department of the Treasury Financial Crimes Enforcement Network, (‘31 Code of Federal Regulation Parts 1010, 1020, 1023, 1024, and 1026 Customer Due Diligence Requirements for Financial Institutions’) that defines the new requirements in terms of identification of the beneficial owner and establishes a control-based approach based on both substantive and formal standards.

Since it operates in New York, Intesa Sanpaolo signed the “US Patriot Act Certification” whereby its commercial and financial operations in the United States are also subject also to United States laws, such as the execution of payment orders in dollars and in general, transactional activities carried out on its own account and on the account of third parties. The transactions that the Bank undertakes on its own account and/or on behalf of its customers are also subject to United States laws when these transactions involve a relationship with parties subject to US legislation (for example US banks, foreign branches of US banks and US Subjects in general).

Basic requirements as regards the abovementioned regulations are the following:

- the obligation to arrange risk prevention measures that are proportional to the type of customer, relationship, product or transaction. More specifically, it is necessary:
- to acquire enough information to identify the customer, the beneficial owner and the scope of the relationship or the transaction;
- constantly monitor the effectiveness of the relationship;
- the obligation not to open a new account, carry out an occasional transaction or maintain an existing account if the due diligence obligations cannot be fulfilled or if there is a suspicion of money laundering or terrorist financing;
- the obligation to report suspicious activity within the scope of active cooperation with the Authorities;
- the obligations regarding use of the cash, bearer securities or other means of payment;
- the obligation for adequate personnel training to ensure the correct application of the provisions;
- the obligation to store the data for anti-money laundering requirements;
- the obligation of the Control Body to report any relevant offences that it becomes aware of when carrying out its duties.

In order to comply with said obligations, the recipients must identify consistent organisational functions, resources and procedures that are in the right proportion to the type of activities carried out, their sizes, organisational complexity and operational characteristics.

The organisation required by the law must be based on:

- the setting up of a special function in charge of preventing and combating the execution of money laundering and terrorist financing transactions, the appointment of a person in charge and a person delegated the authority to report suspected money laundering or terrorist financing transactions;
- a clear definition of roles, duties and responsibilities, and procedures that guarantee compliance with customer due diligence and suspicious activity reporting obligations as well as obligations to store documentation and records of the accounts and the transactions;
- a control function structure with coordinated components, including through suitable information flows, and which is also consistent with the company size and complexity, the type of services and products offered as well as the degree of risk associated with the customers’ characteristics;
- strong accountability by employees and outside business partners and suitable controls that can monitor their compliance with the regulatory obligations, the internal processes, and their implementation.
1.2. Regulations on dealing with embargoes

The Slovak Republic, with the aim to preserve or re-establish international peace and security, has adopted restrictive measures and embargoes imposed by the United Nations Security Council Resolution, resulting in a partial or full suspension or weakening of economic relations with one or more third countries.

The European Union has been adopting restrictive measures and embargoes with the aim to:
- Preserve common values, core interests, independence and integrity, in line with the principles of the Charter of the United Nations;
- Strengthen security in every possible way;
- Observe peace and strengthen international security;
- Promote international co-operation;
- Develop and maintain both democracy and adherence to international laws, human rights and fundamental freedoms.

At community level the main legislative framework consists of:
- Regulation 2580/2001/EC of the Council of 27 December 2001, which establishes an obligation to freeze capital and a ban on the provision of financial services to certain natural persons, legal persons, groups or entities that commit, or attempt to commit, any act of terrorism and legal persons, groups or entities controlled by the foregoing;
- Regulation 881/2002/EC of the Council of 27 May 2002, which imposes specific restrictive measures on certain persons and entities associated with Osama bin Laden, the Al-Qaida network and the Taliban, and forbids providing them with military assistance;
- Regulation 753/2011/EC of the Council of 1 August 2011, concerning additional restrictive measures against certain individuals, groups, companies and entities in view of the situation in Afghanistan, also considering the decisions of the “Sanctions Committee” and “1267 Committee” established by the Security Council of the United Nations;

There are also other European Community sources deriving from the current international framework that establish a particular regime prohibiting investments in certain industrial sectors or exporting to the countries referred to in the company regulation as “Group A Countries”.

In addition to the provisions of directly applicable Regulations, at national level the main legislative framework consists of:
- Act No. 39/2011 Coll. on Dual-Use Items and on Amendment to Act of the National Council of the Slovak Republic No. 145/1995 Coll. on Administrative Fees as amended
- Act No. 289/2016 Coll. of 11 October 2016 on the execution of international sanctions

The legislative framework establishes restrictive and sanctioning measures against governments of third party countries, as well as non-state entities and natural persons or legal entities and specifically:
- arms embargoes;
- other specific or general commercial restrictions (ban on export and import);
- financial restrictions (freezing of goods and resources, bans concerning financial transactions, restrictions on export credits or investments);
- admission restrictions (ban on visas or travelling);
- criminal penalties for those financing terrorist or subversive associations and for those exporting dual-use items in breach of administrative regulations governing dual-use.

1 The Sanction Committee has been set up at the United Nations Security Council (UNSC). It was established according to paragraph 30 of Resolution 1988 (2011) of the UNSC, while the Committee 1267 was set up at the UNSC, according to Resolution 1267 (1999) and 1333 (2000) of the United Nations Security Council.
By introducing obligations and related penalties sanctions for parties (natural persons or legal entities, government or non-government entities) with which the Bank may directly or indirectly establish a business relationship, based on lending operations, this legislation requires that, with regard to oversight of the risk of money laundering and terrorist financing and related risks, measures must be provided to guarantee:

- data registration and operational controls on financial transactions related to imports or exports carried out by customer companies;
- traceability of controls on transactions carried out from/towards countries, natural persons and legal entities subject to restrictions;
- the freezing of goods and resources that can be traced to designated parties that the restrictive measures apply to, and forwarding the resulting communications to the Financial Intelligence Unit (FIU);
- the reporting of suspected terrorist financing or weapons of mass destruction proliferation activities.

Where necessary, the Intesa Sanpaolo Group applies also financial restrictions established by the external legislative framework (e.g. freezing of assets and resources, bans on specific financial transactions, bans on documentary transactions linked to the export of dual-use and/or hazardous goods) and is also subject to embargo provisions issued by the OFAC, whose duty it is to administer and enforce economic and commercial sanctions issued by the United States of America against foreign countries, terrorists, drug dealers and all those suspected of being involved in the trade, production and use of weapons of mass destruction.

---

2 The internal rules of the Parent Company Intesa Sanpaolo, of the Banks and of all the branches and subsidiaries of Intesa Sanpaolo establish how to identify and isolate incoming and outgoing payments in every currency, originating from or addressed to parties (natural persons and legal entities, countries) included in the Sanction Lists of the Intesa Sanpaolo Group.
2. OBJECTIVES, DEFINITIONS AND PRINCIPLES

2.1. Objectives

This Document aims at:

- Setting out the main roles and responsibilities of the Bank’s Corporate Bodies and organizational units which participate in prevention of money laundering, fight against terrorism financing and dealing with embargoes;
- Defining principles applied by the Bank in the process prevention of money laundering, fight against terrorism financing and dealing with embargoes

2.2. Definitions

**Money laundering**: the following actions, if performed intentionally shall constitute “money laundering”:

a) conversion of nature of property or transfer of property, knowing that the property originates from criminal activity or involvement in criminal activity, with the aim of concealing or disguising the illicit origin of the property or with the aim of assisting any person involved in the commission of such criminal activity to avoid the legal consequences of that person’s conduct,

b) concealment or disguise of the origin or nature of property, the location or movement of property, the ownership or other title to property, knowing that the property originates from criminal activity or involvement in criminal activity,

c) acquisition, possession, use and handling of property, knowing that the property originates from criminal activity or involvement in criminal activity,

d) involvement in action under letters a) to c), even in the form of association, assistance, instigation and incitement, as well as in attempting such action.

**Terrorism financing**: it means the provision or collection of funds or property with the intention of using them or knowing that they are to be used, in whole or in part, to commit: a) the criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism and some forms of participation in terrorism or; b) financing of daily needs of a person, where it can be supposed, that this person has the intention to commit or has committed the criminal offence of terrorism and some forms of participation in terrorism, c) the criminal offence of theft, the criminal offence of extortion or the criminal offence of counterfeiting and altering a public document, official stamp, official seal, official die, official sign and official mark or of instigating, aiding or inciting a person to commit such a criminal offence or his attempt aimed to commit a criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism and some forms of participation in terrorism, or d) committing of offences according to ratified and promulgated international agreements, to which the Slovak Republic has committed itself.

**Embargo**: is generally defined as the ban on commerce and trade with countries subject to sanctions, in order to isolate and put their governments in a difficult position with regard to their domestic policy and economy. In these Guidelines “embargo management” means the activities for implementing the controls and measures illustrated in the paragraph describing the governing legislation.

**AML Officer**: a person appointed by the decision of Management Board of the Bank taken into consideration the opinion of the Supervisory Board, as the Head of AML Department, responsible for the measures and activities prescribed by the AML Regulatory References, or the Rulebook, respectively, to detect and prevent money laundering and counter terrorism financing.
The AML Regulatory References: the regulatory references mentioned in detail above (section 1.1 Regulatory framework of prevention of money laundering and fight against terrorism financing and section 1.2. Regulations on dealing with embargoes)

The FIU: the Financial Intelligence Unit of Slovakia.

The Bank: VÚB Bank.

The Parent Company: Intesa Sanpaolo.

Network Unit: organizational unit engaged directly in customer relationship management, including Branch Employees, Tellers, Corporate Relationship Managers, etc.

Network Unit Responsible: employee of a Network Unit assigned with management responsibilities (typically Branch Manager, Regional or Area Manager, etc.)

AML: Anti-Money Laundering.

PEP: natural person who is or has been entrusted with a prominent public function, including the members of this person’s nuclear family or a person known to be a close associate of such persons.

PEP shall also be understood a natural person known to be beneficial owner of a) the same customer or to be otherwise in control of the same customer, as a person referred to in the above paragraph, or runs a common business with a person referred to in above paragraph or b) a customer established for the benefit of a person referred to in the above paragraph.

2.3. General governance model principles

The management model of the Bank for the fight against money laundering and terrorism financing is based on integrity value – to follow the objectives in an honest, correct and responsible manner, fully abiding by rules, the Group’s Code of Ethics and relevant regulations – as well as on other principles aimed to ensure an efficient framework in the fight against money laundering and terrorism financing.

- In monitoring risks relating to money laundering, terrorist financing and breach of embargoes, the Bank has adopted the following general standards:
  - inspiration from the values of honesty, accuracy and responsibility; in substantive compliance with the Code of Ethics of the Group;
  - cooperation with the Supervisory Authorities for the prevention of the issues in question, taking into account the regulatory provisions governing the confidentiality of reporting and information concerning suspicious activity, protection of personal data (privacy) and “banking secrecy”;
  - adoption of oversight standards in terms of guidelines, rules, methods, processes and instruments in line with international principles and reasonably standard at Group level, in accordance with the applicable rules at local level;
  - adoption of ‘risk-based’ control measures that are proportional to the characteristics and complexity of the activity performed and the legal form, size and organisational structure of the Bank.

3. ROLES AND RESPONSIBILITIES

Responsibility for prevention of activities relating to the legalization of income derived from criminal activity and AML tasks performance, including the protection against terrorism financing, shall be within the authority of the Management Board, acting through a separate internal department (AML Department).
The oversight of the processes for the fight against money laundering and terrorism financing and dealing with embargoes demands involvement of the following Bank's interacting bodies and organizational units with their different roles and responsibilities:

- Supervisory Board
- Management Board
- Audit Committee
- Compliance Department
- Anti-Money Laundering Department
- AML Officer
- Legal Services Department
- Operations and IT Division
- Risk Management Division
- Human Resources and Organization Department
- Retail and Corporate Banking Divisions
- Internal Audit and Control Department
- Information Security and Business Continuity Management

3.1. Supervisory Board

The Supervisory Board carries out the following activities:

- Approves, on a proposal from the Management Board, the Bank's AML Guidelines and AML Rulebook and related updates;
- Monitors the compliance with anti-money laundering and counter terrorism financing provisions;
- Supervises the implementation of AML regulations; the Supervisory Board may establish committees such as Audit Committee which have a right to review/investigate all matters of the Bank;
- Provides its opinion to the Management Board relating to the appointment of the AML Officer and his/her Deputy
- Approves the reports submitted by the AML Officer (annual report, risk assessment, semi-annual and ad-hoc reports)

3.2. Management Board

The Management Board is responsible for establishing and functioning of an Anti-Money Laundering Department (hereinafter referred to as the "AML"). The Management Board carries out the following activities:

- Defines the Bank's AML Guidelines and AML Rulebook, and related updates, on a proposal from AML Officer, which submits to the approval of the Supervisory Board;
- Appoints/removes the AML Officer, and his/her deputies, taken into consideration the opinion of the Supervisory Board, with the prior binding opinion of the Head of AML Head Office Department of the Parent Company;
- Approves the training programme concerning anti-money laundering;
- Defines the information flows intended to ensure to the governing bodies and the control functions full awareness and management of the requirements;
- Requires the AML Officer to report on AML activities semi-annually;
- Evaluates the adequacy and effectiveness of AML risk management and control system;
- Reviews the violations of AML provisions promptly communicated by the Audit Committee;
- Sets up and updates the internal procedures, detailing operational processes implemented to manage the AML requirements and the roles and responsibilities attributed to involved structures;
- Assesses the organisational structure and the adequacy of the internal control system with regard to pertinent obligations, submitting them to review if necessary;
- Evaluates and ensures the main remediation actions carried out in relation to relevant violations of AML provisions;
- Rules on strategic decisions concerning anti-money laundering and counter terrorist financing, which submits to the approval of the Supervisory Board.

3.3. Audit Committee

The Audit Committee carries out the following activities:
- Verifies the compliance with anti-money laundering and counter terrorism financing provisions, assessing the effectiveness and efficiency of the governance model, also based on the examination of the results of periodic control activities concerning AML conducted by Internal Audit and Control Division and AML Department;
- Addresses the evaluation of detected anomalies ensuring the implementation of the necessary remediation actions;
- Evaluates any violations of the AML provisions (customer due diligence, record keeping, etc.) based on the information flows received from the other Corporate Bodies and from the AML Officer;
- Requires the AML Officer to report on AML activities semi-annually.

3.4. Anti-Money Laundering Department

The AML Department, which has to be proportionate and adequate to the structure and the risk profile of the Bank, performs the following activities:
- Checks corporate processes and procedures, and proposes, in association with the applicable corporate functions, the organisational and procedural changes required and/or advisable to ensure adequate control over the risk of money laundering, terrorist financing and breach of embargoes;
- Monitors the regulatory framework with regard to anti-money laundering, counter-terrorist financing and payment systems in order to implement any potential changes;
- Checks the compliance of the Bank with local AML Regulatory References and manages the relations with local supervisory authorities;
- Provides consulting, advisory and reporting towards the corporate bodies and the structures of the Bank involved in AML related activities;
- Defines the specific contents of the training programme concerning anti-money laundering;
- Identifies, measures and evaluates compliance risks, and manages them via second level controls;
- Creates and implements AML work plan and programs;
- Identifies control objectives for first level controls to be performed by business network; Analyzes the first level control results;
- Defines and conducts second level control checks and tests;
- Analyses the outcomes of automated transactional monitoring (real-time monitoring of foreign payments; ex-post monitoring of transactions);
- Prepares and updates the rules and methods and supports the drafting of the operating processes relating to profiling methods, customer identification and execution of due diligence (standard and enhanced);
- Assesses and authorises the opening of new accounts, the execution of occasional transactions or the maintenance of existing accounts for customers assigned as high risk, or for medium risk customers when a specific request is submitted by the operational units;
- Evaluates suspicious activity reports (both submitted by the network units as well as stemming from the automated transactional monitoring) and submits them to FIU;
- Maintains registers, reports to outside organisations, interacts with authorities;
- Receives reporting from control structures (e.g. Internal Audit and Control Division) and other operational functions (e.g. Network Units) pursuing AML requirements;
- As AML IT tool's business owner, provides methodological support to AML IT tool' users;
- Ex ante assessment, for its area of competence, of compliance of new processes/products/services
Manages, for the areas it is responsible for, relations with the Financial Intelligence Unit (FIU), the National Bank of Slovakia and the Ministry of Finance;
- Certifies the standard questionnaire relating to the internal processes and procedures adopted by the Bank on anti-money laundering, combating terrorist financing and embargoes handling matters, to generally be delivered to banks or financial institutions that carry out the due diligence to initiate correspondent banking relationships or similar relationships with the Bank.

3.5. AML Officer

The Head of AML Department is entrusted with the role of AML Officer. The AML Officer and his/her substitute are the persons authorized and responsible for the implementation of measures and actions taken to prevent and disclose money laundering and terrorism financing.

The AML Officer is appointed/removed by the Management Board taken into consideration the opinion of the Supervisory Board. The decision is subject to a binding prior approval by the Head of AML Head Office Department of the Parent Company. The AML Officer and his/her substitute perform the following activities:
- Prepares AML Guidelines, AML Rulebook and other related procedures;
- Carries-out AML self-risk assessment and AML reporting;
- Organises and directs AML activities at Bank’s level;
- Cooperates with and reports to the Parent Company’s relevant Anti-Money Laundering Function in order to ensure the alignment of Bank’s internal AML procedures to the provisions issued by the Parent Bank, in compliance with local regulations;
- Reports to Parent Company’s relevant Anti-Money Laundering Function for its evaluation any circumstances, deriving from mandatory local AML Regulatory References, which shall not permit the application of the requirements based on EU Regulation or issued by the Parent Company;
- Assesses customers and transactions positively matched against sanction lists, addressing the initiatives required based on the assessment outcomes;
- Authorises the opening of ongoing relationships with Politically Exposed Persons and correspondent banking accounts and similar accounts with credit or financial institutions located in third countries identified by the European Commission as high-risk third countries;
- Ensures the provision of professional trainings for relevant employees and defines the content of such trainings;
- Prepares an annual evaluation of the financial and material resources of the AML Department;
- In his capacity as an AML Reporting Officer, is responsible for reporting of suspicious cases to the FIU;
- Manages relations with local authorities;
- Submits four types of report to the Supervisory Board and Audit Committee:
  - evaluation, in the form of the annual comprehensive AML report, of the AML risk management system of the Bank, and provides a statement regarding its adequacy and effectiveness;
    - the results of the annual AML risk assessment and the annual AML plan\(^3\);
    - provides an extraordinary (prompt) mandatory report in the event of a significant irregularity or control problem;
    - provides regular reports semi-annually.

- Submits four types of report to the Parent Company’s relevant AML function:
  - semi-annual report or, if justified by the risks related to the AML issue, ad-hoc report;
  - extraordinary reporting if any significant deficiency in AML controls are found in the course of operation (e.g. deficiencies that may result in significant legal or regulatory sanctions, or that bear significant financial or reputation risk)

\(^3\) Once these documents are approved by the Supervisory Board, they are forwarded to the Parent Company’s relevant AML function
- annual comprehensive AML report, of the AML risk management system of the Bank, and provides a statement regarding its adequacy and effectiveness;
- the results of the annual AML risk assessment

The Bank shall make available to the AML Officer the following:
- Unrestricted access to all the data, information and documentation which is necessary for anti-money laundering and counter terrorism financing;
- Adequate authorisation for efficient discharging of his/her duties;
- Adequate staff resources both in terms of number and required skills, and also adequate material and other work conditions including remuneration;
- Adequate IT solutions and automated tools;
- Appropriate conditions which guarantee the adequate level of protection of confidential data and information which are made available to the AML Officer and his/her substitute;
- Adequate IT support which makes possible a permanent and secure monitoring of activities in the area of anti-money laundering and counter-terrorism financing;
- Regular professional education and training for preventing and detecting of money laundering and terrorism financing;
- Substitution to the AML Officer when he/she is absent.

3.6. Legal Services Department

The Legal Services Department carries out activities described in the Bank's business model. Legal Services Department, upon request of AML Department, provides support and counsel on the interpretation of regulations concerning money laundering prevention, fight against terrorism financing, dealing with embargoes, as well as on the implementation and the development of Law cases.

3.7. Operations and IT Division

The Operations and IT Division carries out activities described in the Bank's business model. Operations and IT Division, upon request of AML Department, provides support on the definition of territorial network operating processes and coordination of IT Division interventions on the basis of AML requirements.

Activities of the Division for Applicative SW are of vital significance in prevention of money laundering and terrorism financing and dealing with embargoes, through:
- An appropriate IT support, enabling continuous and safe monitoring of activities of prevention of money laundering and terrorism financing;
- Design, development or purchase of software to support the Bank's business related to prevention of money laundering and terrorism financing, based on requirements of the AML Department;
- The analysis and development of processes of prevention of money laundering and terrorism financing concerning their optimisation by using IT technology;
- Providing undisturbed, right and safe operation of all software applications (both the internally developed and purchased ones) to support the Bank’s efforts in prevention of money laundering and terrorism financing;
- Maintenance and supervision of the work of applications which the Bank uses to support activities of prevention of money laundering and terrorism financing.

3.8. Risk Management Division

The Risk Management Division carries out activities described in the Bank's business model. Risk Management Division, upon request of AML Department, provides support on the definition of operational and reputation risk assessment methodologies and tools.
3.9. Human Resources & Organization Department

The Human Resources & Organization Department carries out activities described in the Bank’s business model.
The Human Resources & Organization Department, upon request of AML Department, provides support on:
- The application of AML requirements when organisational and process changes are planned;
- The definition of correct quantities of resources required to fulfil obligations regarding anti-money laundering;
- The arrangement of employee education, trainings;
- The undertaking of appropriate disciplinary measures, in accordance with regulations, against the employees who have violated their contractual obligations related to AML requirements.

3.10. Retail and Corporate Banking Divisions

All organisational parts which belong to the Retail and Corporate Banking Divisions have an active role in the process of meeting the requirements of prevention of money laundering and terrorism financing and acting in case of an embargoes. It is the responsibility of operating divisions to perform first level controls in the area of AML requirements.

More specifically, in order to obtain greater awareness of customers, the divisions carry out the following activities:
- identify the customers and beneficial owners, acquiring the information and documentation (including any additional information needed in the event of relations with credit institutions and financial institutions) needed to perform the due diligence checks and to assign a risk profile to the customer;
- keep the documentation acquired and keep the relative information updated;
- notify the AML Department of customers classified as high risk for the related authorisation request; for medium risk customers the operating division makes an independent decision on whether to refuse to open an account or execute an occasional transaction;
- constantly monitor relations with customers and the relative transactions;
- inform the customers of the Bank’s decision not to open a business relationship and/or carry out a transaction or of its intention to terminate an existing relationship.

The Manager of the operating division (or the Relationship Manager with respect to Corporate customers) ensures that the due diligence obligations are constantly developed in due compliance with applicable AML policies.

3.11. Internal Audit and Control Department

The Internal Audit and Control Department undertakes activities in accordance with the Internal Auditing procedures.
The Internal Audit and Control Department reviews the processes, scopes and operations related to anti-money laundering at specific, regular intervals and informs the competent Corporate Bodies of the outcome of its assessments.
The activities of AML Department and Internal Audit and Control Department are independent between themselves.

Internal Audit and Control Department shall notify the AML Officer of any relevant findings that are related to Money laundering matters and controls. The AML Officer must inform the Internal Audit and Control Department of any remediation actions aimed at solving such findings.
3.12 Information Security and Business Continuity Management

The duties and responsibilities of the Information Security and Business Continuity Management Sub-Departments are described in its Organisational Codes. The sub-departments define the rules and actions to take to protect the data, information and infrastructures to guarantee business continuity and the legitimate performance of company activities, and to keep security conditions in line with prevailing laws, including with reference to monitoring anti-money laundering, terrorist financing and handling of embargoes.

4. TOPICS COVERED IN MACRO PROCESSES FOR FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING

The macro processes for managing obligations concerning anti-money laundering, combating terrorist financing and handling of embargoes can be divided into the following main areas:

- definition of the guidelines and methodological rules;
- risk Assessment and Risk Appetite Framework;
- regulatory alignment;
- consultation and clearing;
- assurance;
- spreading the culture of anti-money laundering, combating terrorist financing and embargo handling;
- interaction with the Supervisory Authorities and management of non-compliance events;
- specific requirements (customer awareness and profiling; data retention; transaction monitoring; reporting and information management across the Bank)

In addition to these areas there are also some cross processes to support implementation and execution of activities to prevent, monitor and mitigate the risk of money laundering and terrorist financing.

4.1 Definition of the guidelines and methodological rules

The AML Officer, in accordance with the Parent Company’s relevant AML function, defines the applicable guidelines and methodological rules to monitor and assess, at Bank level, the risk of money laundering, terrorist financing and breach of embargoes, such as the AML Guidelines, AML Rulebook and other related procedures.

4.2 Risk Assessment and Risk Appetite Framework

The AML Officer prepares a risk assessment every year, with respect to money laundering, terrorist financing and breach of embargoes (known as AML Risk Assessment). The AML Risk Assessment is part of annual AML reporting towards the Management Board, the Supervisory Board, the Audit Committee and the Parent Company’s relevant AML Function.

The assessment is carried out on the basis of the methods defined by the Parent Company’s relevant AML function. More specifically, the AML Risk Assessment method investigates the extent of the inherent risk and the related vulnerability through mainly quantitative indicators, integrated with qualitative assessments that correlate the type of potential risk (for example the level of customer risk) and the risk mitigation elements for money laundering, terrorist financing and breach of embargoes (for example the number of customers where the beneficial owner was registered) with respect to the size of the company.
4.3 Regulatory alignment

The monitoring of the risk of money laundering, terrorist financing and breach of embargoes is carried out on a preventive basis, firstly ensuring that external laws are constantly monitored and adequately incorporated into the guidelines, processes and internal procedures. Legal Services Department, upon request of AML Department, provides support and counsel on the interpretation of regulations concerning money laundering prevention, fight against terrorism financing, dealing with embargoes, as well as on the implementation and the development of Law cases.

4.4 Consultation and clearing

- Risk is controlled on a preventive basis, including through:
  - the consultation and assistance given to the Corporate Bodies and the Bank units on the interpretation and application of external and internal rules in the AML area;
  - the prior assessment of compliance with prevailing AML laws (clearing) on:
    - innovative projects, including starting up new activities and entering new markets;
    - new products and services to be marketed and/or significant changes to existing ones;
    - sensitive cases and transactions in relation to which the company processes, as governed by the AML Guidelines and the internal rules of the Bank, provide for the prior assessment by the AML Department.
- The AML Department provides consultation and assistance to the corporate bodies and the structures of the Bank on matters relating to the actual application of external laws in the AML area to the company processes and activities, and the behaviour to adopt.

With regard to the clearing activities, the AML Department analyses, inter alia, the compliance of corporate transactions identified as sensitive for the purpose of embargoes and that involve countries, product categories, or parties subject to sanctions and/or restrictive measures.

4.5. Assurance

The control over the risk entails, also on a preventive basis, subsequent checks of the adequacy and effective application of the internal processes and procedures, the suggested organisational changes to prevent risk, and in general, the monitoring of effective compliance with external and internal rules by the company’s units.

With respect to risk monitoring and control, the assurance model assigns:

- the line controls to the operational and business units, carried out on a continuous basis over individual transactions, and the managerial analyses consisting of the systematic monitoring of phenomena characterised by high anomaly levels that have to be promptly dealt with, and/or taking them back to areas of operational and management uniformity;
- the monitoring of the correct application of the applicable methodological and control framework by the operational and business units to the second level control functions, by checking both the design of the processes, procedures and controls and correctly applying the applicable controls;
- The AML Department identifies control objectives for first level controls to be performed by business network and analyses the first level control results. It also defines and conducts second level control checks and tests.
- AML Department responsibilities:
  - identification of control objectives when designing or reviewing business processes, functional to the declination of the first-level controls;
  - definition of second level controls in line with the Parent Company’s second level control framework;
  - analysis of the outcome of controls activities and assessment of the effectiveness of safeguards;
  - define the action plan and provide recommendation to operating structures;
- It is the responsibility of operating structures to perform first level controls.
4.5.1. Interactions with the other control functions and information flows

In carrying out the checks, the AML Department also uses the results of the checks by the Internal Audit which makes the necessary assessments on the processes and behaviour, making the relative results available to the units in charge of monitoring.

The AML Department has access to all the Bank activities and any relevant information to carry out its duties, including through direct interaction with the staff. To this aim:
- it receives and sends the information flows;
- the other company units must inform it, in a timely, complete manner, of any relevant facts in order to monitor the risks in question;
- it may request and receive any other relevant information to carry out their duties from the other company functions.

4.6. Spreading the culture of anti-money laundering, combating terrorist financing and embargoes

The dissemination, at all company levels, of a culture based on the principles of honesty, fairness and compliance in accordance with the spirit and letter of the law is a basic assumption in controlling risk. Efficient application of regulations relating to anti-money laundering, combating terrorist financing and handling of embargoes must incorporate full awareness of the aims and principles underlying the system.

The AML Department works with the Training and Development Sub-department to establish efficient channels of communication and training instruments, identifying the training requirements relating to the applicable matters and preparing the content of the training initiatives for all the Bank resources, in order to ensure that the staff, with specific attention to the sales force for the products and the managers of the business units, have adequate awareness of the applicable laws, the obligations and related responsibilities in the AML area, the consequences resulting from the failure to fulfil said obligations and to ensure they are able to knowingly use support instruments and procedures in fulfilment of the requirements established by the law.

Specific training programmes are also provided to staff in the AML Department so that they are always updated on risk developments in the area.

The AML Department monitors development of the training programmes, checking use and effectiveness, and provides adequate results to the Corporate Bodies, also for the timely identification of any action that may need to be taken.

4.7. Interaction with the Supervisory Authorities and management of non-compliance events

- Relations with the Supervisory Authorities and management of non-compliance events are occasions of special relevance when controlling risk. The AML Department provides for management of the following in the areas it is responsible for:
  - relations with the Supervisory Authorities (Financial Intelligence Unit, National Bank of Slovakia), coordinating the activities needed to provide feedback to the Authorities;
  - non-compliance events, providing assistance and cooperation to the unit in order to ensure the identification and implementation of the actions to undertake to fill any organisational and/or procedural gaps.

- The interaction processes also include sending specific reports to the Authorities, in accordance with the requirements defined by the law with respect to anti-money laundering, combating terrorism and handling embargoes. This reporting includes:
  - transmitting on a quarterly basis, to the Ministry of Finance, communications relating to parties to whom restrictive measures apply within the scope of laws on embargoes and combating terrorist financing;
4.8 Customer awareness and profiling

In order to make sure a customer due diligence is performed, the following activities should be undertaken:

- Customer and beneficial owners identification and collection of identification documents, documents certifying due diligence issued by other Financial Institutions and additional information required for establishing the risk profile to be assigned to the customer; registration of customers and beneficial owners in the Bank's Master File and preservation of the documentation acquired for identification and due diligence, in accordance with confidentiality provisions and measures set forth by internal regulations. These phases are entrusted to the network units which manage customer business relations. If it is not possible to comply with the obligations on customer due diligence, or the customer due diligence points out a negative rating or an unacceptable risk, there is the obligation to refrain from establishing a business relationship or performing the transaction. If this situation happened with reference to a relationship already in place or to an in progress transaction, the Bank should stop to carry on the relationship or to execute the transaction;

- customer risk-assessment based on the risk of money laundering and terrorist financing, carried out by the network units, using information acquired during the customer due diligence process;

- constant monitoring of ongoing business relationships, carried out by the network units as well as by AML Department (based on ex-post transactions monitoring), in order to update customer due diligence, and of the declared purpose of the business relationship, in the presence of transactions that are unexpected, anomalous or inconsistent with the customer’s previously known economic and financial profile or of news of significant events;

- periodic re-assessment of the risk profile and update of data (identification documents, business register certificates, public registers and lists, information, etc.) carried out by the network units, with the frequency required by the risk profile previously assigned to the customer;

- authorisation to open a new business relationship, to execute an occasional transaction or to maintain an existing business relationship on the basis of the risk profile assigned to the customer. For customers classified with a high AML risk, authorisation must be provided by the AML Department. In cases of the online account opening process, enhanced due diligence must be applied but the business relationships are not subject to the AML Department’s authorization, unless higher AML risk indicator may occur in connection with the client (e.g. status of PEP), other than the remote on boarding process.

4.9. Data retention

The data recorded in the course of customer due diligence shall be kept for ten years after the termination of the business relationship or the performance of the transactional order.

4.10. Transaction monitoring

Three main processes have been established to guarantee control of transactions carried out by customers:

- ex ante monitoring by the network units carrying out the transactions, of transactions executed by customers, in order to identify, block and report transactions in which money laundering and/or terrorist financing is suspected. In order to fulfill the obligation of abstention and of assessing the need for immediate application to the FIU to request a suspension order in cases of evident risk, for example those involving an outflow of funds and payment means, the network units may seek advice from the AML Department;

- ex ante monitoring of payments and documents representing goods through the scan against the Sanction Lists and/or Group internal List (“Bad Guy”) and checking the results of control procedures. These checks are automated and involve the Payments Unit and the AML Department;

- ex post monitoring of transactions by the AML Department in order to identify anomalous transactions, with the assistance of the automatic system for managing anomaly indicators. After an anomalous transaction has been identified, the AML Department may contact the network units in
order to carry out a first level investigation and, if it proves necessary, the AML Department reports the suspicious transaction to the FIU.

In order to reduce the risk of money laundering and terrorist financing and the related reputational, legal and operational risks, taking into account specific regulations on the matter, the Bank (i) shall not make cover payments\(^4\) in US currency and (ii) shall operate with payable-through accounts\(^5\) only if customer due diligence is guaranteed by the counterparty bank using said payable through accounts.

4.11. Reporting and information management across the Bank

The Bank is liable to the provisions of AML Regulatory References, and it is therefore obliged to set up processes of reporting to the FIU and Bank corporate bodies aimed at preventing of money laundering and terrorism financing and dealing with embargoes. The content of reports depends on which organisation it is intended for and also on the purpose of reporting, as follows:

- external reporting to supervisory bodies in accordance with requirements established in money laundering prevention and embargoes regulations (i.e. FIU, Ministry of Finance, National Bank of Slovakia);
- reports on AML activities addressed to the Supervisory Board, to the Management Board and the AML function of the Parent Company (please refer to point 3.5.1);

5. FINAL PROVISIONS

This Document shall be approved by the Supervisory Board of the Bank, in agreement with the Parent Company’s relevant AML Function.

As a result of risk assessments and decisions made by the AML Officer or the Supervisory Board, this Document can be amended if the purpose of effective money laundering prevention would reasonably require it.

\(^4\) Cover payment means the transfer of funds used when there is no direct relationship between the orderer and beneficiary’s payment service providers and it is therefore necessary to use a chain of correspondence relationships between the payment service providers. A cover payment involves three or more payment service providers. This payment aims to provide financial coverage of a message sent by the orderer’s provider to the beneficiary’s provider in which it directly communicates transfer of the funds.

\(^5\) Payable-through accounts are cross-border correspondent banking relationships between financial institutions, used to carry out transactions in their own name and on the customers’ behalf.