FINANŠU UN KAPITĀLA TIRGUS KOMISIJA

KUNGU IELA 1 • RĪGA • LV-1050 • TĀLRUNIS +371 6777 4800 • E-PASTS FKTK@FKTK.LV • WWW.FKTK.LV

21 December 2021
Riga

Recommendations No. 169
(Minutes No. 57, Clause 5 of the Meeting of the Council of the Financial and Capital Market Commission)

Recommendations for the Establishment of the Internal Control System for Anti-Money Laundering and Countering Terrorism and Proliferation Financing and Sanctions Risk Management, and for Customer Due Diligence

CONTENTS

Introduction

1. The Financial and Capital Market Commission (hereinafter referred to as – the Commission) has developed the recommendations for credit institutions, payment and electronic money institutions, private pension funds, investment firms, investment management companies, alternative investment fund managers, insurance companies, insofar as they provide life insurance or other insurance services related to the accumulation of funds, insurance intermediaries, insofar as they provide life insurance or other insurance services related to the accumulation of funds, reinsurance companies and to the branches of all of these subjects of Member States and third countries in the Republic of Latvia, as well as credit unions (hereinafter all jointly and each separately referred to as – an institution) for the establishment of the internal control system (hereinafter referred to as – the ICS) for anti-money laundering and countering terrorism and proliferation financing (hereinafter referred to as – the AML/CTPF) and the sanctions risk management, and for customer due diligence (hereinafter referred to as – the Handbook). Explanations provided for in the Handbook are applicable to each institution, insofar as they are consistent with the nature of the activity of the institution, provided services and products thereof, as well as considering the risk inherent to the activity of the institution.

2. According to the requirements of the Commission's Normative Regulation No. 5 of 12 January 2021 "Regulations on the Establishment of Customer Due Diligence, Enhanced Customer Due Diligence and Risk Scoring System and Information Technology Requirements" (hereinafter referred to as – the Customer Due Diligence Regulations), the Commission hereby issues the Handbook, in order to:

2.1. explain the implementation of the risk-based approach, in line with the requirements of the Customer Due Diligence Regulations;

2.2. explain the requirements laid down in the Customer Due Diligence Regulations for the purposes of establishment of the customer risk scoring system;

2.3. explain the measures laid down in laws and regulations to be taken within the scope of customer due diligence (standard, simplified and enhanced);

2.4. provide recommendations based on the best practice in the field of AML/CTPF.

3. The contents of the Handbook have been set up in accordance with the core AML/CTPF principles in the following chapters and the corresponding sub-chapters:

3.1. the first chapter "Risk Assessment" explains the need for performing assessment and the core principles of the money laundering and terrorism and proliferation financing (hereinafter referred to as – the MLTPF) risk and the sanctions risk to enable the institution to establish an appropriate ICS;

3.2. the second chapter "Internal Control System" entails the most significant key requirements for the ICS, explaining the objective of each separate ICS element and the activities required for the implementation of the objective in the sub-chapters;

3.3. the third chapter "Customer Due Diligence" explains the types of customer due diligence – standard, simplified and enhanced – to be applied in accordance with the customer risk. The sub-sections of this chapter provide explanations and examples on the scope and extent of the due diligence measures depending on the risk as well as additionally provide explanations on separate customer due diligence measures, the application whereof requires uniform understanding of the core principles, on the provision of information to customers and termination of the business relationship if the institution is unable to conduct customer due diligence;

3.4. the fourth chapter "Information Technology Solutions for AML/CTPF and Sanctions Risk Management" explains the requirements for information technology (hereinafter referred to as - the IT) solutions and includes recommendations for IT solutions for AML/CTPF and sanctions risk management;

3.5. the fifth chapter "Reporting to the Commission (quarterly reports, requests)" contains questions and answers on the AML/CTPF risk exposure review to be provided to the Commission;

3.6. the sixth chapter"Sanctions and the Prevention of the Financing of Terrorism and Proliferation" explains the risks and characteristics of sanctions and the financing of terrorism and proliferation, and provides guidance to assist institutions in managing those risks and ensuring compliance with regulatory requirements.

4. The purpose of the Handbook is to strengthen the implementation of the risk-based approach, in implementing the requirements in the AML/CTPF and sanctions field and managing the MLTPF and sanctions risk. The risk-based approach means that the institution identifies and understands the MLTPF and sanctions risk (hereinafter also referred to as – the risk) and applies the risk management measures pursuant to the risk the institution is exposed to, for the purposes of effective management of the risk. The AML/CTPF and sanctions risk management measures are to be set in accordance with the risk assessment – for the risk inherent to the activities of the institution (the institution, when developing its operational strategy (customer policy), shall specify in which jurisdictions it operates, the customers it attracts and serves, the services and products it offers, the channels it applies for distribution of the services and products) and for the individual inherent risk of the customer (assessing all risk affecting circumstances – customer risk, country and

geographical risk, the risk of services and products used by the customer, service and product delivery channels risk). Thus, the lower the customer risk, the smaller the scope of the due diligence; in turn, the higher the customer risk – the larger the scope of the due diligence is. This principle with corresponding examples is explained in the relevant chapters of the Handbook. In addition, it is necessary for the institution to develop an effective system enabling one to detect (verify) whether the previously obtained customer due diligence data is true and relevant (for example, obtaining and verification of data from the databases of trade (enterprise) registers, verification of data in publicly available sources), as well as an effective transaction screening system enabling one to ascertain the relevance and authenticity of initially obtained information about economic or personal activities, scope of transactions, source of funds and wealth, determining the frequency of those controls in accordance with a risk assessment. Nevertheless, considering the fact that each institution has different offered products and services, the risks inherent in its operations, as well as the customer base and the risk inherent thereto, measures applied by one institution may differ from the measures applied by another institution. Examples and explanations provided in the Handbook will be enhanced and supplemented, in line with the problems detected in practice.

5. The Handbook provides for a number of examples, in order to explain the requirements of the legal framework and the expected conduct of the institution. Using examples as explanatory information, they cannot be applied to all cases alike without due assessment, because the situations may differ. Real actual circumstances, even though they might seemingly be similar to the circumstances referred to in the examples, may differ, exactly when assessing the details of actual circumstances, which might result in a situation, where it is necessary to subject the institution to measures different from or additional to those referred to in the example. The conduct of the institution is also determined by the assessment of its MLTPF risk and risk policy, while the examples specified in the Handbook are not based upon particular risk assessment and policy.

1. Risk Assessment

1.1. Money laundering and terrorism and proliferation financing risk assessment

6. For the institution to be able to establish the AML/CTPF ICS consistent with its risk, inter alia, to comply with the risk-based approach and to take customer due diligence measures corresponding to the risk, first of all, it is necessary to carry out the assessment of the MLTPF risk of the institution, in order to clarify, assess and understand the risk the institution is exposed to. In the MLTPF risk assessment, the institution shall assess the money laundering, terrorism financing and proliferation financing risks in accordance with the specificity inherent to the services and circle of customer of the institution, geography of distribution of services and products thereof (for example, considering the jurisdictions, where the branch representative offices of the institution are located, etc.) and service and product delivery channels (for example, whether the agent, intermediary services are used, whether the services and products are offered online). In performing the risk assessment, the institution shall take into account both the European Union (hereinafter referred to as – the EU) and national risk assessment. European Banking Authority Guidelines on Risk Factors[1] (hereinafter referred to as – the EBA Guidelines) can serve as an example for the

[1] Guidelines in accordance with Sections 17 and 18 (4) of Directive (EU) 2015/849 on customer due diligence and factors to be taken into account by credit and financial institutions when assessing the risk of money laundering and

identification and assessment of risk factors inherent to an institution (they list both the risk factors inherent to an institution and the risk factors inherent to a customer). Based on the outcomes of the MLTPF risk assessment, the institution shall assess and determine its risk appetite[2].

7. Considering the purpose of the MLTPF risk assessment, it is necessary to update the MLTPF risk assessment, prescribing the frequency of updates according to the inherent risks, but at least once every three years. If an institution intends to make significant changes to, for example, the institution's operations and customer rights, the range of services and products or their delivery channels, it shall carry out a risk assessment of the changes made before the change is implemented. It is necessary for the credit institutions, based on the risk inherent to their activities, to carry out the updating of the MLTPF risk assessment at least once every 18 months.

8. It shall be necessary for the institution to assess whether the risk the institution is exposed to has changed – whether any new circumstances affecting the risk are identified, and to carry out the updating of the MLTPF risk assessment, by assessing whether the existing MLTPF risk management measures are consistent with the risk. The MLTPF risk assessment also enables the institution to set priorities in MLTPF risk management and to effectively perform the planning and allocation of resources necessary thereto (for example, the necessary IT systems, employees and their qualification). It is necessary for the institution to ensure appropriate and adequate resources for managing the risk inherent thereto.

9. In accordance with the requirements of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (hereinafter referred to as – the Law) when performing the risk assessment the institution shall take into account:

9.1. the risks identified by the European Commission in the EU MLTPF risk assessment[3];

9.2. the risks identified in the national MLTPF risk assessment report, as well as in the risk assessment conducted by the supervisory authority;

9.3. other risks inherent to the institution.

---

terrorist financing associated with a business relationships and occasional transactions ("ML/TF Risk Factor Guidelines"), which repeals and replaces Guideline JC/2017/37, available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016934/Guidelines%20ML%20TF%20Risk%20Factors_LV.pdf.

[2] Risk level the institution accepts and is able to manage.

[3] For instance, the assessment of 2019 is available at: https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

Example

Based on the risk assessment, the institution prescribes that low-risk customers would, in a secure manner, be identified off-site. Depending on the type of off-site identification, an increased risk may be inherent to the off-site identification, and it should be taken into account in the risk assessment. However, the evaluation thereof will not always automatically provide that all customers identified off-site are high-risk customers. It is necessary to consider the customer category for which such type of identification is permitted (for example, residents of the Republic of Latvia), what (how secure) the permissible off-site identification type is, which services the institution ensures via off-site identification. It is necessary for the institution to reflect its evaluation and arguments for the opinion reached in the risk assessment.

10. When determining the MLTPF risk the institution is exposed to, the following shall be assessed:

10.1. the inherent risk to which the institution is exposed prior to the application of risk management measures;

10.2. the effectiveness of the MLTPF risk management measures;

10.3. residual risk using the formula:

Inherent risk – effectiveness of the MLTPF risk management measures = residual risk.

11. When determining the **inherent risk** characteristic to the institution, the institution shall assess at least the following categories:

11.1. customer risk (for example, credit turnover of customers considered to be politically exposed persons (hereinafter also referred to as – the PEP)[4]; credit turnover of the customers, whose type of economic or personal activity is to be considered as high-risk, etc.);

11.2. country and geographical risk (for example, credit turnover of the customers, whose country of residence or registration is a higher risk country; payments received by the customers from higher risk countries, etc.);

11.3. risk of products and services used by the customers (for example, the turnover of customers using private banker's services; the turnover of customers using trust or fiduciary transaction services, etc.);

11.4. product and service delivery channels risk (for example, credit turnover of the customers identified off-site; credit turnover of the customers identified by an agent; credit turnover of customers – e-merchants; credit turnover of customers – financial institutions registered outside the EU, etc.).

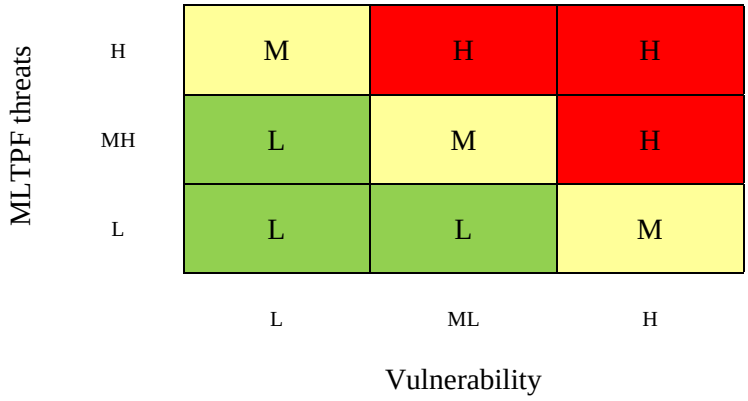
12. Other indicators may also be determined, in addition to those referred to in Clause 11. In each category the institution shall assess the risk increasing factors, in accordance with the rating whereof it shall set the inherent risk of the category.Having obtained the rating for each category, the institution shall prescribe an algorithm for the determination of overall inherent risk.

[4] The turnover of incoming payments of the customer; in cases when the activities of, and the services provided by the institution, do not include the performance of payments, the credit turnover shall be understood to mean the amount of the customer's transactions.

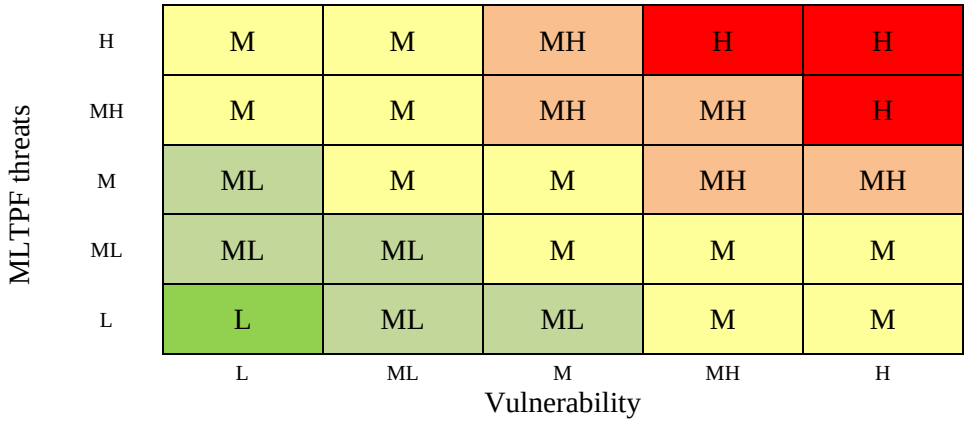
13. When determining **the effectiveness of the MLTPF risk management measures** of the institution, the institution shall assess the measures applied by it in the MLTPF risk management, in order to prevent the MLTPF and to ensure that the risk factors are identified (for example, IT systems, which are applied, requirements of policies and procedures, updating thereof, quality assurance mechanisms, management awareness and involvement, timeliness of introduction of audit recommendations, etc.). The institution shall assign the rating to each measure (for example, conforming, significant improvement, insignificant improvement, not conforming). Having obtained the rating of each individual measure, the institution shall determine the overall effectiveness of the measures.

14. **Residual risk** shall be clarified after the inherent risk has been assessed and the applied MLTPF risk management measures and the effectiveness thereof have been taken into account. It is important to note that, when calculating the residual risk according to the formula referred to in Clause 10, the largest weight shall be assigned to the inherent risk, because, irrespective of how effective the ICS is, it cannot reduce the current or inherent risk to zero.

15. When carrying out the MLTPF risk assessment, it is possible to apply the risk assessment matrices of a different level of detail, for example:



High (H)	Moderate (M)	Low (L)



High (H)	Moderately high (MH)	Moderate (M)	Moderately low (ML)	Low (L)

16. The type of risk assessment matrix applied by the institution depends on the activity of the institution, the size, and the customer base thereof. For example, institutions with a smaller customer base or a limited range of the offered products and services more often use the risk assessment matrix providing for a low, moderate and high risk. In turn, in cases when the activities and size of the institution allow and the customer base is comprised of customers of various profiles, and, correspondingly, a more nuanced risk breakdown would be applied for the effective assessment thereof, the institution may use the risk assessment matrix providing for a more detailed risk breakdown.

1.2. Sanctions risk assessment

17. Sanctions risk assessment, similar to the MLTPF risk assessment, is necessary to enable the institution, in line with the type of its activities, to clarify, assess, understand and manage the sanctions risk inherent to its activities. One of the main tasks of the sanctions risk assessment is to identify the risks associated with the possible circumvention of the sanctions regulation, where the sanctions screening is not sufficient to ensure effective observance of the sanctions regulation. At the same time, it is important to note that the sanctions screening is to be ensured irrespective of the risk rating, transaction amount and customer risk (except for intra-institutional transactions, *inter alia*, payments within the scope of a single institution, provided that a regular (at least daily) screening of the customer database is ensured.

18. Even though the MLTPF and the sanctions risk are different risks (for example, in terms of the MLTPF, a country located in the border area of the country subject to sanctions would not have an increased inherent risk (it would not, for instance, be considered to be a country with a high corruption risk or high risk of criminal offences), while, in terms of the sanctions risk, the same country, due to its location, would have an increased geographical risk related to the sanctions risk), the assessment thereof may, nevertheless, be performed concurrently, and the assessment of both of these risks may be combined in a single document.

19. When conducting the sanctions risk assessment, the institutions shall take into account the risk affecting circumstances (risk factors) both with respect to its customers and with respect to the risk inherent to its activities, services and the regions of the provision thereof.

20. The sanctions risk the institution is exposed to shall be determined, based on the mechanism similar to the one applied in analysing the MLTPF risk, namely, by assessing:

20.1. the inherent risk to which the institution is exposed prior to the application of sanction risk management measures;

20.2. the effectiveness of the sanctions risk management measures;

20.3. residual risk using the formula:

Inherent risk – effectiveness of the sanctions risk management measures = residual risk.

21. When determining the **inherent sanctions risk** characteristic to the activities of the institution, the institution shall determine the risk increasing factors inherent to its customer base and the activities of the institution itself, determining the inherent risk according to the rating thereof.

22. When determining **the effectiveness of the sanctions risk management measures**, the institution shall assess the measures applied by it in the risk management, in order to observe the sanctions requirements and to ensure that the sanctions risk increasing factors are identified (for example, systems and requirements for the screening of customers and their transactions, *inter alia*, payments). The institution shall assess (rate) each measure (for example, conforming, not conforming, significant improvement, insignificant improvement). Having obtained the rating of each individual measure, the institution shall determine the overall effectiveness of the measures. For example, it would not be permissible for the internal control measures to be assessed (rated) as effective, solely on the basis of the circumstances that there have been no cases detected with respect to a violation or circumvention of sanctions.

23. **Residual risk** shall be clarified after the inherent risk has been assessed and the applied sanctions risk management measures and the effectiveness thereof have been taken into account and rated. The institution shall rate the value of the residual risk, applying the risk value rating gradations.

24. Like in the MLTPF risk assessment, in the sanctions risk assessment it is also possible to apply various risk assessment matrices, depending on the activities, size, services offered by and the customer base of the institution (please see the principles of selection of the matrix in Sub-chapter 1.1).

25. The institution shall develop the plan of measures for ensuring the continuity of compliance of the ICS, entailing the sanctions risk and the MLTPF risk management measures.

26. The institution shall develop and document the sanctions risk assessment methodology. When developing the sanctions risk management and the AML/CTPF methodology, the institution may use the risk assessment guidelines developed by the international organisations, for example, Wolfsberg Group guidelines (available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf).

2. Internal Control System

27. After the institution has developed the MLTPF risk and sanctions risk assessments, it shall, in line with the conclusions of the assessment of these risks, establish, maintain and develop the AML/CTPF and the sanctions risk management ICS suitable to its economic activity.

2.1. Independence and effectiveness of the internal control system

28. The ICS shall be effective and independent, also paying attention to ensuring that the ICS ensures the fulfilment of the requirements of laws and regulations in a consistent and uniform manner with respect to all customers, *inter alia*, customers directly or indirectly associated with the stockholders of the institution, as well as the senior management of the institution. For example, when resolving upon the issues of the customers whose (ultimate) beneficial owner (hereinafter referred to as – the BO) is a person associated with the institution, the decisions taken would have to be the same as the ones that would be taken with respect to customers not associated with the stockholders or senior management (Executive, Supervisory Board) of the institution.

29. The institution shall ensure independent decision-taking, *inter alia*, the member of the Executive Board (or the representative authorised by the senior management) in charge of monitoring of the AML/CTPF, when taking a decision, shall ensure the prevention of conflicts of interest, and shall not take decisions with respect to an issue which involves or might involve conflicts of interest. The member of the Executive Board (or the representative authorised by the senior management) in charge of the monitoring of the AML/CTPF, when taking part in the work of the Executive Board and resolving upon the issues under the competence of the institution, shall primarily act from the perspective of the AML/CTPF field.

2.2. Three lines of defence

30. The credit institution shall implement the effective management of the MLTPF risk and the sanctions risk via three lines of defence. When establishing the ICS and developing the internal regulatory enactments, the credit institution and the investment firm shall prescribe the distribution of duties, powers, and responsibilities among the lines of defence.

31. The observance of the principle of three lines of defence is also ensured by other institutions if it is consistent with the scale and substance of the economic activity thereof.

32. The first line of defence is comprised of the employees of the institution involved in the creation and selling of the services and products or the customer, service and product operational support. Within the scope of the first line of defence, the structural unit may be created (or separate employees appointed), which shall perform the functions related to the MLTPF risk and sanctions risk management (for example, transaction monitoring, payment screening).

33. The duty of the first line of defence is to manage the MLTPF risk and the sanctions risk insofar as it is possible as a result of the customer service and product operational support (for example, the institution may prescribe in the policies and procedures that it shall be the duty of the first line of defence to identify certain indications of suspicious transactions that can be detected, when performing customer service on site, additionally setting the duty to report the identified facts to anther structural unit or employee organisationally located in the second line of defence; the institution may set a duty for the customer service specialist, when the customer arrives at the institution in person, to ascertain that the information required for the customer due diligence is updated, etc.). Institutions with a large number of customers may also define a duty for the first line of defence to carry out the customer due diligence or separate activities necessary for the performance thereof.

34. The second line of defence shall ensure the MLTPF risk and sanctions risk control function, inter alia, the second line of defence shall supervise the first line of defence. In addition, in line with the size and structure of the institution, the second line of defence may also perform the MLTPF risk and the sanctions risk management implementation measures, ensuring, for instance, transaction screening (for example, the institution shall define separate indications of suspicious transactions, the identification whereof is under the responsibility of the first line of defence, while the second line of defence shall be responsible for the performance of a comprehensive transaction screening process, being ensured via a special transaction screening system and analysis of the outcomes of supervisory scenarios). The duty of this line of defence is to conduct further enhanced, independent and comprehensive MLTPF risk and sanctions risk identification, measurement, evaluation, analysis and supervision, to regularly report to the management of the institution (both the Executive and the Supervisory Board) the outcomes of the assessment and to conduct the MLTPF risk and sanctions risk administration within the scope of its function.

35. The third line of defence is an internal audit, the duty whereof is to independently supervise the conduct of the first and the second lines of defence in managing the MLTPF risk and the sanctions risk.

36. In the policies and procedures the institution shall prescribe the duties and actions to be performed by the employees, in order to ensure the fulfilment of the requirements of laws and regulations, defining the functions under the responsibility of each of the three lines of defence. The institution shall allocate sufficient resources, to enable them to ensure effective fulfilment of the MLTPF risk and sanctions risk management function in accordance with the defined functions. The law requires that the institution's policies and procedures shall be approved by the board or senior management. This is necessary taking into account the impact of the MLTPF ICS on the prudential operation of the institution, including in the business area. It is permissible for the board or senior management to approve policies (for branches of institutions of other Member States in Latvia, it is permissible to approve the polices by the head of the branch, respectively providing for such delegation in the documentation of the activities of the institution), while the institution's procedures shall be approved by the board member responsible for MLTPF or a representative delegated in accordance with the competence.

2.3. Customer risk scoring system

2.3.1. Customer risk scoring system and the purpose thereof

37. The customer risk scoring system is the constituent part of the ICS, the purpose whereof is to assess the potentially inherent customer risk and to determine the risk management measures corresponding thereto. The customer risk scoring system reflects the MLTPF risk of the customer in numerical expression, applying the risk-based approach.

38. Customer risk scoring system shall serve as a tool for introducing the risk-based approach, when determining the customer due diligence measures and the scope thereof, pursuant to the inherent risk of the customer – both when commencing a business relationship (for example, the customer is subject to standard, simplified or enhanced customer due diligence), and during the business relationship (for example, prescribing the frequency of information updates, setting transaction screening measures consistent with the risk, etc.). This means that the customer with a

lower MLTPF risk is to be subjected to a smaller amount of, and less enhanced customer due diligence measures; in turn, in cases when the inherent customer risk is higher, the larger amount of, and more enhanced customer due diligence measures are to be applied.

39. Correct customer risk scoring system is important for the risk score calculated for the customer to be consistent with the customer risk, thus also ensuring appropriate customer due diligence and supervision measures.

<table>
<tr><td colspan="3">Example

Under seemingly similar circumstances, the risk is determined on a case to case basis:</td></tr>
<tr><td>Description of the customer and the activities thereof</td><td>Customer A – Limited Liability Company (hereinafter referred to as – the LLC) registered in Latvia, whose BO is a resident of Latvia, the type of economic activity is car sales – cars are being bought in the EU Member States and sold in Latvia, correspondingly, the cash flow is planned to these countries, as well as the cash transactions in the amount of up to EUR 5,000.</td><td>Customer B – LLC registered in Latvia, whose BO is a resident of a higher-risk country, the type of economic activity is car sales in Latvia - cars are being bought in Latvia and sold in the countries of a high corruption risk region, correspondingly, cash flow is planned from these countries with cash transactions in the amount of up to EUR 50,000.</td></tr>
<tr><td>Customer assessment of the customer risk scoring system</td><td>Lower than Customer B.</td><td>Higher than Customer A.</td></tr>
<tr><td>Risk increasing factors</td><td>Cash transactions.</td><td>The BO and counterparties (cooperation partners) are a non-EU and non-Organisation for Economic Cooperation Development Member State, cash transactions.</td></tr>
<tr><td>Factors affecting the differences in the score of the customer risk scoring</td><td colspan="2">Country of residence of the BO, region of the economic operation of the customer, planned cash transactions.</td></tr>
</table>

40. The customer due diligence regulations require that the institution, when developing this system, shall take into account the principles and risk-increasing and risk-reducing factors set out in the Law, the customer due diligence regulations and the EBA Guidelines (the customer due

diligence regulations include the basic principles for establishing a customer risk scoring system, while the Law and the EBA Guidelines include risk-increasing and risk-reducing factors).

41. The institution shall review the customer risk score whenever the current customer due diligence is carried out (the inherent (initial) customer risk rating is reviewed, by assessing the customer activities, executed transactions and the risk factors inherent thereto, if any emerge). For example, if the institution updates **a customer questionnaire, it ensures that the customer risk scoring corresponds to the customer's current MLTPF risk (the assessment can be performed manually or by automated supervision systems). If the customer's risk does not change, there is no need to formally review the customer's risk assessment.**

2.3.2. Core principles of the establishment of the customer risk scoring system

42. Customer Due Diligence Regulations prescribe the key requirements for the establishment of the customer risk scoring system; nevertheless each institution, considering its activities and the risks inherent thereto, may prescribe additional requirements, for example, include additional risk factors, in line with the specificity of its activities and risks inherent to cooperation with the customer[5].

43. Customer risk scoring system shall encompass:

43.1. risks and risk increasing factors specified in regulatory enactments and EBA Guidelines, **including the EU risk assessment and the national risk assessment of the Republic of Latvia;**

43.2. risks characteristic (inherent) to the institution itself or the service and products provided by it (for example, customers of the institution are associated with the stockholders), specific risks inherent to the services (for example, ensuring payment acceptance services to the providers of online dating services or foreign online gambling services).

44. The institution may also take into account the risk decreasing factors referred to in the EBA Guidelines or the Law, if the application thereof is consistent with the activities of the institution. If the institution takes into account the risk decreasing factors, then it shall be necessary to substantiate how and to what extent the relevant customer risk decreasing factor decreases the customer risk. It is not permissible that the sum of risk decreasing factors automatically (mathematically) **fully** decrease the score calculated by the customer risk scoring system (namely, the risk decreasing factors may reduce the customer risk, but the situation where the risk of the customer with an increased (higher) risk is reduced **in full** by the risk decreasing factors is not permissible).

45. The Customer Due Diligence Regulations provide for the development of methodology for the establishment of the customer risk scoring system, ensuring that the customer risk scoring system appropriately and effectively, in numerical expression, reflects the overall risk inherent to each customer. If the risk inherent to institution has changed, it shall assess the impact of the change on the methodology accordingly and update it as necessary (e.g., new risk factors).

---

[5] The Institution shall determine them if its activities are subject to risks or risk increasing factors that are not covered by the EBA Guidelines, typologies developed by law enforcement authorities, international or national risk assessments or the Law.

46. The purpose of the development methodology of the customer risk scoring system is to develop the evaluation of the activities and the customer base of the institution, in order to:

46.1. assess, which of the risk increasing factors refer to the institution and are applicable, considering the activities and the customer base of the institution;

46.2. identify the significance of risk factors and the score to be assigned to each risk factor, and to ensure that it is able to detect the cases indicative of an increased risk, and, correspondingly, to ensure the management thereof.

Example
The institution has prescribed that it is not offering trade financing products Consequently, the methodology may prescribe that the factors related to the provision of trade financing service shall not be assigned any score, at the same time ensuring that where the range of the offered services is changed, the methodology shall be reviewed and updated.

47. Based on the methodology, the institution shall set up the customer risk scoring system, prescribing the risk factors to be included therein.

2.3.3. Risk factors and assigning the score to risk factors

48. The Law prescribes the risk increasing factors, upon the occurrence whereof the institution shall perform the enhanced customer due diligence and in accordance with the requirements of Customer Due Diligence Regulations shall apply the enhanced due diligence measures to a corresponding extent. In turn, the EBA Guidelines include risk factors that an institution takes into account in its scoring assessment of customer risk in accordance with the MLTPF risk inherent to its activities. According to the customer's risk scoring assessment, the institution determines which customer due diligence measures are applicable (including whether simplified customer due diligence, standard due diligence or enhanced customer due diligence is sufficient and appropriate for MLTPF risk management). The enhanced due diligence, depending on the risk inherent to the customer or its transaction, is explained in detail in Sub-section 3.4.

49. The institution takes into account additional risk factors inherent to its activities and customer base[6].

50. The EBA Guidelines also entail the risk decreasing factors, in the event of the occurrence whereof the institution shall assess them and may take them into account, by reducing the sum of the risk factor score assigned to the customer.

51. If the risk factor specified in the EBA Guidelines refers to the institution (is applicable, in line with its activities, provided services, customer base), then the institution shall assign the respective score to the risk factor reflecting the impact of the risk factor on the overall inherent risk of the customer.

Example

[6] The institution shall prescribe such requirements, if there are risks inherent to its activities or risk increasing factors, not included in the Customer Due Diligence Regulations or the Law.

The customer, in line with the incorporation documents kept in the customer file, is entitled to issue bearer shares. The bearer shares shall be considered to be risk increasing circumstances, because the transfer of title takes place by transferring the shares.

The institution must assign such number of points to the referred to risk increasing factor that would enable identifying it and taking it into account, when determining the customer risk.

52. Risk increasing factors specified in EBA Guidelines and that apply to transactions are created as indications that may be indicative of an increased risk; nevertheless, the conclusion as to whether they increase the risk in the relevant case may be made, by performing the respective due diligence (Assessing the relevant indication). If the risk factor that may be inherent to the transaction refers to the institution and in essence increases the customer risk, it shall be assessed on an individual basis (to assess, whether, for example, the excess of the monthly, three-month or annual transaction thresholds increases the risk in essence, it shall be assessed, whether the excess of the thresholds is justified. For example, the customer sells medicinal masks and gloves. For example, sales before a pandemic are three times lower than at the beginning of a pandemic, during which demand for a customer's product increases significantly above pre-defined thresholds, which can be explained accordingly; the institution assigns a certain number of points to the risk factor and includes the customer's risk numerical evaluation system.

Example

Information or a request regarding the customer or the transactions thereof in connection with money laundering, terrorism financing or criminal offences is received from the correspondent credit institutions or other credit institutions or financial institutions where the institution has an account.

The institution may assign points to this factor automatically or depending on the outcomes of the customer due diligence, setting the term from the date of receipt of the request, during which the relevant indication is being taken into account, when performing the customer risk scoring (for example, to ensure the option to insert in the system the date of request from the correspondent bank and to provide for the setting of the customer risk scoring system so that the system still takes this date into account for a specified period of time). The institution shall determine the duration, for how long the indication should be taken into account, considering the customer risk. Upon the expiry of the prescribed term, the institution shall reassess the customer risk. Where there is a request from a correspondent bank received during this term and, having assessed the customer transactions, it is to be concluded that the transactions are indicative of the increase of the MLTPF risk, the institution shall renew the date and continue to include these factors into the customer risk scoring. If an increase of MLTPF risk is not detected, the institution shall not take this risk factor into account in the customer risk scoring.

53. Not all the risk factors inherent to a transaction automatically increase the risk and are to be included in the customer risk scoring system. The fact that the risk factor, in terms of essence, increases the risk, may be detected within the scope of the customer due diligence, i.e., after customer due diligence is performed and information is assessed. Respectively, if during customer

due diligence, it is detected that the risk factor impacts the customer risk, the institution shall review and update the customer risk after the performance of due diligence.

54. The EBA Guidelines prescribe the risk decreasing factors referring to the customer risk and service and product risk. The institution shall assign points to the risk factors that reflect the impact of the risk factor on the overall inherent risk of the customer. If the institution has prescribed that it takes into account the risk decreasing factors, then, upon the occurrence of the risk decreasing factor it may reduce the overall risk of the customer according to the significance (impact) of the factors. Points to be assigned may reduce the overall risk of the customer, but they cannot be such that, in terms of points (score), they exceed the score calculated by the system, by summing up the points assigned to the risk increasing factors (for example, if the system may assign the total score of 10 points to the risk factors corresponding to the customer risk, then the total score of risk decreasing factors may not achieve or exceed this score of 10 points), creating the situation that the risk of the customer is too low or the customer has no risk at all, because the score of the risk decreasing factors is being mathematically subtracted from the score of the risk increasing factors.

55. Any of the risk factor scoring algorithms referred to in the EBA Guidelines shall be formed so as to enable the institution to identify the inherent customer risks and to ensure that the risks are taken into account and their impact on the overall customer risk (the relevance) is determined, and such customer due diligence measures are taken, which are consistent with the risk. The assessment conducted by the institution, conclusions and justification thereof must be duly documented.

2.3.4. Exceptions (idiosyncrasies) in the establishment of the customer risk scoring system

56. If the institution, when developing the customer risk scoring system, detects any circumstances preventing full implementation of the prescribed requirements, in light of the idiosyncrasies of the setup of the IT system in the institution, or it cannot ensure system automation to the full extent (if the institution according to the requirements of laws and regulations has a duty to ensure the automation of the customer risk scoring system), it is necessary to address the Commission, in order to assess the relevant situation and solutions. Differences in the customer risk scoring system, *inter alia*, the level of automation thereof, shall be coordinated with the Commission. When addressing the Commission, it is necessary for the institution to specify the reasons underlying the impossibility of full implementation of certain requirements, so as to enable the Commission to assess the substantiation thereof. In addition, the institution shall prepare its own proposals for a possible solution. Information shall be prepared to an extent sufficient for the comprehensive assessment of the situation.

2.4. Governance

2.4.1. Employees in charge of AML/CTPF

57. In accordance with the Law the institution shall appoint one or several employees (persons in charge of the fulfilment of the requirements of the sanctions and AML/CTPF Law), incl., from

the senior management[7], entitled to take decisions and directly in charge of the observance of the requirements of the Law.

58. Credit institutions, licensed payment institutions and licensed electronic money institutions, as well as investment firms shall appoint the employee in charge of the fulfilment of the AML/CTPF requirements both in the senior management, ensuring the monitoring of the fulfilment of the AML/CTPF requirements, and in the internal control structural unit, performing the practical fulfilment of the referred to requirements (recommendations on the division of duties and responsibilities between the three lines of defence are contained in Subsection 2.2). It is recommended that this requirement is also observed by other institutions not mentioned herein above, if they have an increased inherent MLTPF risk, in order to ensure appropriate governance.

2.4.2. Qualification and conformity assessment of the responsible employees

59. The institution, in the MLTPF risk management document, shall prescribe the criteria for the adequacy of resources and the requirements for the adequacy of competence and qualification of the responsible officials.

60. The institution, in line with the size thereof, profile of activities and risk inherent to its activities, may set higher professional suitability criteria for the person in charge of the fulfilment of AML/CTPF requirements, for example, the need for international professional certificates in the AML/CTPF field or equivalent certificates.

61. To achieve the purpose of the law, protect the reputation of the institution, prevent the involvement of the institution in illegal activities, identify and prevent other risks significant for the institution, safeguard the secret of the customer transaction and occasional transaction, a person (who may be an employee of the institution or an attracted third party) or a structural unit specially appointed by the institution shall ensure an appropriate procedure for assessing the suitability of a person for the position of the member of senior management or the employee in charge of the observance of the requirements of the Law, *inter alia*, shall verify the authenticity of information provided by a person concerned (for example, self-assessment questionnaire).

62. In accordance with the requirements of the Commission's Normative Regulation No. 94 of 17 July 2020 "Regulations on the Assessment of the Suitability of the Executive and Supervisory Board Members and Key Function Holders" (hereinafter referred to as – Regulation No. 94) a person in charge of the fulfilment of the AML/CTPF requirements shall be considered to be a key function holder, and credit institutions and investment firms registered in Latvia shall conduct the assessment of both the members of the Executive Board performing the AML/CTPF monitoring and the persons in charge of the fulfilment of the AML/CTPF requirements in accordance with Normative Regulation No. 94, in line with the prescribed frequency of the assessment and the requirements for the suitability of the officials. In accordance with Regulation No. 94 the employee responsible for sanctions risk management is not included on the list of key function holders;

[7] Senior management is the Executive Board (board of directors) of the institution, if any is established, or a member of the Executive Board, official or employee specially appointed by the Executive Board, who has sufficient knowledge of the exposure of the institution to the MLTPF risks and holding a position of a sufficiently high level to take decisions concerning exposure of the institution to the abovementioned risks.

nevertheless the enumeration provided in Clause 2.2 of Regulation No. 94 is not exhaustive. The institution shall be entitled, having assessed the size, scope and complexity of the institution, to prescribe that the person in charge of sanctions risk management is also to be included on the list of key function holders[8]. Pursuant to Section 6, Paragraph three of the Law, this requirement is also applicable to branches.

63. For credit institutions, payment institutions and electronic money institutions it is necessary to inform the Commission about both the member of the Executive Board monitoring the AML/CTPF field and the person in charge of the fulfilment of AML/CTPF requirements, by submitting the relevant documents, *inter alia*, assessments of the officials, before the candidate for the position starts fulfilling his/her official duties or is re-elected to the same position.

64. The Law prescribes that the institution, within a period of 30 days after obtaining the status of the subject of the Law or the changes in the composition of the employees in charge of the observance of the requirements of the Law, shall inform the Commission to this effect. Credit institutions and other institutions with an increased risk inherent to their activities are invited to provide information to the Commission before the introduction of changes in the composition of the employees in charge of the fulfilment of AML/CTPF requirements to enable the Commission, in line with the risk assessment-based approach in the performance of supervision, to ascertain the prudent and well-reasoned activity of the institution (thereby it is possible to timely discuss the suitability of a person concerned and his/her vision of the issues under his/her responsibility). Credit institutions and other institutions with an increased risk inherent to their activities are invited to immediately notify the Commission of the planned termination of employment relationship with a person in charge of the observance of the requirements of the Law.

65. Considering the fact that the Law prescribes a duty of the institution to develop a procedure specifying the powers and responsibilities of the employee (incl., from the senior management) in charge of the observance of the requirements of the Law in the field of the AML/CTPF, and the procedure for ensuring the supervision of activities of the employee (incl., from the senior management) in charge of the observance of the requirements of the Law, it is important to prescribe the subordination of the relevant responsible employees and to ensure the independence of the responsible employees in taking decisions, as well as to prescribe the reporting duty and the reporting line in detail. Determination of detailed subordination, operational supervision and reporting duty is especially important for the group companies, *inter alia*, credit institutions, where such functions are determined at the level of the entire group.

2.4.3. Separation of risk control and compliance control functions

[8] In addition, the Institution may consult the Joint Guidelines of the European Banking Authority and the European Securities and Markets Authority on "Guidelines on the assessment of the suitability of members of the management body and persons performing key functions" (EBA/GL/2017/12), available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/1972984/43592777-a543-4a42-8d39-530dd4401832/Joint%20ESMA%20and%20EBA%20Guidelines%20on%20the%20assessment%20of%20suitability%20of%20members%20of%20the%20management%20body%20and%20key%20function%20holders%20%28EBA-GL-2017-12%29.pdf?retry=1.

66. Commission's Normative Regulation No. 227 of 1 December 2020 "Regulation on Establishment of the Internal Control System" (hereinafter referred to as – Regulation No. 227), setting requirements for the credit institutions and investment firms for the establishment of the ICS[9], prescribe the separation of the risk control function and the compliance control function, not only within the organisational structure of the credit institution, but also specifically at the level of the Executive Board. In accordance with Clause 19.3 of Regulation No. 227 the institution shall ensure the independence of persons performing internal control functions from the business functions, *inter alia*, it is ensured that the chairperson of the executive board is not concurrently in charge of the performance or monitoring of the duties of a person in charge of the fulfilment of the risk control function, compliance control function and AML/CTPF requirements.

67. It shall not be permissible to combine the functions of the head of the risk control function (risk director) and the functions of the head of the compliance control function under a single position. Derogations shall be permissible for the credit institutions that are less significant in terms of the size or nature of the activities thereof, or only for such credit institutions which have not been identified as other systemically important institutions (hereinafter referred to as – the O-SIIs), and only in the case if, by combining both of the referred to internal control functions, the credit institutions implement the requirements of Chapter IX of Regulation No. 227 to an extent ensuring the prevention of existing or potential conflict of interest situations in accordance with Clause 120 of Regulation No. 227. A credit institution not identified as O-SII shall, in any case, assess the application of derogation under the requirements of Clause 120 of Regulation No. 227, taking into account the size and nature of activities of the institution, *inter alia*, the level of business risks.

68. When assessing possible versions of combining the positions, when one and the same person holds several significant positions in the credit institution, in addition to one of the positions of the head of the internal control function, ensuring the observance of the requirements of Clause 118.1 and 118.2 of Regulation No. 227, it shall not be permissible that the relevant person not only fulfils the duties related to the controlled field of activity, but also, concurrently, fulfils the following functions:

68.1. Chairman of the Board;

68.2. member of the Executive Board monitoring the AML/CTPF field andappointed in the credit institution, by way of ensuring the fulfilment of the requirements laid down in Section 10, Paragraph 2 of the Law;

68.3. employee in charge of the AML/CTPF, appointed, by way of ensuring the fulfilment of the requirements laid down in Section 10, Paragraph 1 of the Law.

69. Derogations from that which is specified in Clause 68 shall only be permissible when the head of the compliance control function concurrently performs the functions of the position of the member of the Executive Board monitoring the AML/CTPF, if the holder of the position, in addition to the field of the compliance control function and the AML/CTPF field, is not in charge of the fulfilment of other significant duties in the credit institution.

70. Taking the essential role of the Chairperson of the Executive Board into account in taking business decisions, when implementing the requirements of Clause 118.1 of Regulation No. 227,

[9] It is recommended that the requirements of these Regulations would be, as far as possible, also considered by other institutions, with the increased MLTPF risk inherent in their activities.

the risk director, the person in charge of the compliance function and the Board Member in charge of the AML/CTPF may not concurrently perform the functions of the Chairperson of the Executive Board. In addition, by way of ensuring the requirements of Clause 118.2 of Regulation No. 227, the risk director, the person in charge of the compliance function and the Board Member in charge of the AML/CTPF cannot be directly functionally subordinated to the Chairperson of the Executive Board.

71. In accordance with Section 221, Paragraph 1 of the Commercial Law, an executive board (a board of directors) is the executive institution of the company, which manages and represents the company. Therewith, even though the Board Member in charge of the AML/CTPF monitors the field of the AML/CTPF in the institution, the Executive Board is generally responsible for the activities of the institution, incl., for the observance of the AML/CTPF requirements and appropriate MLTPF risk management.

72. In accordance with the requirements of the Commission's Normative Regulation No. 126 of 11 August 2020 "Regulations on Sanctions Risk Management" (hereinafter referred to as – the Regulations on Sanctions) the institution, when establishing the ICS for sanctions risk management, must determine the procedure for the appointment of the employee responsible for sanctions risk management, including his/her mandate in the implementation of sanction risk management measures. The employee responsible for managing the risk of sanctions shall be appointed to the second line of defence. Depending on the size of the institution, operational profile and risk volume thereof, the institution may resolve upon joining the official duties of the employee responsible for the AML/CTPF and the employee responsible for sanctions risk management, prescribing the duties and responsibilities in each of these fields. Nevertheless, the application of such an approach would not be advisable for a credit institution, namely, in the opinion of the Commission, based on the size of the credit institutions and the risks inherent thereto, it would be advisable that the employee responsible for AML/CTPF and the employee responsible for sanctions risk management is not one and the same person. Credit institutions are advised to appoint a separate responsible employee in each field, prescribing the duties, responsibility and subordination and ensuring the possibility for the responsible employees, if necessary, to report directly to the senior management of the credit institution. Correspondingly, different professional suitability criteria may also be set for the responsible employees of each field.

2.4.4. Committees for taking decisions on the increased risk customers

73. For the purposes of management of the MLTPF risks and taking decisions, the institution may establish various committees, which shall take decisions on the commencement of the business relationship with the increased risk customers, termination of the business relationship, performance of separate transactions, etc. When organising decision-takingin such committees, it would be necessary to level out the composition of the AML/CTPF specialists and the members representing other fields, in order to ensure well-considered and appropriate decisions. Considering the fact that such committees review the issues related to AML/CTPF, it is necessary for the institution to create such a decision-taking system, which ensures that the arguments of the specialists representing the AML/CTPF field are heard and assessed and the taking of a decision cannot take place without due assessment and justification, by adopting the decision merely by voting. The institution may prescribe various voting methods; however it is not permissible for the

adoption of the decision to take place, without assessing the considerations expressed by the members of the committee representing the AML/CTPF field, irrespective of the number of votes. It is essential that the decisions taken at the meetings of such committees are documented, thus enabling the fully-fledged fulfilment of the adopted decisions and the due follow-up of the fulfilment thereof.

74. Decisions taken by the committeesadopting the decisions on the commencement of the business relationship with increased risk customers shall not be automatically considered as equivalent to the decisions taken by the senior management, for example, with respect to the commencement of the business relationship with PEPs, where according to the requirements of the Law it is necessary to receive the consent of the senior management. Whether or not the decision of such committees on, for example, continuation of the business relationship with a PEP, can be equated to the consent of the senior management, depends on the composition of the committee, assessing whether the employees of the AML/CTPF field are represented therein, which position is held by them (with respect to the senior management, essential criteria is that the person has sufficient knowledge about the exposure of the institution to the MLTPF risks and the position of a sufficiently high level, in order to take decisions referring to the exposure of the institution to such risks), the procedure of voting and who has the casting vote in taking the decision.

2.5. Training

75. It is necessary to provide training in the field of AML/CTPF and sanctions for the employees of the institution, *inter alia*, **employees** of the branches of the institution **or representatives performing the functions related to the AML/CTPF and sanctions risk management**.

76. The institution shall prescribe the categories of employees, to whom the training in the field of the AML/CTPF and sanctions shall be provided. When ensuring training in the field of AML/CTPF and sanctions for the relevant employee categories, it is necessary to take into account the knowledge and qualification required for the official duties, responsibility and level of authorisation of the employees (for example, the employee performing enhanced customer due diligence should have the qualification suitable for such a duty, the employee performing customer service should have the appropriate knowledge and qualification in the field of AML/CTPF and sanctions insofar as necessary to be able to adequately conduct customer due diligence in accordance with the procedures (to notice the indications of suspicious transactions, ask additional questions, etc.). As the scope of issues topical for the training may differ, the institution may expand the scope of issues to be included in the training plan, considering the MLTPF risk inherent to the economic activity of the institution.

77. For separate employee categories it is necessary to ensure not only internal, but also external training. Commission's Normative Regulation No. 125 of 11 August 2020 "Regulations regarding the Provision of Staff Resources and Staff Training for Money Laundering and Terrorism and Proliferation Financing and Risk Management", setting the requirements for the provision of staff resources and staff training for the MLTPF risk management, prescribe that the credit institution shall ensure that regular external training, at least once a year, with the involvement of foreign experts (incl. Seminars organised by ACAMS with the participation of foreign experts) is

provided to the Member of the Executive Board responsible for AML/CTPF, the person responsible for the fulfilment of MLTPF requirements and staff of the internal audit structural unit whose official duties include the performance of the audit in the AML/CTPF field, promoting the understanding of the issues of the AML/CTPF field and the current trends in the application of the international AML/CTPF compliance standards. Even though the requirements of these Regulations are binding on the credit institution and their branches, the observance of the core principles is advisable for al institutions, for the purposes of ensuring that the institution conducts the measures necessary for the provision of staff resources and staff qualifications, as well as the training and replacement thereof according to the MLTPF risk inherent in the economic activity thereof, in order to manage the MLTPF and sanctions risk.

78. When planning the training, the institution should be guided by the risk assessment and shall assess what kind of external training is necessary for the employees, inter alia, the Member of the Executive Board responsible for AML/CTP, the employee responsible for sanctions risk management, the employee responsible for AML/CTPF, the employee of the internal audit structural unit, in order to ensure that the training is meaningful, feasible for the relevant employees and provides for new knowledge.

79. When planning the staff qualification requirements, the institution, based on the risk inherent thereto, may set qualification requirements, for example, for the employee responsible for AML/CTPF and the employee responsible for sanctions risk management to obtain international certificates in the relevant field, and to define the presence of such certificates as desirable for the Member of the Executive Board monitoring the AML/CTPF field.

80. Taking the specifics of the new employee's job responsibilities and experience into account, the institution shall provide the new employee with the necessary training to perform the tasks of the new employee. The field of AML/CTPF can be part of the overall mentoring.

2.6. Internal audit

81. The internal audit shall form a part of the entire ICS and it is necessary to also include in the inspection plan thereof, the issues related to the observance of the requirements of the Law in the institution. If the internal audit structural unit, within the scope of its inspections, detects that the institution does not pay sufficient attention to the observance of the requirements of laws and regulations in the AML/CTPF field, it should immediately report it to the management of the institution, because exactly the interest of the senior management in the effective observance of the requirements is essential, in order to reduce the possibility of the institution being involved in money laundering.

82. Considering the fact that in Regulation No. 227, the MLTPF and sanctions risk as the constituent part of the operational risk is defined as one of the material risks of the institution, the internal audit structural unit of the institution shall regularly verify and assess the compliance of the operation of the institution with its MLTPF risk and sanctions risk management strategy and the policies and procedures for the implementation thereof, and must report the outcomes of inspections to the Supervisory Board.

83. Irrespective of the fact that an independent audit of the institution has been performed, the internal audit shall also regularly perform the assessment of the effectiveness of the ICS. The purpose of the internal audit is not to repeat the external audit, but rather to ensure a more enhanced evaluation in the identified risk areas, as well as to ensure the follow-up of the fulfilment of the developed plan of measures.

2.7. Independent audit

This sub-chapter refers to credit institutions, licensed payment and electronic money institutions and branches of the Member State and third-country credit institutions and licensed payment and electronic money institutions in the Republic of Latvia, in line with the Commission's Normative Regulation No. 148 of 1 September 2020 "Normative Regulations on the Performance of Independent Assessment of the Internal Control System for Anti-Money Laundering and Countering Terrorism and Proliferation Financing", laying down the requirements for the performance of the independent assessment of AML/CTPF ICS. It is recommended that the aspects described in this sub-chapter are, as far as possible, also considered by other institutions, with the increased MLTPF risk inherent in their activities.

84. When performing an independent conformity assessment of the operation of the ICS of the institution, in order to form a comprehensive opinion on the conformity of the ICS, it would be necessary to apply a holistic approach – to assess both the requirements of policies and procedures (whether or not they encompass all the necessary MLTPF risk management requirements, for example, customer due diligence, incl., identification requirements, duty to report to the responsible authorities, and whether or not they conform to the risk assessment of the institution and its customers), and the effective practical implementation of policies and procedures, *inter alia*, to perform sample testing of customer files, for example, preferring to select customers causing increased risk for the credit institutions and licensed payment and electronic money institutions for the sample. The number of customer files to be verified would have to be determined in proportion to and commensurate with the total number of customers of the institution (i.e., the number of customer files to be verified would have to be determined to such an extent that enables one to make justified conclusions regarding the operation of the ICS of the institution). Merely sample testing of customer files may not be sufficient to make comprehensive conclusions as to the conformity of operation of the ICS of the institution.

85. When forming the opinion on the conformity of the ICS, it would be necessary to provide for an evaluation of the relevance of the detected deficiencies and flaws, as well as the provided recommendations, assessing their impact on risk management.

86. The independent assessor may only commence the audit after the receipt of approval of the Commission. In turn, the reference point of the audit period is considered the last date when the report on audit results is submitted to the institution.

87. It would be necessary for the institution, following the external assessment of the effectiveness of operation of the ICS of sanctions risk management, within a reasonable period of time, not exceeding three months from the date when the final audit report has been submitted to the institution, to develop a plan of measures for the prevention of the identified deficiencies and

shortcomings and a plan for the introduction of recommendations, to be approved by the Executive Board of the institution. Within one month from the approval of the plan by the Executive Board, the institution shall submit the plan to, and coordinate it with the Commission. The institution shall inform the Commission about the fulfilment of the plan at least once per quarter.

88. The Commission's full inspection is essentially the same as the assessment of an independent external audit, so the term of an independent audit, if the Commission has carried out the inspection, may be set by the Institution in agreement with the Commission, taking the Commission's inspection time into account.

3. Customer Due Diligence

3.1. General issues of customer due diligence

89. Customer due diligence is the risk-assessment based set of measures, within the scope whereof the customer is being identified and measures are taken for the purposes of clarifying the BO of the customer and the purpose and essence of the business relationship, as well as the customer transaction screening and updating of information obtained during the customer due diligence, and source data of customer due diligence is performed according to the customer risk, however at least once every five years. Depending on the customer due diligence measures based on risk assessment, customer due diligence can be divided into simplified due diligence, standard due diligence and enhanced due diligence.

90. Institutions shall ensure permanent transaction monitoring corresponding to customer risk, which does not replace customer due diligence (for example, transaction monitoring does not demonstrate the change in the ownership structure, the change of the BO, etc.), but forms one of the essential measures of customer due diligence, ensuring the timely detection of potentially suspicious transactions or transactions not typical for the customer. In cases where the customer has a low MLTPF risk (standard customer due diligence is conducted) and the turnover thereof consists of everyday household transactions, for example, only work salary or pension, and/or the volume of transaction is limited (for example, low maximum possible limit of turnover is defined for the customer) and the institution understands the customer transactions, and where no conditions for enhanced due diligence occur with respect to the customer, no risk increasing factors are being detected affecting the customer risk profile, no indications of potentially suspicious transactions or activity untypical for the customer are detected within the scope of transaction monitoring, ensuring, at least once every five years, the updating of the key information necessary for customer due diligence, applied in the MLTPF risk scoring of the customer, it might not be necessary to take any additional due diligence measures, during which the customer needs to fill out the customer due diligence questionnaire, observing the risk-based approach.

91. The purpose of customer due diligence is to clarify and know the activities of the customer with respect to the services provided by the institution, for the institution not to be involved in MLTPF. Within the scope of customer due diligence, the institution shall determine the customer risk and shall assess transactions performed by the customer through the services of the institution, for example, the customer, who has just started business relationship with the institution, transfers a significant sum into the account of the customer (the significance of the sum is determined by the institution, taking the outcomes of customer due diligence into account). In such case, based on the

risk assessment, the institution shall obtain information confirming the origin (source) of funds (if information about the transaction has not already been obtained during the initial due diligence).

92. Standard due diligence differs from enhanced customer due diligence so that in the case of standard due diligence no risk increasing circumstances are present and it is not necessary to verify information at all or it is necessary to verify it to a minimum extent, as well as the level of detail of information to be obtained and necessary for customer due diligence.

Example

Situation No. 1
The customer – natural person has specified in the questionnaire that he/she is a paid employee (expert in the field) in the local government of the Republic of Latvia, with the average monthly income comprising EUR 1,000. The customer is willing to open an account with the institution, in order to receive the work salary and to receive a mortgage loan. No risk increasing factors have been detected.

Conduct of the institution: when assessing information provided by such customer about the occupation of the customer and the need for the account, considering the absence of risk increasing factors, the institution may apply standard due diligence, during which it is sufficient to resolve upon the commencement of a business relationship, based on information provided by the customer, without verifying it (for example, it is not necessary to obtain additional information that the customer actually works in the local government).

Situation No. 2
The customer – legal person registered in a high-risk country, specifies in the questionnaire that it is willing to open the current account with the institution for the performance of investments. The economic activity thereof is the performance of investments and the key cooperation partners are enterprises registered in other higher risk jurisdictions.

Risk increasing factors – country of registration of the customer, country of registration of the partners of the customer, economic activity is not related to the Republic of Latvia.

Conduct of the institution: in such case it would be necessary for the institution to verify information provided by the customer, for example, by clarifying more detailed information regarding the planned investments, and to additionally ascertain the origin of funds.

93. In cases of standard due diligence, the degree of detail of information to be obtained is lower, compared to information to be obtained during enhanced due diligence. For example, when obtaining information on the customer's economic or personal activity, in cases of standard due diligence it is sufficient to clarify the customer's field of activity, region (for legal persons) or customer's occupation, employer, profession (for natural persons). When obtaining information about the key business partners, it is sufficient to clarify the payees and the payers, as well as the nature of the transactions to be performed (for example, for covering utility payments), if it is not possible to specify particular cooperation partners.

3.1.1. Scope of application of customer due diligence requirements

94. The regulatory framework for customer due diligence requirements is general, therefore its requirements are applicable to the extent applicable to the risks inherent to the customer. In conducting customer due diligence, the institution uses and evaluates information regarding the services it provides. This means that it obtains the information required by the customer due diligence requirements to the extent that such information is necessary in the context of the provision of services to assess the risk of MLTPF in relation to the services provided.

95. Information which, depending on the scope of the services they provide, may not be available to certain authorities:

95.1. account statements, tax return, statement from the employer or the State Social Insurance Agency – this information may need to be obtained as part of enhanced due diligence to the extent necessary to assess the customer's MLTPF risk in the context of financial services provided by the institution. For example, an insurance company providing life insurance services may need to obtain a statement from a customer's account when assessing the origin of a customer's contributions;

95.2. key business partner – this information is only applicable to transactions performed in the provision of specific financial services. If no cooperation partner has been identified for the customer within the framework of the provided services, the requirements for identification of the key cooperation partner will not apply. On the other hand, if an institution assesses the origin of financial resources and has information about the customer's business partner, it evaluates and takes this information into account when determining the MLTPF risk inherent to the customer;

95.3. Criteria for a group of connected customers – this information is assessed to the extent that it relates to the services provided, for example, a non-lending institution will not be subject to the criterion that the customer uses a loan secured by another customer's trust.

96. The principle of only extending the requirements to the services provided and the transactions performed by the customer is also applicable to the requirements of other customer due diligence, incl. the establishment of a customer risk scoring system. The institution shall only assess and include in the customer risk scoring system those risk factors that are materially attributable to the services it provides (for more information on the customer risk scoring system, see Sub-section 2.3).

3.1.2. Recognition and acceptance of customer due diligence results

97. According to Section 29, Paragraph 1 of the Law the institution has the right to recognise and accept the results of customer due diligence with respect to identification of the customer, the BO of the customer and the purpose and intended nature of the business relationship and occasional transactions that the credit institutions and financial institutions have conducted in Member States and third countries, if the conditions prescribed by Section 29, Paragraph 1 of the Law have been complied with. Thus, the institution does not automatically assume that another credit institution or financial institution has carried out the above-mentioned customer due diligence measures, but obtains the information and evaluates the customer due diligence as necessary according to the MLTPF risk (the procedure for obtaining information is provided in the institution's procedures). Namely, if the institution exercises these rights, then it shall ensure that the credit institution or

financial institution, whose customer identification and due diligence is recognised by the institution, transfers the relevant data immediately. **Recognition of the results of the customer identification and customer due diligence may be used as a source of information for customer identification and due diligence, if the institution agrees on the transfer of information (the form of the agreement is determined by the parties thereto).** For example, a subsidiary may recognise a parent's identification of a customer by obtaining a copy of the customer's identity document. The institution shall also be responsible for the fulfilment of the requirements of the Law in the case when it exercises the rights provided for by the Law to recognise and accept the results of customer due diligence.

98. Recognition of customer due diligence results is separable from off-site identification or the use of third party services for customer due diligence (Cabinet Regulation No. 392 of 03.07.2018 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer" (hereinafter referred to as – Cabinet Regulation No. 392) and Commission Regulation No. 4 of 05.01.2021 "Regulations on Cooperation with Third Parties and Claims for Business Relationship with Customers, the Identification or Research of Which Has Used the Services of a Third Party"). In recognising the results of customer due diligence, an institution relies on due diligence conducted by another credit or financial institution, while off-site identification and the use of third-party services are considered to be a way of providing the institution's services. For example, the measures taken by a credit institution that relies on the identification of a customer by its parent credit institution are separable and different in terms of rights and obligations from the off-site identification of customers (each process has its own requirements).

99. In recognising and accepting the results of customer due diligence, the institution shall assess the impact of the risk associated with the process on the customer's risk and, if necessary, decide on the application of risk management measures.

3.1.3. Scope and type of information necessary for customer due diligence

3.1.3.1. Scope

100. The customer due diligence measures shall be applicable, based on the customer risk assessment, and the institution in the policies and procedures shall set the types and the scope of the customer due diligence measures it applies to the customers of the relevant risk. Therewith, information to be obtained about the customer with a lower inherent risk will be of a smaller scope to the one to be obtained about the customer with a higher risk. For example, with respect to the customers, whose economic activity is not related to the Republic of Latvia or who operate in the transport sector and the economic activity thereof entails countries of high risk, or with respect to customers having a multi-tier ownership structure, which may initially be indicative of a higher risk, it will be necessary to obtain more information about a customer, who is, for example, a manufacturing company of the Republic of Latvia.

101. For the purposes of the performance of customer due diligence, the institution shall obtain information or documents, which substantially helps to understand the economic activity and the specificity of transactions of the customer. The institution shall ensure that it is able to justify how

the obtained information or documents explains the information necessary for customer due diligence.

3.1.3.2. Manner

102. Similar to the scope of information, the manner in which the institution obtains information necessary for customer due diligence may differ, as well. Based on the customer risk assessment, it may be a customer questionnaire, encompassing various questions for the purposes of obtaining information, which is justified and sufficient for the determination of the customer risk, as well as information from public and reliable sources, for example, commercial databases[10]. It is not necessary to request information from the customer in all cases. The use of a publicly available, reliable and independent source must be prescribed in the policies and procedures of the institution, specifying in more detail which sources the institution considers to be reliable. When determining whether or not the source is reliable and independent, aspects such as resources from which the source obtains information, frequency of information updates, person maintaining (operating) information source, etc. may be assessed. For example, information about the enterprises registered in the Republic of Latvia, *inter alia*, during the identification process, may be obtained from the Enterprise Register of the Republic of Latvia (hereinafter referred to as – Enterprise Register or ER), incl., commercial databases maintaining the information of the Enterprise Register; in turn, information about foreign residents may be obtained from the enterprise register database of the relevant country, for example:

EU Member State, Iceland, Liechtenstein, Norway	https://e-justice.europa.eu/content_find_a_company-489-en.do?clang=en
The UK	https://beta.companieshouse.gov.uk/
Ireland	http://www.cro.ie/ena/online-services-company-search.aspx
Cyprus	https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchForm.aspx?sc=0
Luxembourg	https://www.rcsl.lu/mjrcs/displayConsult Documents.do?removeList=true&isFromIndex=true&time=1231934766691
Switzerland	http://www.zefix.ch/zfx-cgi/hrform.cgi/hraPage?alle_eintr=on&pers_sort=original&pers_num=0&language=4&col_width=366&amt=007);
The Czech Republic	https://or.justice.cz/ias/ui/rejstrik
The Russian Federation	https://egrul.nalog.ru/#
Ukraine	https://usr.minjust.gov.ua/ua/freesearch
Estonia	https://www.inforegister.ee
Lithuania	https://rekvizitai.vz.lt/en/

[10] The use of commercial databases constitutes a significant tool for obtaining and verifying the customer due diligence information.

103. The institution, when requesting and obtaining any supporting information or documents from the customer during the customer due diligence, shall ascertain that this information or documents are related to the particular purposes of the customer due diligence (for example, justify the particular transaction, provide insight as to the education and experience of the customer, justify the origin of funds, etc.). The scope of information and documents obtained during customer due diligence must be justified and commensurate to the inherent risk of the customer or the transactions performed by them. The institution shall also document how the information and documents obtained by the institution justify the information necessary for customer due diligence (for example, the circumstances that the origin of funds has been clarified or that the determined BO is the BO of the customer).

Example

The customer-legal person has received the loan from the legal person's BO, concurrently also being the representative of the customer. The economic activity of the customer is clear to the institution and up to now there were no risk increasing factors detected with respect to the transaction. The institution is willing to clarify the essence of the transaction and the origin of funds; therefore it requests an explanation from the customer about the essence of the transaction and the statement of account of the natural person (the representative and the BO of the customer), from which the loan was received, for the period of the last year.

When detecting a transaction untypical for the customer, the institution shall, first of all, assess all the available information – the volume of the performed transaction and what volumes of transactions are characteristic for the sector where the customer operates, the allocation of funds, the amount of wealth of the BO, the duration of the entrepreneurial activity of the customer, etc.

By assessing the available information, the institution shall determine what kind of information is to be requested as the document supporting the origin of funds. For example, when requesting the statement of account, it would be necessary to determine a reasonable period for which the statement of account is to be provided for, and to assess whether there are any other possible documents or information sources, justifying the origin of funds, for example, explanation of the customer regarding the occupation of the representative and the BO, which can be ascertained through publicly available sources, for example, in the explanation it is specified that the BO of the customer owns the enterprise, whereon there is a publicly available information enabling one to ascertain the activities of the enterprise and the scope thereof.

104. From the information and documents obtained during customer due diligence it must be possible to obtain confidence that the institution knows the risks of the customer and takes appropriate measures for managing these risks. It is essential that information about the customer is collected and monitored purposefully in accordance with the risks, and not by merely gathering all possible information about the customer. It shall be necessary for the institution to document the justification that the information and documents at the disposal thereof justify the economic and legal purpose of the activities of the customer.

105. In assessing the customers operating in various sectors, the institution may also take into account the Guidelines for the Subjects of the Law on the Prevention of Money Laundering and

Terrorism and Proliferation Financing Monitored by the State Revenue Service prepared by the State Revenue Service, Chapter 7 whereof provides for a detailed explanation on the possibilities and typologies of money laundering in various sectors of operation. The Guidelines of the State Revenue Service are available at – https://www.vid.gov.lv/lv/vadlinijas.

3.1.4. High-risk third country and higher risk jurisdiction

106. With respect to the countries, laws and regulations apply both the term "high-risk third country" and the term "higher risk jurisdiction"[11]. In accordance with Section 1, Clause 12.[1] of the Law high-risk third countries are countries or territories where in the opinion of an international organisation or an organisation setting the standards in the field of AML/CTPF, there is no efficient system for AML/CTPF in place, including countries or territories which have been determined by the European Commission as having strategic deficiencies in the regimes for AML/CTPF, posing significant threats to the financial system of the EU. From this definition it derives that not only the list of high-risk third countries defined by the European Commission must be observed, but also other lists of international organisations setting the standards in the field of AML/CTPF or the countries having no efficient AML/CTPF system, for example Financial Action Task Force (hereinafter referred to as – FATF) high risk and other monitored jurisdictions (the list is available here: http://www.fatf-gafi.org/countries/#high-risk). In turn, the jurisdictions specified in Clause 2 b) – f), Paragraph 3, Section 11.[1] of the Law would have to be regarded as higher risk jurisdictions.

3.1.5. Determination of relation to a high-risk third country and a higher risk jurisdiction

107. When determining whether the customer (both natural and legal person) is related to a high-risk third country or a higher risk jurisdiction, the institution shall take into account and assess the criteria referred to in the EBA Guidelines:

107.1. jurisdiction in which the customer, the BO of the customer or the key cooperation partners of the customer are located;

107.2. jurisdiction in which the main economic activity of the customer, the BO of the customer or business activity of the key cooperation partners of the customer is carried out;

107.3. jurisdiction in which the customer, the BO of the customer or the key cooperation partners of the customer have essential personal or business activity links.

108. When determining the relation of a natural person to a high-risk third country or a higher risk jurisdiction, the institution shall assess at least the following elements - country of issuance of the personal identification document, country of residence of a person (if such information is available), residential address thereof.

109. Countries of the elements referred to in Clause 108 may differ, for example, the country of issuance of a personal identification document and the country of domicile is the EU Member State, but the country of residence is a higher risk country. In such cases the institution needs to assess risks, in terms of their essence, namely, to assess information obtained during customer due diligence – whether it is indicative of the fact that the customer risk is affected (increased) by a

[11] Clause 2 a), Paragraph 3, Section 11.[1] of the Law.

country not regarded as the country of residence of the customer (i.e., the country where taxes are paid), and this relation to that country increases the overall risk of the customer.

110. Where the relation of any of the elements to a high risk third country or a higher risk jurisdiction is detected, it is necessary to assess whether such link is to be regarded as indicative that the customer is related to a high risk third country or a higher risk jurisdiction, and correspondingly indicative of the higher risk of the customer.

Example

Situation No. 1
Natural person, whose:
1) country of issuance of the personal identification document – EU Member State;
2) citizenship is EU[12] Member State;
3) country of residence (i.e., country of tax payments) – EU Member State;
Based on publicly available information, a person has close personal links with the political elite of the country where a high corruption risk is present (widely available information in public sources about the long-term friendship of a person with the head of the state that has facilitated the commencement and carrying out of the economic activity of a person in the country where a high corruption risk is present).

Assessment.
Even though the relevant natural person has a personal identification document issued by the EU Member and his/her domicile is in an EU Member State, when determining whether or not the customer is related to a higher risk jurisdiction, it is necessary for the institution to also assess and take into account the available information about the private links of a person with the country where high corruption risk is present, which can still create a higher MLTPF risk in transactions with the relevant person, incl., with respect to the origin of funds used for the performance of the transaction.

If the relation to the higher risk country is detected, the institution, provided that the particular actual circumstances correspond to the conditions of indications referred to in the Annexes to the Customer Due Diligence Regulations (for example, association with the higher risk and the turnover of the customer), shall conduct enhanced customer due diligence.

Situation No. 2
Natural person, whose:
1) country of issuance of the personal identification document – country where high corruption risk is present;
2) country of residence (i.e., country of tax payments) – EU Member State;
3) the country of actual residence is an EU Member State.
Within the scope of enhanced due diligence, the institution concludes that the transactions of the customer are clear, no risk increasing factors were detected, no circumstances were detected

[12] Example contains the EU Member, but the same principle would also be applicable to the European Economic Area Member State or the OECD Member State.

that would be indicative of such links of the customer with the country where high corruption risk is present that would affect the customer risk.

Assessment.
Even though the relevant person has a personal identification document issued by the country where a high corruption risk is present, taking into account information obtained during enhanced customer due diligence and assessing whether or not the customer is related to a higher risk jurisdiction, there are no grounds to consider that the customer is related to a higher risk jurisdiction that might pose an increased MLTPF risk for the transactions with the relevant person.

3.1.6. Determination of relation to the Republic of Latvia

The Guidelines contain several risk factors, referring to the cases when the customer, its activities, are not related to the Republic of Latvia. This Chapter explains how to determine the relation to the Republic of Latvia.

3.1.6.1. Determination of relation for the customer-natural person

111. In determining whether or not the customer – natural person is related to the Republic of Latvia, the institution may apply criteria specified in the law On Taxes and Duties – the declared place of residence of the customer is in the Republic of Latvia, the customer is a Latvian citizen who is employed in a foreign country by the government of the Republic of Latvia, or the customer stays in the Republic of Latvia for 183 days or longer during any 12 month period.

112. The customer having a residence permit issued by the Office for Citizenship and Migration Affairs (for example, residence permit not exceeding six months), shall not be automatically considered as a resident of the Republic of Latvia. The customer may be considered to be a resident of the Republic of Latvia, if he/she has a residence permit issued in the Republic of Latvia and he/she has status in the Republic of Latvia (for example, resides, is employed in the Republic of Latvia, pays taxes to the State). When assessing whether the customer stays in the Republic of Latvia, the institution may take the following considerations into account:

112.1. whether a temporary residence permit or a permanent residence permit is issued to the customer;

112.2. whether the customer has a residential tenancy agreement and whether utility payments are paid for the relevant residence;

112.3. whether the customer owns real estate and whether utility payments are paid for it;

112.4. whether there is a statement from the employer of the customer registered in the Republic of Latvia, confirming that the customer is the employee of the relevant employer, whether there has been an employment contract concluded during the last three months between the customer and the employer registered in the Republic of Latvia;

112.5. whether there is a statement from the State Revenue Service regarding the tax payment performed by the employer of the customer;

112.6. whether there is a statement from the State Revenue Service regarding registration with the register of taxpayers and the actual status of tax payments;

112.7. whether there is a statement confirming that the customer studies in the educational institution of the Republic of Latvia;

112.8. whether there is a contract concluded with the educational institution of the Republic of Latvia, where the customer studies;

112.9. whether the customer has a declared residential address in the Republic of Latvia and it is confirmed by successful verification in the portal *Latvija.lv* (verification of whether the person is declared at the specified address).

3.1.6.2. Determination of relation for the customer-legal person

113. In determining whether or not the customer - legal person is related to the Republic of Latvia, the institution may apply the following criteria[13]:

113.1. the customer-legal person is the enterprise registered in the Republic of Latvia and actually operating in the Republic of Latvia (financial statements are being filed to the State Revenue Service), thus creating economic value in the Republic of Latvia, and at least one of the BOs or authorised persons (official) of the customer-legal person is a resident of the Republic of Latvia, in line with the criteria laid down in the Law On Taxes and Duties;

113.2. the customer-legal person is registered in a country other than the low-tax or tax-free country or territory or a high risk third country, and is an enterprise actually operating in the Republic of Latvia, having a provable economic activity in the Republic of Latvia and creating clearly measurable and recordable economic value, and at least one of the BOs of the customer-legal person is a resident of the Republic of Latvia, in line with the criteria laid down in the law On Taxes and Duties.

113.3. the customer–legal person is registered in a country other than the low-tax or tax-free country or territory or a high-risk third country, and is an enterprise actually operating, and the goods flow through the territory of Latvia (for example, there are enterprise warehouses in Latvia).

114. Considering the fact that one of the criteria for determining the relation to the Republic of Latvia is the circumstance that the legal person is an actually operating enterprise, cresting economic value in the Republic of Latvia, it is necessary for the institution to ascertain the presence of this criterion. To ascertain that the customer-legal person is an enterprise actually operating in the Republic of Latvia, creating economic value and having a provable economic activity in the Republic of Latvia, the institution shall collect information or documents to obtain confidence that the legal person is conducting an actual economic activity, whether or not it is economically justified and the legal person has links to the Republic of Latvia, by applying one or several of the following measures:

114.1. obtain information or documents sufficiently explaining the business operational model of the legal person;

114.2. obtain an annual financial report, audited by an external auditor, being independent from the legal person, from which sufficient understanding may be obtained regarding transactions performed by a legal person, and to establish whether the profit corresponds with the commercial activity and turnover of the legal person;

114.3. obtain information or documents confirming the actual movement of products and services within the framework of the commercial activity implemented by the legal person. If the

[13] The institution may also prescribe additional criteria.

activity of a legal person, considering the purpose of foundation thereof, is not related to the movement of products and services, information and documents should be obtained, confirming and describing the compliance of the activity of the legal person with the purpose of foundation thereof (for example, only holding of an asset in accordance with the business activity model);

114.4. obtain information or documents about the key cooperation partners of the legal person, confirming the actual commercial activity of cooperation partners;

114.5. obtain information or documents confirming that the legal person performs tax payments (tax declaration), if the regulatory enactments determine the obligation to pay taxes in the particular situation;

114.6. obtain documents confirming that the legal person has attracted other persons on the basis of a contract (such as employees, outsourcing providers), who actually organise and perform the duties that refer to the commercial activity of the legal person, making sure of the compliance of duties with the commercial activity and turnover of the legal person.

115. The circumstance where, within the group of connected clients, there is a link to the Republic of Latvia identified and documented for one of the participants thereof, shall not be considered to constitute the grounds for determination that all clients belonging to the group have a link to the Republic of Latvia.

3.1.7. Receipt of the management consent for cooperation with the customer related to a high risk third country

116. By implementing the requirement laid down in Section 25.[1] of the Law regarding the commencement or continuation of a business relationship, or performance of an occasional transaction with the customer related to a high risk third country, it is sufficient to only receive consent from the senior management once – before the establishment of a business relationship or performance of an occasional transaction, or when taking a decision to continue a business relationship with the customer from a high risk third country, where the relation of the customer to a high risk third country was detected during the cooperation.

117. The Law prescribes that for the commencement or continuation of a business relationship, or performance of an occasional transaction with the customer related to **a high risk third country**, consent from the senior management of the institution shall be necessary. In turn, the senior management is the Executive Board (board of directors) of the institution, ifany is established, or a member of the Executive Board, official or employee specially appointed by the Executive Board, who has sufficient knowledge of the exposure of the institution to MLTPF risks and holding a position of a sufficiently high level to take decisions concerning exposure of the institution to the abovementioned risks. Therewith, the receipt of consent from the senior management does not mean that it shall be necessary to receive the confirmation from the Executive Board in all cases, namely, consent may be given by a person, who has sufficient knowledge of the exposure of the institution to the MLTPF risks and holding a position of sufficiently high level to take decisions concerning its exposure to the abovementioned risks, i.e., the member of the Executive Board monitoring AML/CTPF. The purpose of the consent (acceptance) of the senior management of the institution is to ensure that the highest possible senior management level is informed about the business relationship with higher risk customers and the institution does not commence cooperation with such person, if there is no appropriate ICS in place.

118. When commencing or continuing a business relationship or performing an occasional transaction with the customer from **a higher risk jurisdiction**, it shall not be necessary to receive consent from the senior management. The institution, having assessed the risk, may set such requirement, however it is not mandatory in accordance with the Law.

Example The customer is from a country with a high corruption risk and studies in the Republic of Latvia. The customer is willing to open an account in the payment institution. In accordance with Section 25.[1] of the Law a country with a high corruption risk is not a high risk third country. Thus, in such case it shall not be necessary to receive consent of the senior management, in order to commence a business relationship with the customer (provided that no other circumstances exist, upon the occurrence whereof in accordance with the requirements of the Law or the internal requirements prescribed by the institution, consent of the senior management is necessary).

3.1.8. Sources that can be used in determining country risk

119. Publicly available sources that can be used in determining country risk (the list serves as an example only and is not exhaustive)

Low-tax or tax-free countries	https://likumi.lv/doc.php?id=294935
FATF country assessment	http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2018.html
	http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-october-2018.html
EU Commission list of high-risk third countries	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG
	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0105
	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R0212 https://ec.europa.eu/taxation_customs/tax-common-eu-list_en#heading_4
KnowYourCountry rating	https://www.knowyourcountry.com/country-ratings-table
USA Patriot Act 311 Special Measures (FinCen)	https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures

Major illicit drug producing or transit	https://www.whitehouse.gov/presidential-actions/presidential-memorandum-secretary-state-12/
Strength of auditing and reporting standards	https://tcdata360.worldbank.org/indicators/h1a88ca92?country=BRA&indicator=694&viz=line_chart&years=2007,2017
Corruption perception index	https://www.transparency.org/cpi2019?/news/feature/cpi-2019
Control of corruption	http://info.worldbank.org/governance/wgi/#home
Political risk/Risk of political violence	https://www.credendo.com/country-risk
Actual UN peacekeeping operations	https://peacekeeping.un.org/en/list-of-past-peacekeeping-operations
Regulatory quality	http://info.worldbank.org/governance/wgi/#home
Global Terrorism Index	https://ec.europa.eu/knowledge4policy/dataset/ds00160_en
Europol's information on terrorism-related risks	https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat

3.1.9. Assessment of the publicly available information

120. Within the framework of customer due diligence (inter alia, enhanced customer due diligence) the institution, based on risk assessment, shall also assess the publicly available information about the customer, the BO, the representative, the cooperation partner. It is important to assess materials containing not only positive, but also negative information (for example, it is not acceptable that the information available about the customer showing their prosperity, the enterprises owned by them working with profit, are taken into consideration and included in the customer's assessment, but information where a possible relation of the customer with fraud is indicated, is not mentioned and is not assessed).

121. When documenting the search and assessment of publicly available information, the institution shall be able to prove what parameters were used to search for the information (customer's name or name and surname, the name and surname of the customer's BO and the name and surname of the representative), on what websites the information was searched, what kind of information was detected, which employee searched and assessed the information, documenting the conclusions with respect to the results of the assessment.

Example
The institution has carried out two enhanced due diligence sessions with respect to the customer for different periods. Within the scope of the first due diligence, the institution specifies that no negative public information is found about the customer. In turn, within the scope of the second

due diligence, the institution has detected negative information about the customer (published after the performance of the first due diligence); however it does not take it into account, because it considers that such information does not refer to the due diligence period, namely, it refers to the previously assessed transactions.

It is necessary for the institution, upon the detection of negative information about the customer, to take it into account and to assess whether and in what way it affects the customer risk and further cooperation with the customer.

122. Search of publicly available information can be performed, for example, in *Google* or *Google Advanced Search* (https://www.google.com/advanced_search). In cases when the customer is related to the countries of the Commonwealth of Independent States, it is feasible to perform the search, for instance, in *yandex.ru* and in Russian.

Example

<u>For natural persons</u>
In Latvian:
- "vārds uzvārds" OR "uzvārds vārds" noziegums OR atmazgāšana OR terorisms OR sankcijas OR aizliegums OR sods OR nodokļi OR krāpšana OR apsūdzība OR arests OR pārkāpums OR narkotikas OR korupcija OR kukuļdošana OR skandāls

In English:
- "NAME SURNAME" OR "SURNAME NAME" crime OR launder OR terror OR sanction OR circumvent OR embargo OR penalty OR tax OR fraud OR charge OR arrest OR violate OR drug OR corrupt OR bribe OR scandal OR breach

In Russian:
- "ИМЯ ФАМИЛИЯ" OR "ФАМИЛИЯ ИМЯ" преступлен OR отмыв OR террор OR санкции OR обман OR запрет OR штраф OR обложить OR мошеннич OR обвинен OR арест OR наруш OR нарко OR коррупц OR взятка OR обман OR скандал

If the person has a father's name, for an additional search it is feasible to specify it along with the forename and surname.

<u>For legal persons</u>
In Latvian:
- "uzņēmuma nosaukums (bez juridiskās formas saīsinājuma)" noziegums OR atmazgāšana OR terorisms OR sankcijas OR aizliegums OR sods OR nodokļi OR krāpšana OR apsūdzība OR arests OR pārkāpums OR narkotikas OR korupcija OR kukuļdošana OR skandāls

In English:
- "Company name (excluding legal type)" crime OR launder OR terror OR sanction OR circumvent OR embargo OR penalty OR tax OR fraud OR charge OR arrest OR violate OR drug OR corrupt OR bribe OR scandal OR breach

In Russian:

- “НАИМЕНОВАНИЕ КОМПАНИИ” преступлен OR отмыв OR террор OR санкции OR обман OR запрет OR штраф OR обложить OR мошеннич OR обвинен OR арест OR наруш OR нарко OR коррупц OR взятка OR обман OR скандал

123. In cases when the firm name of the enterprise is widely used and with a commonly known meaning, it is feasible to also include the abbreviation of the legal form in the search.

3.1.10. Due diligence of the customer administered by the administrator of insolvency proceedings

This sub-chapter refers to credit institutions.

124. Taking into account the consequences and the impact of insolvency proceedings on the rights of a person to administer their property, attention must also be paid to the due diligence of a natural or legal person whose activities are administered by the administrator of insolvency proceedings. On the other hand, the administrator of the insolvency proceedings cannot, in essence, be equated with the legal or natural person he or she represents. Insolvency proceedings dramatically change the situation of an insolvent natural or legal person. For example, when performing enhanced due diligence of an insolvent person, it is necessary to carefully assess the circumstances and, possibly, it may no longer be required to carry out a screening of historical transactions, a study of the origin of funds, a study of the background of the BO and its well-being origin, the origin of financial resources and other relevant factors. However, it shall be borne in mind that each case shall be assessed on its own merits. According to the Insolvency Law, the administrator of the insolvency proceedings is a natural person who has been appointed to the position of an administrator and who has the rights and obligations specified in this Law. In essence, the main task of the insolvency administrator is to ensure the efficient and lawful conduct of the insolvency proceedings of a legal and natural person and the achievement of the objectives of the insolvency proceedings, i.e., covering creditors' claims from the debtor's property to facilitate the performance of the debtor's obligations or the satisfaction of creditors' claims from the debtor's property (in the event of the insolvency of the legal person), and enabling a debtor whose assets and income are insufficient to cover all obligations, to be released from obligations and to restore solvency (in the event of the insolvency of the natural person).

125. In accordance with the Insolvency Law monetary funds received by the administrator of insolvency proceedings, when administering the property of the debtor, shall be deposited in the debtor’s account in the credit institution. Also, after the declaration of the debtor's insolvency proceedings, the administrator acquires the right to manage the debtor's property (incl. Funds). Therewith, the administrator of insolvency proceedings has a statutory task to use the financial services of the credit institution.

126. When carrying out the due diligence of a natural or legal person administered by the administrator of insolvency proceedings, attention must be paid to the following circumstances:

126.1. in accordance with the Law, within the scope of the customer due diligence, the nature and purpose of transactions must be clarified. Business relationship involving the administrator of insolvency proceedings have a different purpose and nature to those of everyday business activities of legal persons. Thus, this circumstance must be taken into account when conducting customer

due diligence and resolving upon the impact of the results of the assessment and customer due diligence before the insolvency proceedings on the business relationship with the customer under insolvency proceedings;

Example
If before the insolvency proceedings, there was a person in the administration of the customer-legal person, with respect to whom information is available affecting the flawless reputation of the relevant person, the institution would have to assess the influence of the relevant person on the customer-legal person and its transactions during the insolvency proceedings. Therewith, the institution would take into account the circumstance that the customer-legal person, during the insolvency proceedings thereof, is no longer conducting the entrepreneurial activity characteristic thereto and the previous functions and rights of the administration thereof are transferred to the administrator of insolvency proceedings.

126.2. as to the issue regarding the BO of the customer administered by the administrator of insolvency proceedings, the institution shall exercise the rights provided for by the Law, correspondingly justifying and documenting the actions taken to determine the BO of the customer. The person holding the position in the senior management body of the legal person may be considered to be the BO of the relevant legal person, if all the possible means of clarification have been used and it is not possible to clarify any natural person – the BO, as well as doubts that the legal person or the legal arrangement has a different BO are excluded. In accordance with the Insolvency Law, the administrator of insolvency proceedings has all the rights, duties and responsibilities of administrative bodies provided for in laws and regulations, the articles of association of the debtor or in contracts. Considering the above mentioned, in cases where the credit institution is not able to determine the BO of the debtor and to obtain information about the BO as prescribed by the Law, the administrator of insolvency proceedings of the customer may be considered to be the BO of the customer.

127. In addition, it should also be taken into account that the administrators of insolvency proceedings are subjects of the Law and they have the task to carry out the activities inherent thereto and the MLTPF risk assessment of their customer, as well as to establish the ICS of the AML/CTPF. Within the scope of the above mentioned, when conducting the assessment of the customer administered by the administrator of insolvency proceedings, the institution, in line with the risk-based approach, shall take into account and assess the measures taken by the administrator him/herself for the observance of AML/CTPF requirements.

128. Credit institutions should take into account the fact that the sole purpose of an account opened at the request of the insolvency administrator in the context of the insolvency proceedings of a legal person is to carry out activities related to the recovery of creditors' funds, the receipt of a deposit or the sale of stocks. In cases where it is established within the insolvency proceedings that the legal person has no assets (so-called empty proceedings) and the current account is only needed to secure the administrator's remuneration, it would not be appropriate to open a current account with a credit institution in the name of the legal person concerned, but the administrator's remuneration could be paid to the administrator's account for economic activities. However, in certain cases, the administrator may also act in its own interests, which may result in initiating the

criminal proceedings. In order to manage this risk, the transactions of the insolvency administrator shall be monitored.

3.1.11. Shell arrangements

129. In accordance with Clause 15.[1], Section 1 of the Law the shell arrangement is a legal person characterised by one or several of the following indications:

129.1. has no affiliation of a legal person to an actual economic activity or the operation of a legal person forms minor economic value or no economic value at all, and the subject of the Law has no documentary information at its disposal that would prove the contrary;

129.2. laws and regulations of the country where the legal person is registered do not provide for an obligation to prepare and submit financial statements for its activities to the supervisory institutions of the relevant state, including the annual financial statements;

129.3. the legal person has no place (premises) for the performance of economic activity in the country where the relevant legal person is registered.

Example

Situation No. 1

An enterprise registered in a country, the laws and regulations whereof do not provide for an obligation to submit financial statements, has declared that it is engaged in the trade of goods (household appliances), but the enterprise has no warehouse, nor can it submit any documents supporting the movement of goods (consignment notes (CMR), bills of lading, etc.), selling prices of goods specified in the contracts are identical to the prices of procurement of goods, there are no transactions in the account of the institution evidencing tax payment, etc.

Situation No. 2

In accordance with information provided by the customer in 2017, a country with high corruption and sanctions risk is specified as the actual place of conducting economic activity, the customer employs five persons. In 2019, the customer informed the institution that the actual place of conducting economic activity has been changed, and submitted the lease agreement concluded in 2018, specifying that the actual place of conducting economic activity of the customer is in a country considered to be a low-tax country. The customer questionnaire completed by the customer in 2019 specifies that five persons are employed – director, secretary, chief financial officer, chief commercial officer and accountant. Upon the receipt of the referred to information from the customer, the status of a shell arrangement granted to the customer is cancelled.

Within the scope of enhanced due diligence, in order to ascertain whether the customer is attempting to avoid being classified as a shell arrangement, it is necessary for the institution to assess at least the following considerations:

- whether the five employees specified by the customer have the necessary permits to work in the country specified as the place of conducting economic activity;
- whether the number of employees is adequate for ensuring the economic activity of the customer (for example, whether the referred to five employees are able to ensure trade in oil and oil products);

- considering the fact that, following the change of the actual address, the activity of the customer has not changed and it is related (affiliated) to a country considered to be a low-tax country, and the actual activity is still being conducted in a country with high corruption and sanctions risk, it is necessary to assess the functions for the performance whereof the customer is leasing the premises in a country considered to be a low-tax country, if, in fact, the entire economic activity is being conducted in another country (for example, by assessing the submitted lease agreement and analysing whether it contains any indications demonstrating a merely formal contract).

130. Credit institutions, payment institutions, electronic money institutions, investment brokerage companies, and, in relation to the management of individual portfolios of customers and the distribution of certificates of open investment funds, investment management companies are also prohibited from commencing and maintaining a business relationship and conducting occasional transactions with the shell arrangement, if it concurrently conforms to the indications specified in Sub-clauses "a" and "b" of the definition of a shell arrangement (Section 1, Clause 15.[1] of the Law).

131. To determine whether the legal person conforms to the indication contained in Sub-clause "a", Clause 15.[1], Section 1 of the Law (Clause 129.1), the institutions referred to in Clause 130, based on the risk assessment, shall take one or several measures referred to in Clause 40 of the Customer Due Diligence Regulations[14]:

131.1. obtain information and documents sufficiently explaining the business model of the legal person;

131.2. obtain the annual financial report of the legal person, audited by an independent external auditor, from which sufficient understanding may be obtained regarding transactions performed by the legal person, and to establish whether the profit corresponds to the commercial activity and turnover of the legal person;

131.3. obtain information and documents confirming the actual movement of products and services within the framework of the commercial activity implemented by the legal person. If the activity of a legal person, considering the purpose of foundation thereof, is not related to the movement of products and services, information and documents should be obtained, confirming and describing the compliance of the activity of the legal person with the purpose of foundation thereof (for example, only holding of an asset in accordance with the business model);

131.4. obtain information and documents regarding key cooperation partners of the legal person, confirming the actual commercial activity of cooperation partners;

131.5. obtain information and documents confirming that the legal person performs tax payments (tax declaration), if the regulatory enactments determine the obligation to pay taxes in the particular situation;

131.6. obtain information and documents confirming that the legal person has attracted other persons on the basis of a contract (such as employees, outsourcing providers), who actually organise and perform the duties that refer to the commercial activity of the legal person, making sure of the compliance of duties with the commercial activity and turnover of the legal person.

[14] The Commission has developed Clause 40 of the Customer Due Diligence Regulations in accordance with Paragraph 2, Section 21.[1] of the Law, and Clause 40 is applicable with respect to the indication "a" of the definition of a shell arrangement.

132. The Customer Due Diligence Regulations prescribe the minimum measures to be taken by the institution, in order to verify whether the customer-shell-arrangement is affiliated to an actual economic activity, whether the operation of a customer forms minor economic value or no economic value at all.

133. The conformity to the indication of the shell arrangement specified in Sub-clause "a", Clause 15.[1], Section 1 of the Law shall be assessed individually, on a case by case basis.

Example Where a customer is a holding company, which owns the shares of other companies (subsidiary undertakings) and whose main task and purpose of economic activity is to carry out the management of the respective investments and assets, it must be assessed whether the subsidiary undertakings owned by the holding company conduct an actual economic activity, whether the group structure is transparent and is not indicative of an attempt to conceal the BO.

134. In cases where the customer, who is registered in the Republic of Latvia, does not conduct actual economic activity or the operation thereof forms minor economic value or no economic value at all, and there is no documentary information at the disposal of the institution that would prove the contrary (for example, there are suspicions that an enterprise is being used for tax evasion schemes, the institution shall terminate the business relationship with the relevant customer, reporting the suspicious transaction to the Financial Intelligence Unit (hereinafter referred to as – the FIU). This requirement would not apply to customers who are inactive and where the institution is satisfied that the termination is justified (e.g., reorientation of operation).

135. The institution shall determine the scope, nature and assessment principles of information and documents to be obtained, both depending on the MLTPF risk (such as legal form, structure of owners), country and geographical risk, the used services and products risk, services and products delivery channels risk, and depending on the type of economic activity of the legal person area of activity, the duration of activity and legal status, namely, considering various categories of legal persons.

136. As regards the indication of the shell arrangement under Sub-clause "c", Clause 15.[1], Section 1 of the Law, the Commission has detected in its inspections that the place of conducting economic activity of the legal person may also not coincide with the country of registration thereof, and the legal person should not be automatically considered to be a shell arrangement merely because of that. Taking the specific nature of activity of a legal person into account, the possibilities of remote work are being used increasingly more often (for example, companies performing translation services, providing IT services to the enterprises of other countries); therefore, it should be additionally assessed, whether the nature of economic activity of the legal person justifies the circumstance that the legal person has no place (premises) for the performance of economic activity in the country where the relevant legal person is registered[15]. In turn, the purpose of the indication of the shell arrangement under Sub-clause "c", Clause 15.[1], Section 1 of the Law is to classify as a

[15] For the purposes of solving the current situation, the Commission has filed proposals for introducing amendments to the Law, by supplementing Sub-clause "c" of Clause 15.[1], Section 1 of the Law.

shell arrangement, those legal persons, which operate as letterbox companies without any clearly understandable economic activity.

3.2. Customer identification

3.2.1. On-site identification

137. On-site identification shall be considered to be an identification procedure carried out by the employee or authorised person of the institution (for example, an agent, with whom the institution has concluded the agreement on customer identification in the interests of the institution, or a representative, who, within the provision of payment services, acts on behalf of the payment institution or is entitled to distribute or redeem electronic money on behalf of the electronic money institution), with the customer being present in person (physically) during the identification.

138. On-site identification shall also be considered to be identification, during which the sworn notary of Latvia has in person identified the principal and the attorney and the attorney arrives in person (on-site) to the credit institution for the establishment of a business relationship, based on the power of attorney issued by the principal. With respect to the identification of the principal performed by the notaries of other countries, the institution shall assess the country risk, ascertain the regulation of the particular country with respect to the authorisation and functions of the notary, verify and assess whether the notary has identified the principal and the attorney and how, as well as whether the identification corresponds to the requirements of the laws and regulations of the Republic of Latvia. A notarised and certified copy of a personal identification document per se without a notary's certification that the notary has performed the verification of the identity (identification) of the holder of the personal identification document is not sufficient to identify the customer.

139. The institution shall prepare the copies of the documents underlying the performance of on-site customer identification.

3.2.1.1. On-site identification of natural persons

140. When identifying the natural person on-site, the institution shall compare the visual similarity of the customer with the photo image contained in the presented personal identification document and shall ascertain that the document does not contain the features of a forged document. In case of doubt and if the institution is not able to ascertain that the customer presenting the personal identification document is the person depicted in the photo image of the document, or if the institution is not able to ascertain that the document does not contain the features of a forged document, it shall not commence cooperation with the relevant customer and, in line with the requirements of the Law, in the case of suspicions regarding the MLTPF, shall report to the Financial Intelligence Unit.

141. A natural person resident shall be identified on-site by verifying their identity on the basis of the customer's identity document, which includes information on the customer's name, surname and personal identification number. Information about the samples of identity documents issued by the Republic of Latvia is available in Cabinet of Ministers Regulation No. 134 of 21 February 2012 “Regulations Regarding Personal Identification Documents”.

142. During the identification process of the customer – foreign resident, a document recognised as valid for entering the Republic of Latvia may be used, which includes the customer's name, surname, date of birth, person's photograph, the number of the identity document and the date of issue, the country and institution that issued the document. Travel documents of foreigners shall be recognised as valid for entering the Republic of Latvia according to the requirements of Cabinet of Ministers Regulation No. 141 of 4 March 2021 "Procedures for the Recognition of Travel Documents of Foreigners".

143. In cases where a person has the right to enter and stay in the Republic of Latvia with an identity document valid for travelling and a valid visa or residence permit issued by the Republic of Latvia, the institution shall not only make a copy of the identity document, but also of the visa or residence permit, as it confirms the customer's rights to enter the country.

144. There may be cases when an identity card of a third country citizen is a residence permit issued by the Republic of Latvia (a temporary residence permit or a permanent residence permit) that is issued in accordance with the regulatory legislation governing the movement of persons. Thus, in cases when the customer has received a residence permit in Latvia in the form of an identity card, their identification may be conducted based on the residence permit.

3.2.1.2. On-site identification of legal persons

145. A legal person, in accordance with the requirements prescribed by the Law, shall be identified on-site by obtaining the document confirming the firm name, legal form and incorporation or legal registration of the legal person, obtaining details about its registered address and the place of actual performance of economic activity (if the actual address differs from the registered address), as well as by obtaining the incorporation document of the legal person and identifying the persons entitled to represent the legal person in the institution.

146. As specified by the Law the institution is entitled to obtain documents certifying the establishment or legal registration of the customer's legal person from a publicly available reliable and independent source, and such use of the sources shall be determined in the policies and procedures of the credit institution. Information about the enterprises registered in the Republic of Latvia may be obtained from the Enterprise Register, incl., commercial databases maintaining the information of the Enterprise Register; in turn, information about foreign residents may be obtained from the enterprise register database of the relevant country.

147. When commencing a business relationship or performing an occasional transaction, in cases where a customer is a legal person registered abroad and has been operating for a longer time (at least one year), in addition it is also necessary to obtain documents proving the relevance of the data obtained as a result of customer identification and which are made no earlier than a year before the commencement of the business relationship (for example, by requiring the customer to submit a certificate from a register, should it be impossible to obtain it from the relevant database of the enterprise register of the country of registration of the customer, issued no earlier than a year ago, about its status or other type of a certificate containing information on the status of the customer

(active or dissolved company) and the structure thereof (for example, Incumbency Certificate, Certificate of Good Standing)).

148. In the case if the director of the customer, which is a legal person, is a legal person, the institution shall pay attention to the status of this legal person and assess it as well (active or dissolved company). In order to ascertain this, the institution shall require the customer to provide a document certifying the signatory powers of the representative of the legal person, which is the director of the customer, and a document certifying the status of the company, which is the director of the company, that is not more than one year old (for example, Incumbency Certificate, Certificate of Good Standing).

3.2.1.3. On-site identification of legal arrangements

149. Legal arrangement, in line with the requirements laid down in the Law, shall be identified, by requesting the documents attesting to the status of the legal arrangement, the purpose of creation thereof, and its firm name, obtaining details about the registered address and the place of actual performance of economic activity thereof (if the actual address differs from the registered address), as well as by clarifying the structure and mechanism of governance of the legal arrangement, including the BO or the person in whose interests the legal arrangement has been created or operates, and the authorised persons of the legal arrangement or other persons holding an equivalent position.

150. Based on the risk assessment (for example, a higher geographical risk is inherent to the customer with respect to the country of registration), regarding the customer registered abroad and having nominal stockholders - legal persons[16], the institution shall obtain the documents issued no earlier than a year ago and attesting to the active status of a nominal stockholder, (for example, Incumbency Certificate, Certificate of Good Standing).

3.2.1.4. Verification of the personal identification document in the register

151. In accordance with the Law, upon verifying the identity of a natural person according to the personal identification document of the customer, the institution shall ascertain that the personal identification document is not invalid, by means of available public registers of the relevant country (for example, the Invalid Document Register). Within the scope of such verification, the institution shall verify the number of the personal identification document submitted by the customer, shall ascertain that the document has not been stolen, lost, perished, withdrawn and that it is not used by a third person etc. As regards a customer who has a personal identification document issued abroad, the institution may use the databases of the relevant country, if any (for example, in Russia – http://services.fms.gov.ru/info-service.htm?sid=2000, in Ukraine – https://nd.dmsu.gov.ua/), but it is advisable to at least verify the number of the machine readable zone of the issued document (for example, by using commercial databases). When verifying the genuineness of the personal identification document, the institution may use publicly available information (for example, http://www.consilium.europa.eu/prado/en/search-by-document-country.html) or commercial databases offering information about the types of personal identification documents in different

[16] The customers, for the registration whereof the services of the legal incorporation enterprises are used, create an increased risk with respect to the possible formal specification of the BO.

countries. At the same time, when identifying the customer, the institution, in addition to the verification of the personal identification document in the register, must pay attention to the legal effect of identification documents – to ascertain that the personal identification document is valid, the term of validity thereof has not expired, it is not damaged and does not contain the features of a forged document.

3.2.1.5. Updating personal identification document data

152. The requirement to update the data of personal identification documents shall apply to all customers of the institution; however the frequency of updates and the type and scope of information to be obtained shall be determined, based on the MLTPF risk assessment.

153. In order to update personal data, the following measures are taken for existing customers:

153.1. obtain updated identity documents using one of the following methods:

153.1.1. any channel for obtaining a copy of an identity document in person (branches) and in absentia (Internet bank, post office, e-mail, etc.) without additional notarial or other type of confirmation (electronic signature);

153.1.2. public or state registers (for example, the Office of Citizenship and Migration Affairs);

153.2. verify the updated identity documents using a risk-based approach, if verification is possible (for example, it may be performed as an additional control element if such a possibility can be provided in one of the state registers or in the case of non-residents – if it is possible to provide it in one of the external service providers in relation to the registers of countries other than Latvia);

153.3. decide on the application of restrictions (for example, new credit agreements are prohibited, but payments, account and payment card use are not restricted) for services, if this is necessary for MLTPF risk management (for example, significant changes in the identity document – change of name, surname, change of citizenship, etc.; suspicion (signs) of forgery of the document).

Example

A citizen of the Russian Federation does not live in Latvia, but it owns real estate in Latvia, the management of which (rent payments, utility payments, etc.) requires an account in Latvia. It is allowed to obtain a copy of the updated identity document by sending it to the Internet bank or by e-mail. The credit institution shall verify the coincidence of the data of the updated identity document (date of birth, place of birth, name, surname, etc.) with the data of the previous identity document and shall continue cooperating with the customer without any restrictions.

154. Regarding natural persons – residents of the Republic of Latvia, one of the ways of obtaining the updated information is by the institution itself obtaining the information about the existence and validity of a new valid personal identification document of the customer from the public register maintained by the Ministry of the Interior of the Republic of Latvia. At the same time, it is necessary to ensure that there is documentary evidence at the disposal of the institution as to how the relevant information was obtained (for example, by preserving a printout or other information attesting to how the relevant information was obtained and when).

155. One of the possibilities for how to achieve the updating of the data in the personal identification document is to set restrictions for the receipt of the services to the customers who need to update the data of the personal identification documents, for example, by restricting transactions in the internet bank, limiting the range of services and conclusion of new service agreements. Nevertheless, such restrictions must be justified by the risk assessment and the application of restrictions must be commensurate to the risk inherent to the customer; for example, the customer has a high inherent MLTPF risk and the customer performs regular transfers to the higher risk countries via the internet bank.

It is neither necessary, nor justified to set the restrictions for the receipt of the services automatically to all customers.

156. Before taking any of the measures for updating the data of the personal identification document, it shall be necessary for the institution to assess the risks caused by the customer – geographical risk pertaining to the customer, economic or personal activity of the customer, services and products to be used and the delivery channels thereof, as well as the performed transactions, by ascertaining whether there are any riskincreasing factors present requiring the performance of repeated customer identification on site.

3.2.2. Off-site (remote) customer identification

157. Off-site identification shall be performed in accordance with Cabinet Regulation No. 392 or Section 23 of the Law. If the off-site identification is performed in accordance with Section 23 of the Law, the enhanced customer due diligence shall only be performed in the cases specified in Section 22, Paragraph two of the Law.

158. When commencing the off-site identification of customers, the FATF Guidelines "Digital Identity" may be useful; the Guidelines are available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html.

159. The Commission has provided recommendations for non-face-to-face customer identification in the "Recommendations for Non-face-to-face Customer Identification" (available at: _____)[17]. The referred to recommendations for Non-face-to-face Customer Identification can be used not only by credit institutions, but also by other institutions, insofar as that which is stated therein is applicable to the activities of such institutions.

3.3. Simplified customer due diligence

3.3.1. Conditions for applying simplified customer due diligence

160. In accordance with Section 26 of the Law the institution may carry out simplified customer due diligence:

160.1. if a low MLTPF risk is present which is not in contradiction with the risk assessment, including the national MLTPF risk assessment report, and measures have been taken to determine, assess and understand the MLTPF risks inherent to its own activities and the customer, as well as

[17] The Commission's recommendations for non-face-to-face identification are also expected to be adopted in the near future, and a reference to these recommendations is planned in the handbook.

if the customer is the Republic of Latvia, a derived public person, direct administration or indirect administration institution, or a capital company controlled by the State or a local government characterised by a low MLTPF risk;

160.2. if there is a low MLTPF risk and the customer is a merchant whose shares are listed on a regulated market in one or more Member States;

160.3. if the customer is the Republic of Latvia, a derived public person, a direct administration institution or an indirect administration institution, or a capital company controlled by the state or local government, which is characterised by a low MLTPF risk;

160.4. if a low MLTPF risk is present and the services provided by the institution conform to all the indications referred to in Clauses of Paragraph 3, Section 26 of the Law, namely:

160.4.1. the transaction has a written contractual base;

160.4.2. the transaction is executed, using a bank account which is opened by a credit institution registered in a Member State;

160.4.3. the transaction does not arouse suspicions, or no information is available that attests to MLTPF, or an attempt to carry out such actions;

160.4.4. the total amount of the transaction is not more than EUR 15,000 or is in a foreign currency which in accordance with the exchange rate to be used in accounting at the beginning of the day of the transaction is not more than EUR 15,000;

160.4.5. the income from the transaction cannot be used for the benefit of third parties, except for in the case of death, disability, obligation to provide subsistence or in similar events;

160.4.6. if at the time of the transaction the conversion of funds into financial instruments or insurance or any other claims is impossible, or if such conversion of funds is possible and the following conditions are conformed with:

160.4.6.1. the income from the transaction is only realisable in the long term – not earlier than after five years from the day of entering into the transaction;

160.4.6.2. the subject-matter of the transaction cannot be used as collateral;

160.4.6.3. during the term of validity of the transaction no early payments are made, the assignment of the claim rights and early termination of the transaction are not used;

Example

The institution, when providing payment initiation or account information services, must apply the customer due diligence measures using a risk-based approach, and the inherent MLTPF risk of the services is to be assessed as limited, considering the fact that the payment initiation service provider, even though it is engaged in the payment chain, is not itself holding the funds of the user of payment services, with whom it, based on the selected cooperation model, creates an occasional business relationship or a business relationship, and the account information service provider is not involved in the payment chain and does not hold the funds of the customer.

The above-mentioned means that in the majority of cases the MLTPF risk would have to be assessed as low, namely, the simplified due diligence measures shall be applicable. At the same time, the institution, when providing the payment initiation or account information services, must have an effective transaction supervision (screening) system in place, enabling one to detect whether the transaction causes suspicions regarding MLTPF, by applying standard or enhance due diligence measures to the customer in cases of increased (higher) risk.

160.5. An insurance merchant, insofar as it is carrying out life insurance or other insurance activities related to the accumulation of funds, and an insurance intermediary, insofar as it is carrying out life insurance or other insurance activities related to the accumulation of funds, is entitled to conduct simplified customer due diligence, if a low MLTPF risk and the circumstances specified in Paragraph 4, Section 26 of the Law are present:

160.5.1. with respect to persons whose life insurance contracts provide for the annual insurance premium of not more than EUR 1,000 or is in a foreign currency which according to the exchange rate to be used in accounting at the beginning of the day of executing the transaction is not more than EUR 1,000, or if the single premium does not exceed EUR 2,500 or is in a foreign currency which according to the exchange rate to be used in accounting at the beginning of the day of executing the transaction is not more than EUR 2,500;

160.5.2. with respect to persons concluding lifelong pension insurance contracts and such contracts do not provide for the possibility of early disbursement, and it cannot be used as collateral;

160.6. a private pension fund is entitled to conduct simplified customer due diligence in relation to contributions to pension plans if the customer cannot use the abovementioned contributions as collateral and cannot assign them, and in relation to such contributions to pension plans which are made by way of deduction from wages;

160.7. insurance intermediaries and investment brokers that do not carry out transactions with financial resources;

160.8. account information service providers and payment initiation service providers using only the information contained in the services they provide.

161. According to the provisions of Section 26 of the Law, in the case of simplified due diligence, the institution shall be entitled to take customer due diligence measures referred to in Section 11.[1] of the Law, inter alia, the measures for determining the BO of the customer, within the scope corresponding to the MLTPF risk inherent to the nature of the business relationship or occasional transaction. The Law does not release the institution from the duty to perform customer due diligence, inter alia, to clarify the BO of the customer, but allows the performance of simplified due diligence – obtain information necessary or customer due diligence within the scope corresponding to the risk, for example, if the business relationship with the city council (local government) is commenced, in light of the functions thereof, it shall not be necessary to obtain information about the purpose of opening the account, key cooperation partners, planned volumes of transactions, etc. The scope of information to be obtained during the customer due diligence will be smaller than in cases of standard customer due diligence, when it is necessary to clarify information about the volumes of transactions planned by the customer, key cooperation partners, etc. Elements required by law. The manner of obtaining information may also differ, and the institution shall obtain information necessary for simplified customer due diligence in accordance with the risk (please see Sub-clause 3.1.3.2 for more information).

162. Simplified customer due diligence shall not be applied in the cases referred to in Section 26 of the Law if, on the basis of a risk assessment, the institution determines whether it has information about MLTPF or attempted to perform such activities or the increased risk of such activities (there are risk increasing factors). For example, if a BO changes for a high-risk customer and the new BO does not have risk-increasing factors, it would not be appropriate to apply simplified customer due diligence, as, in order to manage the MLTPF risk, it would be necessary

to carry out enhanced customer due diligence for a certain period of time in order to manage the risk associated with BO changes.

163. According to the Law, there are conditions that stipulate the obligation to conduct enhanced customer due diligence. For PEP and high-risk third country customers, the Law provides a framework for enhanced customer due diligence measures. Measures to identify risk increasing factors should be proportionate to the risk, as recommended by the FATF, and in truly low-risk scenarios, information to identify risk increasing factors may be limited. For example, measures to clarify the status of a PEP for small-scale transactions (e.g., parking fees) would not be proportionate to the MLTPF risk inherent to such a transaction (for more information on the enhanced due diligence applied to a PEP, see Sub-section 3.6).

164. The set of enhanced due diligence measures applied to a customer with a low inherent risk of services will be different and smaller than to a customer with a significant amount of transactions with a higher inherent risk of MLTPF. For example, regarding life insurance services with contributions up to EUR 4,000 per year, the life insurance company carries out an assessment of the source and amount of income indicated in the questionnaire, to verify the origin of the funds, i.e., verifies that the planned contributions are proportionate to the income and that the income declared is appropriate to the position held, only requesting additional documents if it identifies an increased risk of MLTPF during the due diligence.

Example

When concluding an annuity insurance contract with a customer, the institution shall obtain the completed application and a copy of the identity document of the customer. Given that the funds that will be used to make the monthly payments are received from the State Social Insurance Agency as a person's accumulated state-funded pension capital, the institution may determine in internal procedures that, taking into account the low MLTPF risk inherent to the service, the information necessary for the customer's due diligence is obtained from the completed application, which allows the institution to presume the purpose of the business relationship, the expected nature and the origin of the funds used.

Also, given the low risk inherent to the service, an institution may expect it to ascertain compliance with PEP status for customers who conclude annuity insurance contracts to the extent that it obtains information from the customer's completed application, provided that, in accordance with international recommendations, measures to ascertain the status of an PEP should be taken according to the risk, whereas the presence or absence of PEP status to a customer does not have a significant effect on the risk inherent to an annuity service.

165. Taking into account the above mentioned with respect to the companies with stock being listed on a regulated market, and the customers being the Republic of Latvia, a derived public person, direct administration or indirect administration institution, or a capital company controlled by the State or a local government (characterised by a low MLTPF risk), it shall be necessary for the institution to take the BO clarification measures to an extent corresponding to the MLTPF risk.

166. In accordance with Paragraph 10, Section 26 of the Law it shall be the duty of the institution, upon applying simplified customer due diligence, to obtain and document information attesting to compliance of the customer with the conditions for applying simplified due diligence specified in Section 26 of the Law, as well as, after the establishment of a business relationship, to carry out the supervision thereof, based on the risk.

167. Taking the requirements of Paragraph 2, Section 26 of the Law into account, when determining the MLTPF risk inherent to the cooperation with the customer, and assessing, whether in the particular case there are grounds to apply simplified customer due diligence, it shall be necessary for the institution to assess whether the information available about the capital company is sufficient to obtain confidence that it is a capital company controlled by the State or a local government with low inherent MLTPF risk.

3.3.2. Additional criteria for simplified due diligence

168. Pursuant to the Law, the Commission has the right to determine the criteria for simplified customer due diligence. The criteria for simplified due diligence, depending on the financial services provided:

168.1. it is carried out for customers-natural persons – residents, whose transactions involve the regular receipt of remuneration or other stable income, the source of which is clear and comprehensible and the total monthly credit turnover does not exceed EUR 15,000 (linear) (the Commission took into account the customer's nationality and the fact that the customers of such a risk profile income and the amount thereof have an understandable and legal origin, which would be proportionately assessed by conducting customer due diligence to a lesser extent and regularity);

168.2. it is performed for legal persons, enterprises registered in Latvia with BO residents of Latvia, for example, clearly understandable small entrepreneurs with individuals as customers on the one hand and some specific suppliers of materials and services (incl. EU companies may be known) on the other hand;

Example

Customer risk profiles to which the simplified due diligence applies:
- customer-natural person – a resident of the Republic of Latvia. Receives a state pension granted by the Republic of Latvia, spends funds in shops in the territory of the Republic of Latvia and makes utility payments. Uses a current account and debit card;
- customer-natural person – a resident of the Republic of Latvia. A student who receives a scholarship and salary from a state-owned joint-stock company, spends its money in shops in the territory of the Baltic states, makes utility payments and settlements for studies. Uses internet banking, current account and debit card;
- customer-legal person registered in the Republic of Latvia. Engaged in the retail sale of food products, makes payments in connection with economic activities (settlements for goods, rental of real estate, utility payments, etc.) and pays taxes in the Republic of Latvia. Uses internet banking, current account and POS terminals;
- customer-legal person registered in the Republic of Latvia. State joint stock company engaged in the maintenance of the electricity network. The company makes payments in connection with

economic activities (salaries, utility payments, etc.) and pays taxes in the Republic of Latvia. Uses internet banking, current account and overdraft.

168.3. it is carried out for customers whose annual insurance premium under life insurance contracts does not exceed EUR *4,000* or its equivalent in foreign currency (the Commission took into account that in most cases this product was chosen taking into account the possibility of receiving a refund of the paid income tax on the declared income, and the amount of the premium and the MLTPF risk inherent to the product).

169. In simplified due diligence, the institution provides for simplified customer due diligence activities to a lesser extent. It would be sufficient to identify the customer and verify the source of income and the amount of planned transactions. Completion of the questionnaire and verification of the source of income in the case of simplified due diligence shall be performed if the necessary information cannot be obtained in another way, for example, from a completed application or contract to receive a service.

170. In addition, simplified customer due diligence activities during a business relationship may include:

170.1. acceptance of the purpose and nature of the business relationship, given that a product may have only one purpose;

170.2. updating customer information only if there is a change in the services provided to the customer (for example, the customer starts using a new service or product);

170.3. supervision of transactions only above a threshold reasonably set by the institution.

171. If an institution identifies, in the context of transaction monitoring, risk-increasing factors that result in a change in the customer's inherent MLTPF risk, the institution shall establish appropriate customer due diligence measures, which may include standard customer due diligence or enhanced customer due diligence or it is necessary to apply risk mitigation measures.

Example

Situation No. 1

The institution concludes a life insurance contract with the customer (without savings) with an insurance amount of 500,000 euros, indemnity payment is only possible in the event of the death of this person and is payable to the heirs. The customer undertakes to pay a monthly premium (payment for the service) in the amount of 100 euros by making a transfer from its account with a credit institution, and payments are planned for the entire term of the agreement for 20 years. When concluding a contract with a customer, the institution obtains the customer's completed application and a copy of the identity document. The contract also specifies information about the insurance term, the chosen frequency of payments, etc.

Taking the customer's projected monthly premiums for a life insurance policy of around EUR 1,200 per year into account, the institution may determine in its internal procedures that, taking into account the low MLTPF risk inherent to the service, the customer's inherent MLTPF risk (including PEP status) is determined by evaluating the information from the completed application, which allows the institution to assume the purpose and expected nature of the

business relationship. At the same time, the institution should include in its internal procedures the size of transactions or risk increasing factors, upon the occurrence of which it would ask the customer to provide additional information, such as the origin of the funds, if the customer wishes to make a large lump sum payment.

Situation No. 2
The customer of the credit institution is a resident of the Republic of Latvia with an income of 1,500 euros per month, the source of income is the salary in a publicly known shopping centre. The expenditure structure consists of daily payments.

The credit institution shall perform an initial assessment of the customer's risk and, if no other risk increasing factors are identified, apply a simplified customer due diligence which provides for the update of customer data every five years (unless other risk factors are identified during this period) when the customer communicates with the credit institution within the framework of the services provided by the credit institution.

3.4. Enhanced customer due diligence

3.4.1. Enhanced due diligence requirements

172. The institution shall perform the enhanced customer due diligence in the following cases:
172.1. in cases prescribed by the Law;
172.2. in accordance with the results of the customer risk scoring (score or level of risk), upon achieving the threshold level specified by the customer risk scoring system of the institution, when enhanced customer due diligence is to be performed;
172.3. according to a risk factor that contains a feature that may indicate a suspicious transaction (enhanced due diligence of the transaction).

173. It is not always possible to automatically detect the occurrence of all risk factors, merely by means of technological solutions. There are certain risk factors, the occurrence whereof shall be detected manually, within the scope of the customer due diligence of transaction screening.

174. In order to ensure that the measures taken by the institution and the information obtained from the customer are proportionate and effective, the institution shall use publicly available sources when obtaining information about the customer and shall take into account information obtained from its previous due diligence activities. As part of the enhanced due diligence, an institution obtains information from a customer if the customer's risk profile has changed and it is necessary to assess the customer's inherent MLTPF risk.

175. If, as a result of the enhanced customer's due diligence, the institution is unable to satisfy itself that it is able to manage the MLTPF risk inherent to the business relationship or occasional transaction, it shall terminate the business relationship or not execute the occasional transaction. The purpose of this requirement is not to expose the institution to a MLTPF risk that it cannot manage. In some cases, such as when the pension fund is unable to pay the provision or the credit institution maintains the terms of the loan repayment agreement, the business relationships are partially terminated. This means that no new services are provided and the business relationships

are terminated as far as reasonably practicable. In this way, the institution minimises the MLTPF risk to which it is exposed.

176. Providers of life insurance or other insurance services related to the accumulation of funds (including insurance brokers), if the customer does not provide the information required for the enhanced customer's due diligence or a risk of MLTPF is identified, risk mitigation measures, including the refusal to accept new contributions, shall be applied until the required information is received or the contract expires.

3.4.2. Enhanced due diligence in accordance with the requirements of the Law

177. The law provides for cases where the customer's enhanced due diligence is automatically applicable:

177.1. the customer has been identified using off-site identification, which has not been performed in accordance with Cabinet Regulation No. 392;

177.2. the customer is a politically exposed person, a family member of a politically exposed person, or a person related to a politically exposed person;

177.3. the BO of the customer is a politically exposed person, a family member of a politically exposed person, or a person closely related to a politically exposed person;

177.4. starting a correspondent relationship;

177.5. the customer is from a high-risk third country.

178. In accordance with the requirements of the Law and customer due diligence regulations, enhanced due diligence shall result in information that is corresponding to the customer's risk. Therewith, the enhanced due diligence measures (information to be obtained, documents supporting it) must be taken to an extent corresponding to the risk of the customer (for example, scope of information and documents obtained about the customer-student from the high risk third country, by assessing the nature and volume of the transaction, may differ from the scope of information and documents obtained about the customer coming from a high risk third country and using the services of a private banker).

179. The regularity of the customer's enhanced due diligence in the cases specified by law is determined by the institution by assessing the risk inherent to the customer (for more information on the enhanced customer's due diligence period, see Sub-section 3.4.5).

Example
During the business relationship, the customer incurs an indication: the customer is related to a high-risk third country. The institution shall take these enhanced due diligence measures: - examine if the customer’s transactions carried out, services and products used correspond to the customer's declared economic activity; - obtain additional information in order to verify that the BO indicated by the customer or ascertained by the institution is the BO of the relevant customer; - verify the origin of the funds of the customer;

- analyse the economic or personal activity of the customer, incl., in cases when the customer is a company registered in a low-tax territory. The institution shall obtain and document evidence about the customer's relation to a company carrying out actual economic activities and its relation with the BO of the customer.

The range of the volume of information and the type of documents obtained by the institution (for example, contracts, invoices, documents attesting to the movement of goods or documents proving the provision of services, etc.), when applying each and every of the enhanced due diligence measures, depends on the information and documents already at disposal of the institutor – it is not necessary to repeatedly obtain or request the documents attesting to the transactions with the key cooperation partners of the customer, if such documents are already at the disposal of the institution[18].

For example, it shall be necessary to understand the supply contract with the term of validity of several years and submitted already a year ago, and to assess whether the performed transactions still correspond to the provisions of the contract, and to correspondingly document it.

When implementing the requirement with respect to, for instance, knowing the economic activity of the customer, it shall not be necessary to automatically request that the customer updates the customer questionnaire (besides, merely updating the questionnaire or the verification of data of the questionnaire does not mean that the institution ascertains the economic activity of the customer, it shall be necessary for the institution to assess all risk factors inherent to the customer or the activity thereof as a whole and whether there are sufficient documents and information at disposal of the institution characterising the activity of the customer), where the customer specified the same type of economic activity as before.

The purpose of the requirement to know the economic activity of the customer is for the institution to assess whether it still knows the economic activity of the customer and whether it has sufficient information regarding the conformity of the previously clarified information to the existing circumstances. Nevertheless, there might also be situations, when, in implementing this requirement, it is justified and commensurate to request that the customer updates information about the economic activity and to also obtain additional documents, because the transactions do not correspond to the information at the disposal of the institution or the institution has doubts as to the conformity of the performed transactions – for example, the transactions are performed with the cooperation partners operating in a sector different from the sector of the customer, and these sectors are not substantially related and the mutual transactions do not seem logical; the institution detects that, probably, the region of economic activity of the customer may have changed, because the modelof transactions has changed.

Enhanced due diligence measures shall be applied according to the risk and the actual circumstances.

[18] Based on the risk, the institution may also obtain information about the key cooperation partners from public sources, for example, if the activity of the customer corresponds to the declared one and there is public information available about the key cooperation partners (for example, the customer is a farm, ensuring the supply of dairy products to milk processing enterprises).

180. Enhanced due diligence measures may also vary during regular enhanced customer due diligence. The application of the measures depends on the risk identified by the institution in assessing the customer's transactions and the information available about the customer during the regular due diligence. The measures applied are aimed at managing the identified risk of MLTPF.

181. In the event if the customer corresponds to any of the risk factors referred to in the Law, but has not performed any transactions during the reporting period or the transactions have been insignificant (the institution shall correspondingly record it in the due diligence) and if there are no other circumstances present requiring further due diligence measures, the institution shall not conduct further due diligence measures. This means that it shall not be necessary for the institution, by documenting the circumstance that the customer has not performed any transactions or that the performed transactions have been insignificant (based on the rating set by the institution, which the institution shall justify), to apply enhanced due diligence measures to the customer corresponding to any of the risk factors referred to in the Law.

Example

Indication: *The customer is a natural person who is recognised as an PEP, or a family member of the PEP, or a person closely related to the PEP.*

It shall be necessary for the institution to consider both whether the customer is to be recognised as a PEP and the average credit turnover/volume of transactions. The customer's due diligence activities and the period after which the due diligence is performed, if a customer who is a PEP and makes contributions, such as EUR 8,000 per month and whose transactions are not limited to day-to-day expenses, will be different from a situation where the customer is a PEP and once a year contributes EUR 3,000 into the third pillar pension capital.

Nevertheless, at the same time, the institution must ensure effective transaction screening, so that, upon receipt of the funds of a larger amount, differing from the average monthly contribution of the customer, which the institution has assessed and recognised as commensurate, it would be able to detect such instances and would perform the necessary due diligence actions with respect to such contribution.

3.4.3. Enhanced due diligence in accordance with the customer risk scoring results or other circumstances

3.4.3.1. Enhanced customer due diligence[19]

182. On the basis of the customer risk scoring results (score or risk level), the institution shall determine the risk scoring threshold level, to which the enhanced customer due diligence is correspondingly applied. The threshold level for the performance of enhance due diligence before the establishment of a business relationship and during the business relationship will be different, just like the applicable enhanced due diligence measures and the scope thereof (depending on the inherent risk).

[19] Enhanced due diligence before and during the business relationship at regular intervals.

183. The institution may determine the customer's due diligence on the basis of other circumstances as well, including the occurrence of any of the risk factors similar to the cases of mandatory due diligence specified by law.

184. In assessing the risk-increasing factors inherent to the customer and in determining the measures and regularity of due diligence, the institution shall assess the appropriate risk management measures and take into account the actual risk inherent to the customer. For example, when assessing the risk inherent to the economic activity of a customer or its beneficial owner, an institution shall identify the nature of the economic activity of the legal person and take into account the MLTPF risk of the customer's used financial services and the impact of the customer's BO on the customer's MLTPF risk.

Example

Situation No. 1
The customer incurs an indication that the economic activity of the beneficial owner has an increased MLTPF risk.

The institution shall, by conducting customer due diligence prior to the commencement of the business relationship, identify the nature of the customer's economic activity and the source of income. The fact that the customer's beneficial owner is engaged in an economic activity with an increased MLTPF risk means that the institution assesses the impact of that circumstance on the customer's inherent MLTPF risk.

The Institution, concluding that the activities of the beneficial owner are separable from the economic activity and transactions of the customer, shall establish measures to enable it to identify the occurrence of an increased risk of MLTPF in good time and to apply enhanced due diligence.

Situation No. 2
The customer's type of economic activity is computer programming, provision of IT services, one of the key business partners since the opening of the account is a Russian company, the customer's BO address is in Russia and the contact phone number in the questionnaire is in Russia.

The institution shall assess the risk factors inherent to the customer:
1) customer risk – the type of economic activity is the provision of services for which it is difficult to substantiate the fact of provision of services;
2) geographical risk of the customer, its BO and the key cooperation partner – connection with a country which is not the Republic of Latvia, the EU, the European Economic Area or an OECD member state.

In order to manage the risk inherent to the customer, the institution shall assess the risk inherent to the customer as high and shall provide for due diligence measures to ensure that the customer's economic activity is economically justifiable.

In the event of a link between the customer's and the beneficial owner's transactions indicating an increased risk of MLTPF, the institution shall conduct enhanced customer due diligence.

185. When setting the threshold level or other circumstances and the enhanced due diligence measures applicable thereto, the institution shall ensure that the applicable enhanced due diligence measures and the scope thereof are appropriate and effective enough for the institution to be able to assess and understand the economic or personal activity of the customer.

186. The risk level inherent to the customer shall define the frequency of enhanced due diligence, i.e., the lower the risk, the less frequent the enhanced due diligence, and vice versa – the higher the risk, the more frequent the enhanced due diligence.

187. When setting the frequency of enhanced due diligence, the institution shall specify the point of reference for calculating the term of one year or months in the policies and procedures, observing the purpose of the Customer Due Diligence Regulations – to ensure the continuity of the process of enhanced due diligence.

3.4.3.2. Enhanced due diligence to evaluate customer transactions

188. The EBA Guidelines and the Financial Intelligence Unit typologies (available here: https://www.fid.gov.lv/lv/darbibas-jomas/vadlinijas-tipologijas-riki) include risk factors that may be inherent to a customer's transactions, such as to changes in the amount or nature of the customer's transactions, taking into account the customer's declared economic activity. In accordance with the Law, during cooperation with a customer, the institution supervises transactions in accordance with a risk-based approach. As a result, higher-risk customers need to be more closely monitored.

189. Upon the occurrence of the risk factor inherent to a customer’s transaction, the institution shall conduct the enhanced customer due diligence (transaction due diligence), by taking **some of the enhanced due diligence measures**, which are substantially required, in order to ascertain the economic and lawful purposes of the transactions, i.e., performs the customer due diligence to an extent required to clarify whether the occurrence of the risk factor creates suspicions about the MLTPF or causes an increase of the MLTPF risk. In addition, the information already available to the institution should be taken into account and assessed in these cases.

Example

The indication occurs: *transaction is concluded or outsourced on behalf of the customer by a third person (an accountant, attorney or a service provider for the establishment and functioning of a legal arrangement acting on behalf of the customer (not applicable to the opening of a temporary account as long as the company does not have the status of a legal person, as well as for transactions regarding the increase of share capital).*

This factor means that the institution, when detecting that the transaction in the interests of the customer is concluded or performed by a third party, for example an outsourced accountant, attorney or a service provider for the establishment and functioning of a legal arrangement acting

on behalf of the customer, shall perform customer due diligence to such an extent that enables one to clarify whether it creates suspicions about the MLTPF or increase of the MLTPF risk.

When setting the applicable enhanced due diligence measures, the institution shall take into account the information about the customer at its disposal - for example, an enterprise registered in the Republic of Latvia with three employees, engaged in sewing (tailoring) service, has authorised an outsourced accountant for the performance of transactions, because it does not employ an in-house accountant; largescale production enterprise authorises the attorney for the performance of transactions, in order to conclude a secure agreement, taking into account the knowledge of the attorney. For such customer, the scope of due diligence will differ from the scope of due diligence that must be applied to a higher risk customer, for example, shell arrangement, on behalf whereof the outsourced accountant is acting.

Not all the customers using the third party services (for example, outsourced accountant) shall automatically be considered as high-risk customers.

3.4.4. Period for which enhanced due diligence is to be performed

190. The institution shall prescribe the period of enhanced due diligence (i.e., the period of time for which the activity of the customer is being assessed, the enhanced due diligence reporting period) in the policies and procedures, observing the circumstances that have formed the basis for the performance of enhanced customer due diligence. Neither the Customer Due Diligence Regulations, nor any other laws and regulations prescribe any particular period, for which enhanced due diligence is to be performed, but they define the purpose of enhanced due diligence - to ascertain that the institution knows the activity of the customer and there are no suspicions present about the MLTPF.

191. Regarding the customers, who are required to have enhanced due diligence when the threshold for customer risk scoring is reached or other circumstances arise, the customer due diligence regulations require the continuity of enhanced due diligence. Therewith, when setting the frequency of enhanced due diligence, the institution shall specify the point of reference for calculating the term of months, by observing the purpose of the requirement – to ensure continuity of the period of enhanced due diligence (this does not apply to a situation where the customer's risk changes, according to which the enhanced due diligence does not have to be applied).

The core principle for setting the period with respect to the customers of enhanced due diligence is – the time period since the performance of the last enhanced due diligence (considering the final date of the period of the last enhanced due diligence as the reference point).

Nevertheless, depending on the transactions and the MLTPF risk, there may be situations when it is necessary to also include the period (or a part thereof), for which the due diligence was performed, in order to understand the activity of the customer.

Example

Situation No. 1
Incurs an indication: *The customer is a shell arrangement.*

In view of the increased risk of MLTPF inherent to shell arrangements, the Institution shall apply enhanced due diligence measures every six months.

Situation No. 2
Incurs an indication: *the customer's economic activity has an increased risk of MLTPF (trading of precious metals, precious stones).*

The institution shall assess the risks inherent to the customer's activities and the extent of the transactions and decide on the determination of the enhanced due diligence period. If it is determined that an increased MLTPF risk is inherent to the customer, the institution shall determine the period of enhanced due diligence in accordance with its policies and procedures. The institution may decide to monitor transactions and, if changes in the volume of transactions or other risk-increasing circumstances occur, set a shorter enhanced due diligence period accordingly (for example, if the period is 12 months and the volume of transactions increases, the institution shall set an enhanced due diligence period of six months).

192. If the customer incurs the risk factor or a combination of risks and previously the standard due diligence was performed, but enhanced due diligence was not performed, then the institution shall set the enhanced due diligence period from the last performed standard customer due diligence. Nevertheless, depending on the transactions and the risk, it might be necessary to also include the period, for which the due diligence was already performed.

193. In determining the period for which enhanced due diligence is to be performed, the institution shall take into account the MLTPF risk inherent to the customer and the detected risk factor or the time of the previously performed enhanced due diligence, if any has been previously performed with respect to the customer (enhanced due diligence is to be performed, in order to understand whether the particular risk factor creates suspicions about the MLTPF or risk increase, therewith the period is to be set according to the risk factor).

Example

Incurs an indication: *The customer is ordering an asset to be invested in a financial institution jurisdiction with high MLTPF risk.*

This factor refers to the cases, when the customer orders asset (monetary funds, financial instruments, etc.) investment in a financial institution located in a higher risk jurisdiction (insofar as the institution knows that it is the financial instruments' investment).

The institution shall apply the enhanced due diligence measures for such period that enables an understanding of whether such order of the customer creates suspicions about MLTPF or risk increase. To set the period, it shall be necessary to assess the information about the customer at

the disposal of the institution – whether the institution understands the activity of the customer, whether such transactions are typical for the customer, whether and when the enhanced due diligence was performed for the customer, etc.

The core principle for setting the period with respect to the risk factor inherent to the customer's transaction – the MLTPF risk of the customer and the detected risk factor.

3.4.5. Enhanced due diligence term

194. The customer due diligence regulations provide for a certain period of time during which enhanced due diligence shall be performed. The purpose of the term is to identify the potential risk of MLTPF within a reasonable period of time and to take appropriate risk management measures. The term of regular enhanced due diligence is 35 working days from the occurrence of the preconditions for the performance of enhanced due diligence.

195. The institution may extend the period of enhanced due diligence if it is reasonably necessary, for example, obtaining information from a multinational corporation takes longer. In such a case, the institution has the right to extend the term of the enhanced due diligence up to 25 working days. Where risk increasing circumstances are identified, the Institution shall decide on the application of enhanced supervision measures. The institution shall document the reasons for the extension.

196. If, after the expiry of the enhanced due diligence, the institution is unable to complete it due to a lack of available information, the institution shall assess the impact of the missing information on the MLTPF risk to which it is exposed. If the substantive enhanced due diligence has been carried out and the missing information is to be regarded as additional information only, and the institution's activities and transactions are clear and comprehensible, the institution may extend the term and obtain additional information. The institution shall prepare the conclusions of the enhanced due diligence within the time limit of enhanced due diligence, i.e., 60 working days if the time limit is extended.

197. The term of enhanced due diligence to investigate the risk factor inherent to a transaction should be proportionate to the risk inherent to that factor. Following the information provided, the institution shall assess the impact of the specific risk factor on the MLTPF risk and decide, as appropriate, on a prudent and reasonable term for risk management when deciding on enhanced supervision measures, if necessary.

3.4.6. Determination of groups of connected customers

198. Upon the commencement of a business relationship, the institution, by means of a risk-based approach, shall verify, assess and document whether the customer belongs to a group of connected customers according to the criteria set in the Glossary of the Customer Due Diligence Regulations. The higher the MLTPF risk inherent to the customer, the greater attention must be paid to the criteria.

199. Based on the MLTPF risk inherent to the customer, there might be a situation when the criteria set in the Glossary of the Customer Due Diligence Regulations are not to be applied at all or attention must be paid to separate criteria. Particular criteria and in the situations of what type of risk they shall be applied, in order to determine the group of connected customers, shall be defined by the institution.

Criteria shall be assessed on the basis of the risk. There is no requirement set to perform the assessment of all criteria with respect to all customers of the institution.

200. Detection of a group of connected customers in cases when an increased risk is present, enables the institution to assess the transaction scheme as a whole, thus ensuring more comprehensive assessment about the performed transactions and detection of suspicious transactions. When assessing transactions of a single customer separately, information about transactions is narrower, therewith the indications of potentially suspicious transactions might as well not be detected. In turn, the broader the information about the transactions (*inter alia*, intra-group transactions), the more comprehensive the assessment possible to determine whether the transactions have economic justification and purpose and whether the transactions have the characteristics of suspicious transactions.

201. There might be situations, when the criteria for the group of connected customers can be detected automatically (for example, the customers have one and the same BO). Nevertheless, part of the criteria can only be detected within the scope of enhanced due diligence - manually (for example, family relationship (family ties) between the BO, the customer uses a loan, the collateral whereof is another customer's financial instruments).

202. In the policies and procedures the institution shall set the requirements for the assessment of the indicative criteria of the group of connected customers referred to in the Glossary of the Customer Due Diligence Regulations. The institution shall be liable for justification of the implementation and adequacy of the set requirements.

203. The Customer Due Diligence Regulations do not provide that, upon the detection of any of the criteria referred to in the Customer Due Diligence Regulations, it shall be automatically considered that the customers comprise the group of connected customers. In cases where two or more customers have a common BO, these customers would have to be considered as a group of connected customers. Whereas in cases where family ties of the BOs, a coincidence of the authorised representative or contact information is identified for two or more customers, the institution must, first of all, assess these characteristics and, in case of necessity, must obtain additional information, taking into consideration the fact that they may indicate the existence of a group of connected customers.

Example

Situation No. 1
Several customers of one and the same institution are detected, whose actual addresses coincide.

Possible conduct: to clarify what kind of building is at the particular address – private house, office building – and whether there are any suspicions present as to the use of a letterbox address.

In this case it should be assessed whether there is a connection between the customers (for example, it is planned to carry out interrelated transactions), in order to determine whether the customers are considered to be a group of connected customers.

Situation No. 2
Customer A of the institution is an enterprise engaged in dairy farming and supplies its products to another customer of the institution – customer B, whose economic activity is the manufacture of dairy products. Customer A performs various payments for the expenses and maintenance of the farm, while the incoming transactions are mainly (~85%) payments from customer B for the supplied products.

Possible conduct: the institution detects that the transactions of customer A and customer B correspond to the indication of the group of connected customers "the mutual transactions form at least 30 per cent of the customer's monthly turnover", however, having assessed the economic activity and performed transactions of customer A and customer B, there are no grounds to consider that customer A and customer B form a group of connected customers.

Situation No. 3
Apartment owners of a multi-apartment house have established the association for the management of the house. The BO of the association is presumed to be its Executive Board, consisting of the owners of five apartments.

Apartment owners, even though their actual address coincides, would not be considered to be a group of connected customers.

204. When assessing whether a group of connected customers exists, the institution shall assess both the indications referred to in the Customer Due Diligence Regulations and also the transactions of potential participants of the group (*inter alia*, payments, mutual loans, transactions in financial instruments, mutual guarantees (sureties), etc.).

Example

Customer A and customer B of the institution own a joint company *Kļava.* Customer A is the BO of the company *Bērzs.* In turn, customer B is the BO of the company *Ozols*.

The economic activity of the company *Kļava* is catering services. The economic activity of the company *Bērzs* is construction services. In turn, the economic activity of the company *Ozols* is related to the sale of real estate.

To assess the existence of the group of connected customers, the institution shall consider the circumstances that the enterprises are operating in the sector featuring increased risk with respect to the use of cash, as well as the circumstances that the company *Kļava* has two BOs, each of which is also the BO in another company.

To ascertain whether or not the company *Kļava* is related (connected) to the companies *Ozols* and *Bērzs*, the institution shall assess both the types of economic activity of the companies, and whether or not the companies perform mutual transactions (payments, loans, guarantees (sureties), etc.).

Considering the fact that the companies demonstrate an indication with respect to a common BO, the institution shall form the mutually connected customer group or groups:
1) including all the companies in one group;
2) including the companies *Kļava* and *Ozols* in one group and the companies *Kļava* and *Bērzs* in the second group.

When selecting which of the group formation options to apply, the institution may be guided by the number of participants of the group and the substance (nature) of participants of the group (for example, if each BO has its own holding, it is reasonable to form separate groups for each holding company).

205. Having identified a group of connected customers, the institution shall document the role of each customer in the group and shall schematically depict the flow of money and goods within the group and with the counterparties outside the group, in order to understand the role and meaning of each participant in the group. If one BO has several companies with the same direction of economic activity, then the institution, on the basis of the risk, shall clarify and document the reason for setting up several companies with the same economic activity and the economic substance of such conduct.

206. When documenting the participants of the group of connected customers and their role within the group, the institution shall ensure that each participant has information at its disposal that the customer is in the composition of the group (specifying the relevant group) and when the activity of the group was generally assessed, but it shall not be necessary to include the rating itself in the file of each participant. It shall be necessary to ensure the traceability of the rating and retrieval thereof in case of necessity, for example, if an independent external audit of the verification of the Commission is being performed.

207. Upon the detection of a group of connected customers, the risk score of each participant of the group shall be defined according to the customer risk scoring system. Therewith, the risk of the participants of the group may differ (if one participant of the group has a high risk, it shall not automatically mean that all participants of the group have a high risk and the activity of the group and the risk inherent thereto is to be assessed as a whole).

3.4.7. Enhanced due diligence for the group of connected customers

208. The institution, by means of a risk-based approach, must prescribe in the policies and procedures the frequency at which it is necessary to perform not only the enhanced due diligence of a particular customer, but also the enhanced due diligence of the customers forming the group of connected customers with the relevant customer, i.e., to study the activity of the group of customers as a whole within the scope of the institution (attention must be paid not only to the incoming and outgoing payments of the group, but also to intra-group transactions). The purpose of this requirement is to ensure that the institution not only knows the economic or personal activity of the customer, but also the activity of all customers forming the group of connected customers, thus obtaining a more complete understanding of the performed transactions (the transactions of each separate customer may also not be indicative of suspicious transactions, in turn, by assessing the transactions of the group as a whole, it is possible to better understand the substance of transactions and to detect suspicious transactions).

According to the regulation of customer due diligence regulations, a group related to a customer is other customers of the institution, **which are clarified by conducting enhanced customer due diligence.** Therefore, in **standard** cases, when applying the requirements for simplified or standardised due diligence, the institution is **not** required to identify and conduct enhanced entire group due diligence, but if any risk factor is identified that requires enhanced due diligence, then this due diligence should identify the group associated with that customer and evaluate that group as a whole.

209. If the customer belongs to a group of connected customers, the institution conducts enhanced due diligence in order to determine whether enhanced due diligence is to be performed for the entire group of connected customers; the institution **shall assess the role of the relevant customer within the group and shall consider the date and results of the last enhanced due diligence performed for the entire group of connected customers**[20]:

209.1. if the role of the customer is significant and enhanced due diligence has not been performed for the group within the term set by the institution, enhanced due diligence shall be performed for all customers belonging to a group of connected customers;

209.2. if the role of the customer is significant and enhanced due diligence has been performed for the group within the term set by the institution, enhanced due diligence shall be performed for the customers of enhanced due diligence only;

209.3. if the role of the customer in the group is not significant, the enhanced due diligence shall be performed for the customer of enhanced due diligence only;

[20] If risks were detected during due diligence that require more frequent transaction analysis, enhanced due diligence shall be performed more often. The criterion of significance and the results of the last due diligence must be viewed in a complete way, in order to avoid the situation where under the influence of the significance of various participants of the group, enhanced due diligence for the entire group must be performed incommensurately often.

209.4. if, when performing customer due diligence, unclear issues or discrepancies with the activity of the group of the customer as a whole have been detected, enhanced due diligence shall be performed for the entire group of customers according to the identified unclear issues, discrepancies.

The circumstance determining the performance of enhanced due diligence for the entire group or for a separate customer for which the institution conducts an enhanced due diligence is the role (influence) of the customer within the group and the date and result of the previously performed enhanced due diligence of the group. In turn, if, when performing the due diligence of a customer belonging to the group of customers, unclear issues or discrepancies with the activity of the group of customers as a whole are detected, it may form grounds for performing due diligence for the entire group of customers.

210. The institution shall determine the significance (influence) of the role of the customer within the group, by assessing the activity of the customer, its BO, volume of transactions, purposes of transactions, risk increasing factors, etc. For example, when determining the significance of the role within the scope of holding companies, it must be taken into account that only one of the holding companies might have a significant turnover, which does not automatically mean that enhanced due diligence must be performed for one company only. It shall be necessary for the institution to evaluate whether there are any risk increasing factors present, for example, whether the BO of the holding is a PEP, what the purpose of the performed transactions is, for example, a holding company receives money once a month in accordance with the consulting agreement, by assessing whether the institution has sufficient information and understanding of the lawful purpose of the transaction at its disposal.

211. If, based on the result of the customer risk scoring, it is necessary to perform enhanced due diligence for the customer, the institution shall assess the group of customers as a whole and shall understand the role of each participant of the group of connected customers and the influence thereof on the entire group. In cases when the institution can justify that such separate customers from the group of connected customers do not influence the group as a whole, not all of the customers belonging to the group of connected customers should be subject to enhanced due diligence, but only those having influence on the group.

212. When commencing a business relationship with a new participant of the group of connected customers, the institution shall assess the role of the new participant in the group and the regularity of the enhanced due diligence prescribed for the group of connected customers – if the customer does not have a significant role in the group and the group has undergone enhanced due diligence in accordance with the prescribed regularity, it shall not be necessary to perform enhanced due diligence of all customers. If the role of the new participant is significant, it shall be necessary for the group to perform enhanced due diligence of all customers belonging to a group, if enhanced due diligence has not been performed for the group in accordance with the prescribed regularity.

213. Upon the occurrence of the risk factor inherent to a customer’s transaction, it shall not be necessary to perform enhanced due diligence of all connected customers every time; however, it

may be necessary, if the institution detects an influence on the entire group of connected customers during the due diligence of the relevant factor.

3.4.8. Measures within the scope of enhanced due diligence

214. Within the scope of enhanced due diligence, it is necessary to obtain additional (more detailed) information about the economic or personal activity of the customer. Thus, based on the risk assessment, the institution shall not only obtain the name of the type of customer's economic or personal activity (for example, trade, intermediation in trading activities), but also more detailed information about it, for example:

214.1. how the customer organises its economic or personal activity;

214.2. what the actual place of the economic activity is;

214.3. what the number of employees in the company is;

214.4. what the distribution channels of goods and services are;

214.5. what the economic activity of the previous periods is (turnover, profit, partners, etc.);

214.6. whether the customer has a licence or special permission, if the customer's declared economic or personal activity provides for the obtaining of such a licence and it is connected with MLTPF and a high sanctions risk industry that impacts the customer's risk assessment[21].

215. The institution, based on the risk assessment, shall also obtain the documents confirming this information. Based on the risk assessment, the institution may require the submission of supporting documentation of transactions or account statements for the previous period of activity, which enables one to assess the customer's previously conducted transactions, counterparties, volume of transactions and compare it with the information declared by the customer with the institution. In addition, the institution may obtain other information from public and independent information sources, in order to gain a complete understanding about the customer's economic activity and its volume.

Example

Situation No. 1

In the case if the customer issues loans and it is not its declared economic activity, by means of a risk-based approach (for example, if the customer is registered in a high risk jurisdiction and its economic activity is not related to lending, the loans are issued to persons from high risk jurisdictions), it shall be necessary for the institution to follow up on whether the loans issued during previous years are being repaid. For example, the customer issued a loan in 2016, with the repayment term expiring in 2017. The institution conducts enhanced customer due diligence in 2017 and only assesses the transactions performed in 2017, but is no longer assessing the transactions of 2016, in accordance with which repayment of the loan would have to be received in 2017. Repayment of the loan is not received in 2017. The customer continues issuing new loans, which, probably, will never be repaid, and it is not planned that they would be repaid. These circumstances may be indicative of a fictitious activity.

[21] Ascertaining the existence of a licence shall refer to the cases when the legal nature of the activity of the customer is related to transactions exposed to a higher MLTPF risk (for example, provision of financial services, organisation of gambling, etc.).

Situation No. 2

On 26 February 2019, the customer *SD Ltd* transfers to the institution for management (fiduciary transaction), financial resources in the amount of EUR 700,000 in favour of the company *AB LP*. One and the same BO is specified for both companies - A.S.

On 26 February 2019, the institution issues the company *AB LP* a loan in the amount of EUR 700,000, which it, in turn, transfers to Spanish companies *X S.L.* (03.03.2019, 400,000 *euros*), *Y S.L.* (04.04.2019, 150,000 *euros*) and *Z S.L.* (04.04.2019, 150,000 *euros*) and the payment objective – *payment for replenishment of the authorised capital* (all companies have accounts with a credit institution in Spain).

Within the scope of enhanced due diligence, it is necessary to clarify the economic substance and lawful purpose of the referred to transaction scheme:
when concluding a transaction regarding a fiduciary loan, it was clarified that the company *AB LP* needs the loan for an investment project in Spanish companies (without specifying the firm name of particular companies), further performing the acquisition of the investment object. The company SD Ltd places the available financial resources in deposit for the purposes of receiving interest income.
The customer has submitted an explanation regarding this situation, which has been accepted, that it is not considered correct for one company to issue the loan to the other company, because then it would be the financing of investment activities of one company on the account of current assets of the other company.
Upon the receipt of an explanation from the customer, it shall be essential for the institution to ascertain the appropriateness and justification thereof itself, assessing the conformity of the explanation to the sectoral practice, by verifying information in public sources, etc. It is important to document the justification of a conclusion:
- in addition, within the scope of enhanced due diligence, it would be necessary to assess whether the scheme of fiduciary transactions is used to conceal the actual origin of the financial resources used for investments, which come from *C. Inc.*, *LM Ltd* and *A.O. L.P.* (financial resources from these companies have been paid into the account of the customer *SD Ltd* and the transactions of the customer *SD Ltd* with the referred to companies are of a one-off nature).
Supporting documents have been requested with respect to this situation. They have been received in the Spanish language, and on the due diligence checklist it was specified with respect thereto that they are in regard to an agreement on the acquisition of real estate in Spain.

To ascertain the content of the documents and to assess it, the institution needs a document in a language that the employee of the institution understands – the customer may be asked to submit such or the institution may translate the documents itself. It shall be necessary for the institution to ascertain that the documents support the transactions performed in the account of the customer.

Situation No. 3

The customer *WA LP* is a company registered in a EU Member State, with the account being opened in 2015, type of economic activity – investment activity.

In 2017, several fiduciary agreements have been concluded between the institution and the customer *WA LP* on the financing of several loans. The customer has taken over the liabilities of another customer of the institution – *DX LLP*. The customer *DX LLP* has invested into the fiduciary transaction, the financial resources received in the form of a loan from another customer of the institution - *OL Ltd,* in accordance with the loan agreement concluded in 2014 on the issuance of the loans in the amount of USD 1.2 million and EUR 700,000 for the term of three years.

Within the scope of enhanced due diligence, it is necessary to clarify the initial origin of the financial resources, invested into the fiduciary transaction and lent by another customer of the institution *OL Ltd*.

Situation No. 4
The customer ABC LTD is a company registered in a EU Member State, for whom the institution ensures payment acceptance services. *ABC LTD* is selling food supplements on internet sites. The institution transfers the funds from card users received within the scope of payment acceptance to the account of *CDE LTD* in another financial institution. A large number of complaints have been detected in the public environment regarding the fact that after the performance of purchases on the trading sites of *ABC LTD,* unauthorised payments are being charged from the cards of the purchasers or that the received goods are of improper quality. Likewise, within the scope of transaction screening, it has been detected that 90% of the received card payments are performed with payment cards issued by another country (other than the EU Member State and not considered to be a high risk third country). In the questionnaire, the customer *ABC LTD* has specified that the key cooperation partner thereof is *CDE LTD*, which ensures telemarketing services.

Within the scope of enhanced due diligence, considering the risk increasing factors, it is not sufficient to be limited by the conclusion that the activity of the customer – online trading – corresponds to the activity declared in the questionnaire, but the scheme of the activity of the customer must be assessed as a whole, incl., what measures have been taken to ensure that unauthorised payments are not charged. The institution must obtain information and documents characterising the key cooperation partners of the customer, *inter alia*, it must assess how the customer acquires and performs payment for the goods sold on its internet sites, and whether the customer has alternative channels of income, taking into account the fact that the entire income from acceptance of the payment cards is transferred for telemarketing services only. The institution must also assess information at its disposal about the actual place of performance of economic activity of the customer, considering the fact that card transactions demonstrate that the main target audience of online trading are purchasers not from an EU Member State, but another country (other than an EU Member State and not considered to be a high risk third country).

3.4.9. Enhanced due diligence, when performing an occasional transaction

216. The Law prescribes that the institution shall conduct enhanced customer due diligence, when commencing and maintaining a business relationship or when performing an occasional transaction with a customer with increased inherent MLTPF risk.

217. **It shall be necessary** for the institution, **before the execution of an occasional transaction, to obtain information about the purpose and substance of the transaction to the extent necessary to determine whether the transaction features any risk increasing factors and whether it is necessary to perform enhanced due diligence before the execution of the transaction** (for example, in accordance with the operation of and services offered by the institution, particular risk factors or the set thereof shall be determined, upon the occurrence whereof enhanced due diligence is to be performed, as well as by prescribing the level of scope of due diligence, based on the set of risk factors inherent to the customer.

Example
When offering contactless cash transfers to the higher risk jurisdiction, such transaction (depending on the sum and other circumstances) would have to be subject to enhanced due diligence to an extent adequate to the specific nature of the transaction, besides, performing it prior to the execution of the transaction, considering the fact that after execution it might not be possible to find the customer (for example, by clarifying what the purpose of performance of the transfer to the higher risk jurisdiction is, what the origin of the funds used in the transaction is, etc.).

3.5. Beneficial owner (BO)

3.5.1. Determination of the BO

218. In accordance with the Law, when conducting customer due diligence, the institution shall, in all cases, determine the BO of the customer. In cases when the risk is higher, the institution shall also ascertain whether the determined BO is the ultimate BO.

219. Section 1, Clause 5 “a” of the Law states that the BO is a natural person who is the owner of the legal person or who controls the customer, or on whose behalf, for whose benefit or in whose interests the business relationship is being established or an individual (occasional) transaction is being executed, and it is at least regarding legal persons – a natural person who owns, in the form of direct or indirect shareholding, more than 25 per cent of the capital shares or voting stock of the legal person or who directly or indirectly controls it.

220. The BO is always a natural person who owns, or in whose interests the particular legal person is established or operates, or who directly or indirectly[22] implements control over the legal person. The BO is a natural person, who ultimately owns or who controls the customer, or a natural person, for whose benefit the transaction is performed, therewith this notion entails persons who implement ultimate control over the legal person, namely, ownership or control is being implemented not only by the ownership right, but also via other means of control, which are not considered to be direct control. The purpose of disclosure of the BO is to determine the natural person who actually owns the legal person or who has actual possibilities to control it, irrespective of whether or not the person is the owner of the legal person and whether or not it holds any official

[22] In the case of a direct shareholding or control, the BO controls the legal person directly, while in the case of an indirect shareholding or control, the control is implemented through the intermediation of another – natural or legal – person.

position in the legal person. **The significant feature of the definition of the BO is that it is applicable to the actual control – based on the actual situation, it can exceed the legal ownership and the limit of control.**

Example

100% of capital shares of the customer - legal person is owned by person X. According to the information at the disposal of the institution (information obtained both from public sources and from the customer, within the scope of cooperation), the actual control over the customer is implemented by person C, who is the husband of person X.

It shall be necessary for the institution to assess whether there are reasonable doubts as to the BO.

If, having assessed the economic activity of the customer (whether it is understandable for the institution and the performed transactions do not create suspicions as to the MLTPF, or any information of a negative nature is available), the institution detects that the disclosure of such BO within the scope of the family is understandable (for example, husband has a board business and several companies, where family members are specified as BOs, who correspondingly also implement control or gain benefit in each company, nevertheless, in parallel, the husband also implements control or gains benefit), the institution, based on the results and conclusion of due diligence and by documenting them, may specify both persons as the BO. It shall not be necessary for the institution to obtain the consent of the customer with the results of the performed customer due diligence.

In turn, in cases when the institution, having assessed the activity of the customer and information about the specified BO, incurs doubts (it does not obtain information about the actual ability of the specified BO to be the BO – no sufficient knowledge, no information that would demonstrate that the BO controls or gains benefit from the customer), the institution, if it cannot obtain information about the actual BO, shall act in accordance with the provisions of the Law and shall terminate or not commence a business relationship with such customer, and in cases when there are suspicions about the MLTPF, reports it to the Financial Intelligence Unit.

221. In cases when none of the natural persons owns more than 25 per cent of the capital shares or voting stock of the legal person and it is not possible to determine which natural person controls the customer (for example, the association formed for the purposes of management of the multi-apartment house), the senior management of the legal person may be regarded as the BO, if the doubts that there is another BO are excluded (please see more details regarding this issue in Sub-chapter 3.6.4).

222. The institution, in its policies and procedures, shall prescribe detailed requirements for the manner of determination and the conformity check of the BO.

223. In accordance with the requirements of the Law the institution shall determine the BO of the customer, using information or documents from the Enterprise Register. In addition, on the

basis of risk assessment, the institution shall determine the BO of the customer in one or several of the following ways:

223.1. by receiving a statement on the beneficial owner approved by the customer[23];

223.2. by using information or documents from the information systems of the Republic of Latvia or foreign countries;

223.3. by determining the BO on its own if the information regarding him or her cannot be obtained in any other way.

224. From the requirements of the Law, it derives that obtaining information from the Enterprise Register is mandatory. In cases when the customer risk is low, it shall be sufficient to determine the BO according to the ownership rights, by using information from the Enterprise Register[24]. On the basis of the risk assessment, the institution must also take other measures for verification of the BO (for example, a self-declaration approved by the customer would be permissible in cases of a lower risk, while in turn, in cases of higher risk, it would not be sufficient, if the self-declaration is used as the only measure for the verification of the BO). The lower the risk, the less complicated form of verification is permissible.

225. As regards the use of information and documents from the registers or internet resources, the institution shall observe the risk-based approach, meaning that it shall ascertain whether the referred to manner of determination of the BO is sufficient and whether there are any reasonable doubts about the conformity of the obtained information (please see the ways of obtaining information necessary for customer due diligence in Sub-chapter 3.1.3.2). It shall be necessary to mandatorily verify the information, if there are data at the disposal of the institution, which contradict that which is specified in the registers.

226. In the event of increased MLTPF risk (for example, the company is registered abroad and its economic activity is associated with high risk, the customer's behaviour creates doubts as to the authenticity or justification of the provided information, etc.) it shall be insufficient to merely clarify the percentage breakdown of the capital shares of the customer, which is an indicative parameter for determination of the BO and does not automatically mean that a person who owns at least 25 per cent of the company is its BO. The BO may also be another – third-party. The institution shall determine whether the specified BO is formal and whether the customer is **controlled in any other manner by** another person or the business relationship is established in the favour and in the interests of another person. The institution shall take commensurate measures in accordance with the MLTPF risk in order to determine a person controlling the customer, for example, shall obtain additional information from the customer, shall verify information in the publicly available sources, etc.

227. In cases of increased risk, when one natural person owns the majority of capital shared (more than 50%), it might be necessary to also determine other natural persons who own the capital shares of the customer (for example, publicly available information shows that a person who owns

[23] In accordance with Section 195.[1] of the Criminal Law a person who knowingly commits the provision of false information to a bank which is authorised by law to request information regarding the BO may be held criminally liable and a criminal penalty may be imposed thereto.

[24] In practice, information can also be obtained from websites where up-to-date data from the Register of Enterprises are available.

less than 50% of capital shares is the BO of the customer). If the institution incurs doubts as to whether a person who owns the largest number of capital shares is the person who controls the customer, and if the increased risk is inherent to the customer, it would be necessary to also determine and assess other persons who own the capital shares of the customer, in order to determine a person who ultimately controls the customer (for example, to assess whether there are any family ties, personal ties among such persons that may be used to conceal the ultimate BO).

228. Taking the structure of the enterprise into account, if possible, it might be important to identify all the shareholders in cases where none of the shareholders (owners of capital shares) holds 25% shares and they have the rights to represent the customer individually or jointly with other persons, since the control of shareholders over the customer is implemented through the representation rights. Thus, it shall be necessary for the institution to assess which shareholder has control over the customer (for example, five natural persons each hold 20% of the capital shares and three out of five holders, are on the customer's Executive Board, and each of them has the right to represent the customer individually).

3.5.2. Ascertaining the BO

229. The institution, in its policies and procedures, on the basis of risk assessment, shall set the criteria, in which cases and under which procedure it ascertains the genuineness of the declared BO, *inter alia*, shall define the features which might be indicative of the possibility that the customer or the BO thereof acts in favour of a third person (for example, the registered owners and BOs of the company in the public registers does not coincide with the ones specified to the institution, the customer or the BO is unable to provide a motivated explanation about the origin of wealth and funds, the BO does not gain benefit from the company or it is of a minimum amount and is not proportionate to the turnover of the company; the company has large planned turnover, but the previous activity of the BO is not related to the relevant field of business).

230. The institution shall verify the BO using a risk-based approach prior to the commencement of the business relationship as well as through the first enhanced due diligence. During the next business relationship, the institution needs to verify the BO if, in assessing the information in its possession, there is any doubt that the BO identified is indeed a BO. Exceptions are providers of life insurance or other services related to the accumulation of funds (including insurance intermediaries) who, in accordance with the Law, have the right to verify the BO even after the commencement of the business relationship, but not later than at the time when the beneficiary begins to exercise the rights specified in the insurance contract. Doubts about the BO can be considered justified if, when evaluating the customer's activities during the relevant period or monitoring the customer's transactions, circumstances occur that may indicate that the identified BO is not a real BO (for example, public information indicates that the customer could act in the interests of a third party; the BO does not have the relevant knowledge and resources to do business, all matters are handled by another person, such as a family member (if there is no understandable justification).

231. As regards the gaining of benefit by the BO, the institution must take into account the fact that, based on the economic activity and the form of the customer, the BO does not always gain benefit from the company in monetary expression. The institution would have to assess what kind

of benefit the BO gains. If the profit of the BO is of the minimum amount, the institution shall assess why the profit is not generated and whether the absence of profit is appropriate and normal practice in the relevant field.

232. When defining the cases and actions to be taken, in order to ascertain the BO, the institution must use the risk-based approach. In cases when a low MLTPF risk is present, the ownership structure of the customer and its economic activity is transparent and economically justified and the volumes of transactions are insignificant, the institution may as well not take additional measures for verification of the BO. Even in cases where within the framework of regular enhanced due diligence after assessment of the customer's activity in the relevant period, the customer's activity is clear and understandable to the institution and there are no indications that the identified BO is not a real BO, no formal information is required from the customer.

Example
The customer is a resident of the Republic of Latvia, the company has been operating for a long time already, the risk thereof is low, the type of activity is not to be classified as an increased risk activity, no risk increasing factors are detected, the volume of transactions is insignificant. The customer is registered in the Republic of Latvia, the economic activity of the customer is not of an increased risk, and no material tangible investments are necessary for carrying out the economic activity of the customer, it is a company engaged in the creation and selling of handicrafts.

233. If an increased risk of MLTPF is identified, further due diligence is required. In cases when the additional due diligence does not eliminate the suspicions regarding the activity of the customer in the interests or in the favour of another person, the business relationship shall not be commenced or shall be terminated, or the occasional transaction shall not be performed.

234. The purpose of ascertaining the BO is for the institution to obtain confirmation that the specified BO is not specified formally and is really gaining benefit from the activity of the company. When ascertaining the BO, the institution, on the basis of risk assessment, shall apply various measures. One of the possible measures to be applied, if it corresponds to the actual circumstances, is to obtain additional information about, for example, previous professional experience and education of the BO and to compare it to the publicly available information or to clarify the property status of the BO, by obtaining information about the tax payments performed by the BO (for example, by obtaining the tax returns submitted in the country of residence of the BO).

235. By obtaining additional information, the institution may ascertain that the specified BO is the actual BO, or, to the contrary – assessing information, *inter alia*, documents, the suspicions that the specified BO is not the ultimate BO can be proven. To ascertain the genuineness of the BO, it is important not only to obtain documents and information, but also to verify them on their merits and in terms of logic, for example, by comparing information obtained from the customer and from

public registers with the substance and volume of transactions performed by the customer and the cooperation partners of the customer[25].

236. It shall be necessary to assess the documents and information, and the documented final conclusions of the due diligence must be well-reasoned and justified with particular facts, namely, how the information and documents obtained by the institution justify the fact that the BO determined by the institution really is the BO of the customer.

237. One of the criteria for ascertaining the conformity of the BO of the customer, which is applied on the basis of risk assessment (for example, in cases, when the institution has reasonable doubts as to the genuineness of the BO of the high-risk customer or increased risk customer, whose BO concurrently is the authorised person of the customer), and which can be analysed, is the IP addresses, from which the login to the internet bank is performed. Nevertheless, in such a case it shall also be necessary to assess, whether the persons using the internet bank are the legal representatives of the customer, namely, authorised signatories, accountants, etc. (hired persons). The use of the IP address check is an effective way to ascertain the conformity of the BO to the results of the due diligence of the institution, to detect the country of residence of the customer, as well as to help detect the groups of connected customers and to better understand the transactions performed by the customers. For example, when detecting that legally unrelated business partners or customers perform login to their internet bank from the same IP addresses, it must be assessed whether it is indicative of the fact that these customers are actually managed (and the benefit is gained) by the same persons.

Example

Determination and assessment of the property status of the BO: it is necessary to obtain and assess information that the property status of the determined BO is proportionate and corresponding to the volume of transactions of the customer and the specified BO can really be the BO of the customer. By requesting information or documents supporting the wealth of the BO, the institution shall assess and set the period for which the information or documents are required for it, considering the actual circumstances, to be able to understand and ascertain the property status of the BO. If the wealth of the BO has been formed many years ago (for example, 15 years ago), it shall be necessary for the institution to also consider the regulation in effect at the time, when requesting information (whether according to the regulation there must have been documents about the specific transaction, whether there is a duty to retain them, to submit them to corresponding public authorities, whether the BO has already declared his or her income to the tax administration, etc.).

The verification of gaining benefit from the activity of the company by the BO is one of the elements that may serve as measures for ascertaining the BO. Nevertheless, gaining benefit in property terms is not necessarily present in all cases.

238. It shall be necessary to describe in the policies and procedures of the institution the actions and processes to be performed exactly according to the specificity of operation of the institution

[25] Please see more about the ways of obtaining information in Sub-chapter 3.1.3.2.

and the customer risk (for example, when the documents are necessary, when it is sufficient to obtain the explanation of the customer, when - information from public sources, to what extent, etc.).

239. With respect to BO verification, by using the risk-based approach, it shall be necessary to also ensure sufficiently documented and clearly justified conclusions about essential issues, such as origin of funds, origin of wealth, obtaining property benefit from the customer or explanation about the circumstances, why the property benefit is not being obtained, affiliation between the customer and the country where the business relationship is established or occasional transaction or economic activity is performed. It shall be necessary to assess whether information gathered by the institution contains contradictions and creates suspicions that the ultimate BO is being concealed.

Example

The BO of the customer has changed, and the indications inherent to the changes cause suspicions about the concealment of the BO.

Situation No. 1
The customer *P.Limited*, at the moment of opening of the account in February 2017, specified V.T. as the BO. In the customer due diligence conducted by the institution in 2017 it was concluded that the change of the BO has taken place and the BO of the customer is D.Z.

As a result of the customer due diligence, the institution has documented that, considering the fact that since the moment of opening of the account the company has not been very active and it was not intended to be used within the structure of the group of companies, V.T. and D.Z. are long-term friends and business partners, they were working together in the nineties of the twentieth century in a foreign company X, V.T. transferred the ownership rights in the company P.Limited to D.Z. without remuneration.

In such a situation, when ascertaining the BO, it would be necessary to assess whether the transfer of ownership rights of the company without remuneration is formal conduct, also additionally assessing publicly available information.

Situation No. 2
The customer is a foreign company, the type of economic activity – investment activity in IT projects. The BO specified by the customer was born in 1945. The BO of the customer is a housewife, the origin of funds – borrowed funds. The son-in-law of the BO is specified as a consultant in the planned business, on whom there is public information available that he is an entrepreneur in another country and has established and is managing several large companies.

Factors to focus on in this situation:
- the type of activity of the customer is investments in IT projects and the customer has specified that the borrowed financial resources will be used for the performance of the activity;
- the son-in-law of the BO specified by the customer will provide consultations with respect to the activity of the customer.

Within the scope of customer due diligence, it would be necessary to assess whether the BO specified by the customer is acting in the interests of a third person, for example, son-in-law, by obtaining information about the economic or professional activity, education, previous professional experience of the BO, to ascertain that the BO has corresponding knowledge and experience, in order to operate in the field of investments with respect to the IT projects.

240. Regarding customers-capital companies that are 100% owned by the Latvia or the local government of Latvia, as well as legal persons of Latvian public law and their institutions, the institution shall ascertain the true beneficiaries (natural persons) by obtaining information on the senior management of the institution.

3.5.3. Determination of a complex customer structure

241. Aspects that may be indicative of a complex customer structure entail several levels of owners; moreover, the owners come from various jurisdictions (for example, legal person owned by several other legal persons, which are also owned by further companies) and such companies are registered in various jurisdictions.

242. On the basis of risk assessment, if the company has a complex ownership and governance structure (for example, the customer is registered in the country, where no public registers of shareholders are available and there are several nominal owners within the censorship structure; the customer is a company registered in an EU Member State and it has several owners – legal persons, whose legal form encumbers the determination of their owners and BOs (for example, the funds)), the institution would have to request that the customer submits the scheme of ownership and governance structure. In such cases, it is important to understand each level within the company structure.

243. Where the ownership structure is complex but traceable, and it is possible to determine the BO of the customer, such customer per se would not be automatically considered as an increased risk customer, because a complex ownership structure may be justified by business specificity and is not prohibited per se.

244. To determine whether or not the ownership structure of the customer is to be considered as complex and such that increases the customer risk, it shall be necessary to assess not only the number of levels of ownership structure and the jurisdictions of the owners, but also whether or not such structure allows for the determination of the BO. If, notwithstanding several levels of owners and their jurisdictions, it is still possible to determine the BO of the customer, besides the economic activity of the customer is understandable and does not create doubts for the institution; the structure of the customer alone should not increase the customer risk. The structure might be complex, but still transparent. In turn, in cases when the structure is complex and the determination of the BO of the customer is encumbered, this is to be deemed as a factor increasing the customer risk.

Example

Situation No. 1
The customer, who is a SIA (Limited Liability Company) registered in the Republic of Latvia and owned by another company registered in the Republic of Latvia, which, in turn, is further owned by the company registered in a Scandinavian country (the ownership structure of several levels is present), with information about the BO whereof being available in the public registers of the relevant country and whose economic activity is clear (for example, wholesale network with chain stores throughout the Republic of Latvia), would not have to be automatically considered as an increased risk customer, on the basis of its ownership structure.

Situation No. 2
The customer-legal person owned by another company registered in the Republic Latvia, which, in turn, is owned by an offshore company with nominal directors and with respect whereto there is no information about the BO available in the registers of the relevant jurisdiction, may be considered to be a customer with a complex ownership structure, which increases the customer risk. In addition to this circumstance, it would be necessary to also assess the economic activity of the customer and other information obtained within customer due diligence, in order to assess whether any other circumstances are existing that would demonstrate an increased MLTPF risk or create suspicions about the MLTPF (for example, having assessed the economic activity and ownership structure of the customer, the reasons for the formation of such structure are not clear).

3.5.4. BO – a person who holds a position in the executive body

245. Only in cases where all the possible means of clarification have been used and it is not possible to clarify the BO, and also doubts are excluded that the legal person or legal arrangement has a different BO, may the institution consider the person holding the position in the customer's executive body to be the BO of the customer.[26] In that case, the institution shall identify the representative of the customer's executive body who has the power to take management decisions. For a lower risk customer, it would be sufficient to obtain information about the representative of the executive body. Higher-risk customers would need additional due diligence to make sure that the person is actually making management decisions (for example, about the right of the *Chief Executive Officer* to decide on the management of the customer's assets). In such a case the institution shall justify and document the actions that it has performed to clarify the customer's BO. It shall not be necessary for the institution to obtain consent from the person holding a position in the executive body of the customer, for him or her to be specified as the BO.

Example

The fund manager registered in the Republic of Latvia acquires the units of the fund registered in an EU Member State and being correspondingly supervised and controlled. The fund is public and operates in the regulated market. The fund securities are being bought by various persons through the intermediation of a credit institution in a EU Member State. Forests in Latvia are being bought for the obtained money.

[26] Pursuant to Section 18, Paragraph seven of the Law, the terms "presumed BO" and "BO" are separable, therefore the amount of information referred to in Section 18, Paragraph two of the Law would not apply to BO within the meaning of Section 1 (5) of the Law.

Taking into account the possibility of the fund manager to determine the BO of the fund is encumbered, the fund manager may consider the senior management of the fund to be the BO of the fund, correspondingly justifying and documenting the actions taken for the determination of the BO of the customer.

246. A person holding a position in the executive body is a person controlling the company and adopting decisions on behalf of the company. For example, in the case of a joint stock company, such person is the chairperson of the Executive Board, the member of the Executive Board (depending on the authorisation to act, for instance, if the Executive Board consists of five members, each of whom is entitled to represent the customer separately, all members of the Executive Board shall be specified); as regards the capital company established by the state, the senior management of the capital company would have to be considered to be the BO, namely, the Executive Board; in the institutions or public authorities where decisions on behalf of the authority are adopted by the Supervisory Board – members of the Supervisory Board.

247. In cases when a person holding a position in the executive body of the customer is to be considered the BO of the customer, when carrying out enhanced customer due diligence and ascertaining whether the determined BO of the customer is the BO of the customer, it shall not be necessary to obtain information of the same nature as in cases when the customer has a BO, who gains actual benefit from the company. In the case of a presumed BO, It shall be necessary to ascertain that there is no change in the circumstances under which the BO of the customer, who is a legal person or legal arrangement, has been identified by the institution as a person having a position in the executive body of the customer, and whether the actual BO is being concealed. The institution indicates in the system that the person is a presumed BO.

248. The institution would have to use the risk-based approach and describe in its policies and procedures the necessary volume of information to be analysed and documented, for the institution to be able to confirm that it has performed the gathering and analysis of information corresponding to the risk, which gives confidence and does not create any doubts as to the ultimate BO, namely, there are sufficiently documented conclusions and the gathered information does not contain any contradictions and no suspicions arise that the ultimate BO is being concealed.

3.5.5. Identification of the real beneficiaries – customers – associations

3.5.5.1. Definition of the true beneficiary in associations

249. Section 1, Clause 5 of the Law states that the **BO is a natural person** who is the owner of the legal person or **who controls the customer**, or on whose behalf, for whose benefit or in whose interests the business relationship is being established or an individual (occasional) transaction is being executed, and it is at least regarding legal persons – a natural person who owns, in the form of direct or indirect shareholding, more than 25 per cent of the capital shares or voting stock of the legal person **or who directly or indirectly controls it.**

250. As indicated on the website of the Register of Enterprises[27], the law does not contain special regulations regarding the specified obligations depending on the nature, type or purposes of the legal person's activity. A legal person is a legal fiction in which, in all cases, the natural persons operate, who organise, direct or control it, therefore a situation in which there is no real beneficiary is not possible – **it may simply not be possible to determine it according to the definition provided by law.** Consequently, the Law does not provide for a situation in which a legal person does not have a real beneficiary. In addition, it should be noted that in situations where it is not possible to determine the true beneficiary, credit institutions as well as other subjects of the Law are obliged to consider (technically presume) a person holding a position in the executive body as the true beneficiary in accordance with Section 18, Paragraph seven of the Law. This means that the persons who have the right to make financial decisions and exercise day-to-day control in the association are identified as BOs, and the institution shall record that these persons are presumed BOs.

251. The purpose of identifying the true beneficiary in the case of associations is to identify the person who effectively controls the customer and makes decisions to identify and manage the risk associated with the use of the customer, MLTPF. Persons who seek to use the association for unauthorised activities often form organisations in which they hold control positions to make the necessary decisions to implement their intentions. Consequently, it is important for the institutions to find out the controlling persons of the association in order to carry out their due diligence and supervision of transactions in accordance with the risk of the association.

252. The aim of the association is determined in the Articles of Association, and it is limited to compliance with the Constitution, laws and international agreements binding on Latvia, and may be directed to the public benefit, its members' interests. In order for an association to have a public benefit purpose, the association does not have to be registered as a public benefit organisation. In cases where the members of the association are working to achieve their individual goals, it is necessary to assess how many members there are in the association. Accordingly, **in the case of associations, if their members only exercise their rights as members of the said legal persons and the purpose of the association is aimed at the public benefit or the purpose of the association is aimed at members interests, but the number of members is large, it will not be possible to identify the true beneficial owners unless those legal persons actually control specific natural persons according to the definition of the beneficial owner.**

Example

Situation No. 1

The association is set up to achieve the goals of individual members, for example, to organise sports activities, hunting, etc. for individuals or their children. This does not apply to associations established for the purpose of providing sports or leisure activities to a wide range of persons. If the association is established in the interests of certain persons, then the beneficial owners are those specific persons for the purposes of which this association has been established, and they should be indicated in the Register of Enterprises as the beneficial owners.

[27] https://www.ur.gov.lv/lv/patieso-labuma-guveju-skaidrojums/biedribas-arodbiedribas-politiskas-partijas/.

Situation No. 2
The association (joint real estate management) has eight members – both natural and legal persons – all of whom are active members of the association. The association operates to achieve the goal set in the statutes. The executive body of the association acts in accordance with the statutes of the association, general meetings of the members of the association are held, and the members of the association have actual opportunities to influence the activities of the executive body, incl. decide to change it. In this situation, it will not be possible to determine the beneficial owner.

Situation No. 3
The members of the association no longer actively exercise their membership rights. The association used to be active, but its activities are no longer relevant to the members and they no longer participate in the activities of the association. Members' meetings do not take place, and in fact the association is an empty shell. At the same time, the assets of the association are still used by a member of its executive body in accordance with its interests and decides on the disposal of the association's property, thus exercising effective control over the association. In this situation, as the association continues to operate, the beneficial owner, given that the members no longer exercise their rights, will be a member of the executive body.

253. Following the aforementioned information, each association shall assess the situation individually, i.e., it should be examined whether the association's activities are aimed at supporting the general public, promoting events that are in the interests of the general public or a large number of members, or the association is chosen as a legal form and its activities are carried out in the interests of a limited number of specific persons. In most associations, if they are established and operate according to the nature of the association's status, it will not be possible to identify the beneficial owners.

3.5.5.2. Identification of the beneficial owners of associations in the Register of Enterprises

254. The executive body of the association is obliged to find out whether the received (clarified) information about the beneficial owners is true, and even if the association concludes that it is not possible to find out the beneficial owner, it shall be able to substantiate it. If it is not possible for the association to find out the beneficial owner, because either the number of such persons is large or the association acts in the interests of the general public, this conclusion shall be made by the association in the person of its executive body.

255. In accordance with Section 22 of the Transitional Provisions of the Law, all legal persons, incl. associations registered in the register kept by the Register of Enterprises or for which the application for registration was submitted by 01.12.2017, had to submit the application for their beneficial owner to the Register of Enterprises by 01.03.2018, in accordance with Section 18^2, Paragraph two of the Law.

3.5.5.3. Responsibilities of credit institutions in identifying and verifying the beneficial owners

256. In accordance with the requirements of the Law, when conducting customer due diligence, a credit institution shall in all cases take steps to find out the beneficial owner of the customer. In cases where the risk is higher, the credit institution shall also verify that the identified beneficial owner is indeed a beneficial owner.

257. Pursuant to Section 18, Paragraph three of the Law, a credit institution shall identify the beneficial owner using information or documents from the Register of Enterprises, and in addition, based on a risk assessment, the credit institution shall identify the beneficial owner in one or more of the following ways: upon receipt of a statement approved by the customer regarding the beneficial owner; using information or documents from the information systems of the Republic of Latvia or foreign countries; independently ascertaining the beneficial owner, if the information about it cannot be obtained otherwise.

258. In view of the above, a credit institution shall use the information from the Register of Enterprises to determine the beneficial owners of legal persons registered in Latvia. If the information is not available in the Register of Enterprises, the credit institution may also use a statement approved by the customer about the beneficial owner to determine the beneficial owner. The lack of information in the Register of Enterprises can be assessed as a factor increasing the customer's risk, taking into account the fact that all legal persons were obliged to identify the beneficial owners by 01.03.2018.

259. In a situation where the beneficial owner is registered in the Register of Enterprises or the customer independently confirms its beneficial owner or that it is not possible to determine the beneficial owner of the customer, the credit institution shall take into account the customer's risk level and, if necessary, identify the beneficial owner independently.

Example
The association is also the sole member of several limited liability companies. The previous member of this limited liability company was a member of the executive body of the association. In this situation, it is necessary to assess whether the association is not used to hide the beneficial owners in limited liability companies, carefully assessing the information about the beneficial owner of the association itself.

260. In accordance with Section 18, Paragraph one of the Law, a credit institution shall in all cases ascertain the beneficial owner of the customer, whereas in accordance with Section 18, Paragraph seven of the Law [28]in a situation where all possible means of ascertainment have been used and it is not possible to ascertain any natural person – the beneficial owner within the meaning of Section 1 (5) of the Law – as well as there is no doubt that the association has another beneficial

[28] The norm referred to in the legal framework is determined in accordance with Section 3 (6) (II) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 684/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

owner, a credit institution may ascertain a person holding a position in the executive body [29]to be the beneficial owner of the association, duly substantiating and documenting the actions taken to identify the beneficial owner.

261. Considering the above, if a credit institution, performing the identification of the beneficial owner independently or in accordance with the information registered in the registers kept by the Register of Enterprises, concludes that it is impossible to identify the beneficial owner of the association because it does not exist within the meaning of the Law, it presumes the person who holds a position in the executive body of the association as the beneficial owner of the association and registers it in the system. It should be noted that in cases where a credit institution may consider a person holding a position in the executive body of an association to be the beneficial owner, that person shall not change his or her status or acquire additional rights or obligations. This activity is performed on the basis of the statutory obligation of the credit institution and is aimed at ensuring the operation of the credit institution's ICS by conducting customer due diligence measures. The mere fact that a credit institution indicates that the person is considered to be the beneficial owner does not confer any additional rights or obligations to the person.

262. Section 18, Paragraph seven of the Law provides that a credit institution may consider a person holding a position in the executive body of the association to be the beneficial owner, but in these cases the credit institution does not have to receive a statement signed by the association. Namely, these persons are presumed to be the beneficial owners on the basis of the Law, and are not in fact the beneficial owners. At the same time, this does not deprive the association of the right to submit a certified statement on the beneficial owner, which the credit institution may use in the process of identifying the beneficial owners in such cases.

263. In accordance with Section 18, paragraph 3^1 of the Law, the credit institution is required to report to the Registrar of Enterprises, which sends the relevant report to law enforcement authorities, about situations where the information on the beneficial owner ascertained in the course of the customer's due diligence does not correspond to the information registered in the registers kept by the Register of Enterprises.

264. The fact that the customer's BO ascertained by the institution does not correspond to the BO registered in the Register of Enterprises may be assessed as a risk-increasing factor, therefore it is necessary to assess its impact on the customer's MLTPF risk.

3.5.6. The determined BO does not correspond to the BO registered in the Enterprise Register

265. Taking into account the fact that within the determination of the BO, by verifying data in the ER, it shall be necessary for the institution, on the basis of risk assessment, to apply additional measures, there might be situations where the institution detects that the publicly available information about the BO contradicts the information obtained by the institution, by taking additional measures for the determination of the BO. The referred to circumstance is to be assessed

[29] In accordance with the term “the natural person (s) who holds the position of senior managing official (s)” used in Directive 2015/849, as well as the purpose of indicating the person who is considered to be the beneficial owner, in this case the management body shall mean the highest management body of the association, the board.

as a risk increasing factor, and it shall be necessary to take corresponding enhanced due diligence measures for the management thereof.

266. Only upon completion of the enhanced due diligence measures and having obtained confidence that the detected information about the BO does not correspond to information registered in the registers maintained by the ER, the term prescribed in Paragraph 3.[1], Section 18 of the Law occurs for the duty to immediately, but no later than within a period of three business days, report the discrepancy to the ER.

267. In the case of a discrepancy between the information in public registers and that which is provided by the customer, the institution applying the enhanced due diligence measures, may also ask to submit additional information and carry out additional due diligence measures, to ascertain that the information provided by the customer about the BO is true.

268. The circumstance that the information specified in the ER does not correspond to the information obtained and clarified by the institution, is also to be assessed as an increased risk in the further management of the risks inherent to the customer. If, as a result of the enhanced due diligence, the institution detects a suspicious transaction, it shall report it to the Financial Intelligence Unit and resolve upon the termination of the business relationship.

269. In addition, the institution, pursuant to the provisions of the Law, shall report the discrepancy between the information about the BO of the ER and the information about the BO clarified by the institution to the ER, under the procedure prescribed by the ER guidelines.

270. The institution must distinguish the nature of the discrepancy:
270.1. whether the detected discrepancy is, for instance, a spelling mistake or other type of mistake;
270.2. whether it is a discrepancy, in terms of substance.

271. The ER guidelines provide for the explanation of the ER as to the situations in which, and how to report that information is probably incorrect in terms of substance, and when – a spelling mistake is detected in the information. Additionally, the ER has also explained the situations, when the difference in information shall not be considered as a mistake and, therewith, it shall not be necessary to report the discrepancy. The explanation is available here: https://www.ur.gov.lv/lv/patieso-labuma-guveju-skaidrojums/kludas-metodika/.

272. When detecting that information about the BO at the disposal of the institution does not correspond to the information about the BO registered in the ER (spelling mistake, incl., insignificant differences in information identifying the person, *inter alia*, information of the personal identification document) and such discrepancy does not create suspicions that the BO of the customer specified in the ER might be another person, the institution shall inform the ER about the detected discrepancy.

273. In situations when the institution has determined and ascertained the BO in accordance with Paragraph 7, Section 18 of the Law (the BO shall be considered to be a person holding the position in the executive body of a legal person or a legal arrangement), but the registers maintained

by the ER contain the feature that “it is not possible to determine the BO” or “the BO is the shareholder in the joint stock company with the stock being listed on a regulated market, and the type of implementation of control over the legal person arises out of the shareholder’s status”, it is not justified to report possibly false information about the BO.

274. In practice the situations are possible, when the discrepancy has been detected between the BO presumed by the institution, within the meaning of Paragraph 7, Section 18 of the Law, and the BO specified in the ER. For example, pursuant to Paragraph 7, Section 18 of the Law, the institution specifies as the BO a person holding the position in the executive body of such legal person; in turn, the head of the management body of the holding company of such legal person is registered as the presumed BO in the ER. In such cases, the discrepancy shall not be assessed as a discrepancy in terms of substance, but rather as the difference in the information about the presumed BO at the disposal of the institution and the one registered in the ER. Thus, it shall not be necessary to report the discrepancy in terms of substance.

275. When detecting the discrepancy in terms of substance, the institution would have to assess what further measures are to be taken to manage the risk. If the institution has taken appropriate measures and has ascertained that the determined BO is the BO (for example, the change of the BO has recently taken place, the customer has submitted the documents attesting thereto and the institution has assessed them and ascertained the conformity thereof), then it shall be necessary to report the discrepancy to the ER. The ER shall correspondingly assess whether the recently performed change of the BO has been applied for registration and would be resolved upon the submission of a further report to the State Police. In such situations, it shall not be necessary to mandatorily apply the risk management measures, for example, enhanced supervision. In turn, in cases when it is not possible to ascertain the BO or the submitted information is not sufficient to ascertain this, the institution shall report it to the ER and consider this circumstance when assessing further cooperation with the customer and determining the applicable types of risk management measures, for example, enhanced supervision, in the case if the cooperation continues. Detection of the discrepancy per se shall not automatically mean the termination of a business relationship with the customer; however, such decision of the institution is possible, on the basis of risk assessment.

276. When detecting the record in the ER that the discrepancy is existing between the BO determined by the ER and by another subject of the Law, it must be noted that there is no information available as to the justification of such discrepancy. Therewith, the record per se shall not be considered to constitute the requirement to terminate the business relationship with the customer, on whom there is a record in the ER that another subject of the Law has detected a discrepancy. Primarily, the determination of the BO remains the duty of the subject of the Law within the particular business relationship, and the circumstance that the referred to record has been detected, forms an additional element within the scope of the due diligence to be assessed jointly with other circumstances, in order to conduct a holistic customer assessment.

277. Upon the coming into effect of the requirement of the Law to report to the ER regarding the non-conformity of the BO to the one specified by the ER (from 1 July 2020), there is no duty imposed on the institution to carry out the reassessment of the entire existing customer base. At the same time, it should be noted that Paragraph 3, Section 18 of the Law prescribes that, when

determining the BO of the customer, information and documents from the ER shall be mandatorily used. Therewith, the institution, as soon as the necessity of any type or the duty arising out of laws and regulations occurs to clarify or update information about the BO (for example, within the scope of an enhanced due diligence), must be used and the information about the BO registered in the registers maintained by the ER and the corresponding actions must be taken in the case of discrepancies in information.

3.6. Business relationship with the customer, who is a politically exposed person (PEP)

3.6.1. Determination of the PEP

278. The enumeration of the PEP positions specified in the Law is of a descriptive nature and is not exhaustive, because it is not possible to enumerate all possible positions which are to be considered as exposed.

279. When assessing the question of significance (exposure) of a position held by the person, it is necessary to assess whether the position enables the person to influence the decision-making in public sector that could serve as a basis for other people to be interested in corrupting or bribing the relevant person or the person could use the publicly significant powers granted thereto for obtaining personal benefit in another manner (abuse of public power).

280. The circumstance that the PEP may dispute the decision and the adopted decision is not final, shall not affect the fact that a person holding positions prescribed by the Law or another significant (exposed) public position, would not have to be considered as the PEP. The PEP status shall not be applicable to the middle level and lower level officers.

Example

Situation No. 1
Land Registry judges

The Law prescribes that the judge of the Constitutional Court, the Supreme Court or the court of other level (member of the court authority) shall be considered to be the PEP. The Land Register's departments are also included in the composition of the district city courts. They record the real estate objects in the Land Register sections and corroborate or register the rights related to such real estate objects. Rights (title) to the real estate are corroborated on the basis of the decision of the judge of the Land Register.

When determining whether the Land Register judge is to be regarded as the PEP, it shall be necessary for the institution to assess whether this position allows the influencing of decisions in the public sector. The circumstance that the Land Register departments are included in the composition of the district city courts does not mean that the Land Register judges are to be regarded as PEPs. At the same time, given the presence of certain factors (for example, high customer risk, certain volume of transactions of the customer and the model of performed transactions), the institution may consider the customer, who is the Land Register judge, to be a PEP.

Situation No. 2
Honorary consul

When determining whether the honorary consul of the Republic of Latvia in a certain country would have to be considered a PEP, it shall be necessary for the institution to assess whether such position allows the influencing of any important decision. The honorary consul or general consul of the Republic of Latvia shall be a person to whom the Republic of Latvia entrusts the performance of state representative and consular functions, on the basis of a special mandate of the Minister for Foreign Affairs (the State Secretary of the Ministry of Foreign Affairs), thus such person fulfils representative and consular functions without any decision-taking powers.

281. Even though the Law provides for enumeration with respect to persons considered to be family members of a PEP, it must, nevertheless, be considered that a person not included in the number of persons considered to be a family member of a PEP, may be a person closely related to a PEP (for example, if a PEP and a person are in an unregistered marriage). The institution shall apply the notion "other close relations" individually, based on the assessment of information at its disposal and risk assessment. When adding content to the notion of a "person closely related to a PEP", the institution must assess whether there are such trust and commitment relations existing between its customer and a PEP that may form the grounds for a PEP, through such person, to conceal the abuse of public authority for gaining private benefit. To determine whether the customer corresponds to the status of a person closely related to a PEP, information at the disposal of the institution would have to be assessed within the context of the transactions planned by the relevant customer and the volumes thereof, to assess whether the cooperation may create the MLTPF risk.

282. Measures to clarify the status of the PEP must be proportionate to the MLTPF risk of the customer and the financial services provided to it. Customers with a very low MLTPF risk with limited access to the service would not need to check the compliance of their PEP status (for example, a parking payment transaction with a very low MLTPF risk and taking steps to ascertain the status of the PEP and verify compliance would be disproportionate to the risk inherent to such a transaction). For low-risk customers, the compliance check of the PEP status is sufficient by processing the customer questionnaire and checking the compliance in the publicly available database of the State Revenue Service (the information is updated once a day). If the institution has information indicating that PEP status may exist, it shall conduct enhanced customer due diligence. For high-risk customers, the institution applies additional measures, including the evaluation of publicly available information, the evaluation of information obtained through regular enhanced customer due diligence, and the use of commercial databases to verify that the customer is not a member of the PEP family or a person closely associated with the PEP.

3.6.2. Scope of enhanced due diligence to be applied to a PEP

283. In accordance with the Law a PEP, a family member of a PEP or a person closely related to a PEP shall be subject to enhanced due diligence. Nevertheless, the enhanced due diligence measures shall also be applied to a different level of depth, based on the risk - depending on the actual circumstances, information obtained within the scope of the customer due diligence and transactions performed by the customers.

Example

The customer is the state capital company or the local government, and the BO thereof is considered to be a person holding a position in the management body of the capital company or the local government, for example the mayor of the city municipality.

In such a case, the officer of the executive body, when fulfilling the official duties entrusted thereto, is acting in the interests of the public. The manifestation of risk from a business relationship with the customer, who is, for instance, the local government, even though its BO is to be considered to be a person deemed to be a PEP, differs from the risk inherent to the customer, who is, for instance, the company registered offshore, whose BO is the member of parliament of a foreign country, gaining benefit as the actual BO. Therewith, the risk for the customer whose BO is a PEP actually gaining benefit from the activity of the customer differs from the risk present in the situation, when the BO of the customer is considered to be a person holding position in the executive body of the customer and exactly due to such position is to be deemed a PEP. Thus, the measures applied to the institution in such situations must correspond to the risk.

284. The risk and, therewith, the applicable enhanced due diligence measures may also differ, by assessing which jurisdiction the PEP comes from – the Republic of Latvia, a EU Member State, a third country. For example, the risk of the customer, who is a company registered offshore and whose BO is the resident - PEP - of a country with high corruption risk, may be higher than that of the customer, who is a resident of the Republic of Latvia and whose BO is a resident of the Republic of Latvia and considered to be a PEP, because there is a risk present that the company, whose BO is a PEP in the country with high corruption risk, through such a company, attempts to launder funds outside the borders of the country, the origin whereof is probably related to corrupt practices. To assess the risk, it shall be necessary not only to consider the circumstance that the BO is a PEP, but also to assess the activity of the customer as a whole (economic activity, substance of transactions). Not all of the customers, who are themselves (natural persons) or whose BOs (legal persons) are considered to be PEPs, have an identical risk, therefore the scope of the applicable due diligence would differ as well, based on the risk of the particular customer.

285. The Commission has provided its recommendations with respect to the determination, due diligence and transaction screening of PEPs, their family members and persons closely related thereto in its Recommendations No. 55 of 2 March 2016 “Recommendations for Credit Institutions and Financial Institutions to Establish and Research Politically Exposed Persons, their Family Members, and Closely-related Persons and to Monitor Transactions” (available at: https://www.fktk.lv/tiesibu-akti/kreditiestades/fktk-izdotie-noteikumi-2/citi-ieteikumi/ieteikumi-kreditiestadem-un-finansu-iestadem-politiski-nozimigu-personu-to-gimenes-loceklu-un-ar-tam-ciesi-saistitu-personu-noskaidrosanai-izpetei-un-darijumu-uzraudzibai/). The referred to recommendations can be used not only by credit institutions, but also by other institutions, insofar as that which is stated therein is applicable to the activities of such institutions.

3.7. Origin of funds and origin of wealth

286. Verification of the origin of funds and wealth of the customer is the risk assessment-based measure. The institution, based on the MLTPF risk of the customer, shall define the applicable measures, and it shall be the duty of the institution to prove that the measures taken by it (for example, the obtained explanation of the customer, obtained documents or publicly available information) correspond to and are commensurate with the risk inherent to the customer.

287. When assessing the origin of the customer's well-being, it is necessary to take into account the fact that the customer has declared the funds in accordance with the Law on Declaring the Property Status and Undeclared Income of Natural Persons, i.e., has submitted a declaration of property status or so-called zero declaration. The origin of the well-being generated 5–10 years ago needs to be assessed if a justified need is identified (e.g., a possible link between the customer or his/her BO and the MLTPF, criminal proceedings are initiated, risk increasing factors are identified, etc.). If the customer submits a document that he or she has declared his or her income in the tax administration of the relevant country, it shall be necessary for the institution to assess the declared amount – whether it corresponds to the volumes of transactions in the institution and whether there are any other risk increasing factors present. When determining the term for researching the origin of the customer's funds, the customer risk scoring, the nature of the transaction, the amount of the transaction, the relevance of the transaction to the customer's economic activity (industry, volume of transactions, permanent business partners of good repute, etc.), limitation shall be taken into account.

288. When investigating the origin of well-being of the customer's legal person (except for the legal person's BO), a general summary on the duration of the company's activities, including turnover, profits, etc., for the last three years is permissible, assuming that the origin of the well-being is the result of the company's economic activity.

289. The origin of the financial resources should be considered in detail in cases where the customer (legal or natural person) enhanced due diligence is due to a specific transaction or activity (including assessing the origin of the customer's well-being) and the origin due diligence period should be comparable to a particular transaction or transactions, e.g., a transaction uncharacteristic of an economic activity in the context of its amount or payment details, including:

289.1. a contribution to the share capital or an increase of more than EUR 50,000, if the increase is more than 50%;

289.2. a loan or its repayment, an assignment agreement (and similar transactions that are not the customer's day-to-day transactions) for an amount exceeding 10% of the annual turnover;

289.3. use of the deposit in case the source of the deposit has not been examined before (enhanced due diligence is performed for the customer for the first time);

289.4. other reasons.

290. When examining the origin of the financial resources of the customer legal persons BO or the origin of funds of natural persons, the basis on which that income has accrued shall also be taken into account. If this basis is clear and follows from the specifics of the business, then an examination of the origin of the income is not useful.

Example

Companies whose shareholders act as partners – audit companies, law firms, etc.

Co-owners of companies, i.e., partners, do not usually become such through acquisitions of shares or share capital investments, but become such as a result of the contribution made to the joint business during the working years, so that the well-being of the partners is most often self-created from zero. In these cases, a specific examination of the origin of the funds is useless, because the basis on which that income has accrued follows from the specifics of the business. An exception is the examination of a specific transaction or provision of these co-owners that is not typical or related to the firm's operations. Usually, the ownership shares determine for the partners the proportion of the potential profit distribution. Often, after termination of their professional activity, partners lose or transfer their ownership shares to other partners.

291. The location of the funds and other circumstances that could significantly affect the customer's ability to provide the information required for the examination should also be taken into account when conducting an examination of the customer's legal person's BO or natural person's funds. At the same time, the institution shall comply with Section 28, Paragraph two of the Law, which stipulates the institution's obligation to terminate the business relationship with the customer and decide on early fulfilment of the customer's obligations if the subject of the law does not obtain the true information and documents necessary for the fulfilment of the customer due diligence requirements specified in the Law to the extent that enables it to perform a substantive due diligence. In such cases, the institution shall also decide to terminate the business relationship with other customers who have the same beneficial owners or to require the early fulfilment of the customer's obligations.

Example

The origin of the funds is a provision in another credit institution, for which the customer submits an appropriate account statement. Accordingly, a large part of the financial resources has been received for several years from the customer's account with another credit institution, for which the customer can no longer submit an account statement (no longer a customer, the credit institution is in another country, visiting the country is difficult in the current situation, etc.). Information on the origin of the customer's well-being is general (positions, jobs, etc.), but the situation as a whole does not give rise to the suspicion of a criminal offence. In this situation, it would not be appropriate for the institution to examine the origin of the customer's funds if the account statement cannot be submitted and the customer is not suspected of a criminal offence in general, as well as no negative information is available and, without receiving this account statement, but it is still possible to conduct substantial customer due diligence, etc.

292. It shall neither be necessary nor proportionate to determine that, with respect to all transfers from another credit institution, the customer account statement must be submitted from the credit institution from which the transfer has been received. The institution may set such requirements, upon the occurrence of certain criteria (for example, for higher risk customers, when reaching the transaction limit defined in line with the risk assessment of the institution or when

detecting other circumstances that may be indicative of the increased risk or evasion from the limits).

Example

Situation No. 1
The customer is a resident of the Republic of Latvia – natural person, a paid employee with the average monthly credit turnover in the amount of EUR 3,000. The customer transfers the amount of EUR 40,000 into his or her account from another institution.

The institution, within the scope of customer due diligence, clarifies that the transferred funds represent a deposit held by the customer in another credit institution, but now he or she has decided to keep the funds in the institution. Additionally, it was clarified that, in 2012, the customer has submitted the property status declaration (the so-called zero declaration), specifying savings in the amount of EUR 30,000.

Having assessed all the information available about the customer and detecting no risk increasing factors, as well as having assessed that the further allocation of funds is corresponding, information obtained within the scope of customer due diligence might be appropriate and proportionate to the customer risk.

Situation No. 2
The customer is a resident of a higher risk country – natural person, the owner of several enterprises, with the average monthly credit turnover in the amount of EUR 1,000,000, the funds are being transferred from the customer accounts in other institutions outside the borders of the Republic of Latvia.

The institution, within the scope of the customer due diligence, clarifies that the customer owns several enterprises registered in the country where high corruption risk is present and it is not possible to obtain additional information about the volumes of economic activity of such enterprise from public sources. The customer specifies revenue from the activity of his or her enterprises as the source of origin of wealth and submits the extracts from returns submitted to the tax administration of the relevant country for the years 2016 and 2015 for the sum equivalent to EUR 700,000.

Information obtained within the scope of customer due diligence is not sufficient for clarifying the origin of wealth. In addition, it would be necessary to obtain information about the economic activity of the enterprises owned by the customer (for example, information contained in public registers, financial statements of the enterprises), the volumes thereof, in order to ascertain that the economic activity of the referred to enterprises is carried out to such an extent that allows the customer as the BO to gain benefit in the amount transferred to the account of the customer. The submitted declarations do not justify the origin of funds held in the account of the customer in the institution, origin.

Situation No. 3

The institution commenced cooperation with the customer E.D., who is a resident of the country where a high corruption risk is present. E.D. transferred into the management of the institution, the financial instruments in the value of EUR 5,000,000, having been transferred from the account of company *M* owned by E.D. (country of registration – an EU Member State, where the services of companies of legal establishment are widely used for the purposes of establishing the enterprises), opened with credit institution *L*. The institution, in order to ascertain the origin of financial instruments owned by E.D., has obtained the documents which, in its opinion, attest to the economic activity of company *M* - an edited statement of the account of company *M* with credit institution *L*, demonstrating separate incoming transactions about the receipt of the payment from the partner of *M*, agent's agreement on the provision of intermediation services to the partner of *M*, from whom the funds were received, separate acceptance and delivery acts on the supply of goods in the country where a high corruption risk is present, and several invoices issued by company *M* to the partner.

Documents obtained within the scope of enhanced customer due diligence are not sufficient to ascertain the origin of the financial instruments. The referred to documents merely reflect the possible fact of cooperation between the shell company owned by the customer and the partner thereof, besides the submitted statement of account demonstrates the receipt of monetary funds in separate transactions, but it is not possible to ascertain whether the relevant financial instruments have been acquired exactly from the referred funds. Within the scope of enhanced due diligence, considering the increased risks inherent to the customer, it would be necessary to assess the need to also obtain an unedited statement of the account that would attest that the relevant financial instruments have been acquired with the funds held therein, and it must be assessed whether the transactions, as a whole, do not have the indications of suspicious transactions, if it were to be detected that company *M* would allocate all funds received for intermediation services for the acquisition of financial instruments, which is not characteristic for normal economic activity and might be indicative of MLTPF.

293. The Commission has provided recommendations with respect to evaluating the origin of funds of the customer and origin of wealth characterising the property status of the customer in its "Recommendations to Credit Institutions for Determining the Source of Customer Funds and Wealth" (available at https://www.fktk.lv/tiesibu-akti/kreditiestades/fktk-izdotie-noteikumi-2/citi-ieteikumi/ieteikumi-kreditiestadem-klientu-lidzeklu-un-labklajibas-izcelsmes-noteiksanai/). The referred to recommendations for determining the source (origin) of customer funds and wealth can be used not only by credit institutions, but also by other institutions, insofar as that which is stated therein is applicable to the activities of such institutions.

3.8. Storage of documents

294. In accordance with the requirements of the Law, it shall be necessary to make copies from the documents, on the basis whereof the customer identification was performed. Copies of the documents shall be used for the institution to be able to prove the grounds, on which the identification was performed, and to further use them to ascertain that the customer, who has arrived in the institution is the same person (for example, when the customer is willing to perform the transaction, the institution, before serving the customer, shall ascertain that the customer presenting the personal identification document is the same person who has already been identified

as the customer of the institution, by comparing the personal data of the customer specified in the presented personal identification document with the data in the copy of the personal identification document of the customer, which is at the disposal of the institution). If the institution can ensure that the system contains information about who has performed the customer identification and scanned the relevant document and when, it shall be acceptable that the identification documents are scanned and not copied.

295. The institution, for a period of five years[30] after the termination of a business relationship or performance of an occasional transaction, shall store the entire information obtained during customer due diligence, as well as information about all payments performed by the customer and correspondence with the customer, *inter alia*, electronic correspondence.

3.9. Supervision of business relationship

296. The institution shall ensure constant supervision of the customer and the transactions performed by the customer, entailing diligent monitoring of the transactions performed by the customer, in order to ascertain that they correspond to the information at the disposal of the institution about the economic or personal activity of the customer and the MLTPF risk level initially determined and assigned to the customer.

297. Depending on the scale, nature of the activities of the institution, number of customers and the share of risk inherent thereto and the volume and number of transactions performed by the customers, it shall be necessary for the institution to introduce such system of transaction supervision that enables the effective detection of suspicious transactions, as well as enables managing the risk for the institution to become involved in the MLTPF or the attempt of such actions. It shall be necessary for institutions with a large number of customers or large number of performed transactions or occasional transactions, or a large share of customers for whose transactions enhanced supervision must be ensured, in order to ensure the effective fulfilment of the AML/CTPF requirements, to introduce an automatic solution for the supervision of transactions performed by the customers. In turn, in institutions with a small number of customers and small volume of transactions performed by the customer, it shall be permissible that the transactions performed by the customers are supervised, by means of manual or partially automated solutions.

298. The institution would have to introduce automatic solutions for the purposes of ensuring that it does not commence a business relationship, as well as does not execute the transactions, within the scope whereof the customer or its cooperation partner is a person against whom any financial restrictions are set. The system of supervision of the actions and transactions of the customers established by the institution must enable one to identify transactions (payments) and conduct untypical for the customer, on the basis whereof the due diligence of the particular situation or transaction would have to be performed, in order to ascertain whether or not the transaction is to be considered as suspicious.

299. To perform high-quality and effective supervision of the customers and transactions performed by them, the institution, when commencing a business relationship, must

[30] In accordance with the provisions of Section 37 of the Law.

correspondingly assess the customer risk level and obtain information corresponding to the risk level about the customer and the economic or personal activity thereof, so that during the business relationship it would be able to correspondingly carry out the supervision of the customers and the transactions performed by them.

300. If the transaction supervision is not ensured by means of various scenarios generating alerts on a possibly suspicious transaction, it is essential that the transaction scenario algorithms are developed in accordance with the products and services offered by the institution and the risks inherent to the customers, and that they are able to timely identify potentially suspicious transactions, enabling the institution to carry out the due diligence thereof and, if necessary, abstain from the transaction or file a suspicious transaction report to the Financial Intelligence Unit.

301. The institution, in its policies and procedures, shall establish a detailed procedure for the performance of transaction supervision, inter alia, shall prescribe the procedure for the review of the scenarios, their effectiveness, for defining the fields of responsibility, etc.

3.10. Correspondent (banking) relationship

302. In accordance with the requirements of the Law it shall be necessary for the institution to perform enhanced due diligence, upon establishing and maintaining the correspondent (banking) relationship with the credit institution or financial institution (respondent). In accordance with the Law the correspondent (banking) relationship shall also be deemed to include the relationship between credit institutions and financial institutions or the relationship between financial institutions, if the correspondent institution provides the respondent institution with the services, including services involving the performance of payments and settlements, or the services similar thereto, according to a mutually concluded contract. Therewith, the financial institution, other than the credit institution, for example, payment institution, when providing payment services to another financial institution, on the basis of a mutually concluded contract, must also observe the requirements set for the performance of enhanced due diligence, correspondingly developing the requirements for the performance of enhanced due diligence for such relationship in its policies and procedures. The purpose of the requirement is to ascertain that the respondent has established an appropriate ICS and, thereby, manage the risk that the institution might be used for the MLTPF, when executing the payments performed by the customer of the respondent.

303. The institution, when maintaining the business relationship with another financial institution, shall ensure the observance of the “know your customer” principle. If the credit institution has defined the customer categories it does not cooperate with, for example, non-licensed gambling organisers, then the credit institution must assess whether the payment or electronic money institution is not serving such customers.

3.11. Enhanced supervision

304. Enhanced supervision is a customer due diligence measure designed to manage the risk of MLTPF by taking additional measures to monitor the business relationship. These measures shall not be applied automatically by the institution when conducting enhanced customer due diligence. They apply depending on the risk, i.e., if the institution identifies an increased MLTPF risk during

the enhanced customer's due diligence (for example, by evaluating the customer's transactions or information available about the customer) and measures are required for the supervision of the customer while the other enhanced customer's due diligence is being conducted.

305. The customer due diligence regulations list the types of enhanced supervision measures. Enhanced supervision measures do not always involve obtaining additional information from the customer. The institution may determine that enhanced supervision measures reduce the customer risk scoring (risk mitigation).

306. The institution may impose enhanced supervision measures outside the enhanced due diligence if this is appropriate to the MLTPF risk inherent to the customer. It is important that the institution also provides for this right in civil law agreements concluded with the customer.

3.12. Information on the grounds for termination of the business relationship and financial refund to the customer

307. When an institution terminates a business relationship with a customer, there may be several scenarios for terminating the contract and repayment of the balance of funds to the customer:

307.1. termination of the business relationship on the basis of Section 28 of the Law;

307.2. termination of the business relationship in compliance with the general terms and conditions of the transaction;

307.3. transfer of funds to the account specified by the customer;

307.4. transfer of funds to another customer's account with a credit or financial institution.

308. The conditions listed apply depending on the level of MLPTF risk. The law stipulates that the business relationship shall be terminated if the institution is unable to complete the substantive due diligence due to a lack of information. FATF Recommendation 10 requires a business relationship or occasional transaction to be terminated if the institution is unable to conduct customer due diligence.[31] In this context, it is necessary to assess whether the reason for the refusal to provide financial services is a materialised MLTPF risk (for example, an institution identifies signs of a MLTPF (rather than a probability)) or the institution's prudent MLTPF risk management (risk policy or decision not to take MLTPF risk inherent to a particular business relationship).

309. If the institution establishes the occurrence of an actual MLTPF risk, due to which the institution cannot continue cooperating with the customer, the grounds for termination shall follow from Section 28 of the Law, which further involves the obligation to repay the customer's funds by transferring them to the customer's account with another credit or financial institution in order to prevent MLTPF risk. The justification provided to the customer may also be the general terms and conditions of the transaction, provided that they provide for a right of termination in a situation where the institution does not accept the customer's inherent MLTPF risk.

310. In other situations, the institution shall terminate the business relationship in accordance with the terms of the agreement between the customer and the institution.

---

[31] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

! Repayment of the funds to the customer, when terminating the business relationship, is also a customer transaction that is subject to supervision, i.e., if an institution determines that it has reasonable suspicions about MLPTF, it refrains from the transaction and reports to the FIU.

Typical situations and good practices of institutions in terminating a business relationship or not performing an occasional transaction

Situation No. 1

The institution has refrained from the execution of transactions to the customer's account and has reported to the FIU. After the FIU examination, the institution receives a reply that the refraining was justified, but the FIU does not decide to continue the refraining (the origin of the refraining funds is not entirely related to the offence or the amount of the refraining funds is relatively insignificant, etc.)) and instructs the Institution to terminate the refraining. The institution shall terminate cooperation with this customer due to a reasonable suspicion of money laundering.

Action by the institution:

- **grounds for termination of cooperation** – reference to Section 28 of the Law;
- **The requirements of Section 43 of the Law** – applicable.

Situation No. 2

In a short period of time, the customer carries out significant transactions to the credit institution's account with the transit features of payments, which is the basis for initiating enhanced due diligence. The enhanced due diligence cannot be completed in substance because no significant explanations or documents have been received from the customer.

Action by the institution:

- **grounds for termination of cooperation** – reference to Section 28 of the Law;
- **The requirements of Section 43 of the Law** – applicable.

Situation No. 3

Enhanced due diligence is initiated for the customer (one or more risk criteria – complex structure, high-risk transactions, etc.). During the due diligence, the customer is asked clarifying questions, including the submission of up-to-date documents describing the economic activity, which reflect the transactions for the examination period.

The customer replies that part of the requested documents will not be provided, as the institution can mostly ascertain the cooperation partners indicated in the request from public sources, the requested documents describing economic activities are confidential, and the customer has not violated any law to explain its activities to the institution. There is no clear suspicion that the customer has carried out suspicious transactions, however, there is no complete clarity about the nature of the customer's transactions, therefore a decision is made to terminate the cooperation.

Action by the institution:

- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

Situation No. 4

The institution has conducted enhanced customer due diligence and, in the opinion of the institution, obtained reasonable and sufficient information to consider that sufficient due diligence has been performed. Public historical negative information is available about the customer or the customer's BO, as well as transactions that may be related to the relevant information have been identified. There is no information on any procedural action (administrative or criminal) and the institution has no reason to refrain from executing transactions. However, the institution shall decide to terminate the cooperation.

Action by the institution:

- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

Situation No. 5

The institution has conducted enhanced customer due diligence and, in the opinion of the institution, obtained reasonable and sufficient information to consider that sufficient due diligence has been performed. The customer's turnover is mainly formed by transactions with Central Asian partners, and they exceed the risk appetite of the institution or the ability to qualitatively manage the specific risk. As a result of the due diligence, a decision is made to terminate the cooperation.

Action by the institution:

- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

Situation No. 6

The customer is a financial service provider whose risk appetite exceeds the risk appetite of the institution (serves a sector of economic activity whose representatives are not directly served by the institution), or the institution has identified significant, long-term deficiencies in the financial service provider's ICS.

Action by the institution:

- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

Situation No. 7

The institution has sent more than one report to the FIU on individual suspicious customer transactions in the medium term, which are isolated and small in relation to the total turnover of

the customer. As far as the institution can find out, no further action has been taken on these reports, but a number of reports may be a reason for the institution to decide to terminate the cooperation with the customer.

Action by the institution:
- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

Situation No. 8
Previously, enhanced due diligence revealed that the customer could **potentially** have signs of envelope pay. Repeated enhanced due diligence shows that the situation has not improved significantly.

Action by the institution:
- **grounds for termination of co-operation** – reference to the general terms and conditions of transactions;
- **The requirements of Section 43 of the Law** are not applicable.

3.13. Providing information to customers

311. Institutions are restricted by law from disclosing information about reporting to the Financial Intelligence Unit and the further evaluation and pre-trial process of the information provided in the report. This obligation is also laid down in Directive (EU) 2015/849[32].

312. Institutions have an obligation not to disclose information to the extent necessary to ensure that, in cooperation with the customer, the institution does not disclose information that may make the customer prudent about the identified possible MLTPF and thus impede the successful implementation of government and law enforcement actions.

313. In practice, institutions may need to explain to a customer the reason why it is necessary to provide information in order to conduct customer due diligence or to justify the termination of a business relationship. Informing the customer facilitates cooperation with the customer, obtaining the information necessary for MLTPF risk management and the availability of financial services.

314. When evaluating the obligation specified in the regulatory framework and its purpose, the institution may provide the following information to the customer:

314.1. information regarding the requirements of regulatory enactments, explaining why it is necessary to submit information or why the business relationship shall be terminated;

314.2. information regarding the deficiencies in the submitted information, indicating the purpose of obtaining them;

[32] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 684/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

314.3. in the event that cooperation is to be terminated due to incomplete information, information regarding the nature of the missing information;

314.4. information regarding the customer's MLTPF risk mitigation measures that may be applied to continue the business relationship.

315. The institution shall not disclose the following information related to MLTPF risks:

315.1. information on the customer's inherent MLTPF risks (indications that may indicate a suspicious transaction) that it has identified and the circumstances that it examines;

315.2. information regarding the risks due to which it terminates the business relationship or does not execute the transaction;

315.3. the fact of reporting to the Financial Intelligence Unit (including refraining from executing the transaction).

316. The institution may provide details in so far as it relates to information required from the customer, as well as the MLTPF risk mitigation measures, at the same time carefully monitoring that the actions taken by the institution and the conclusions drawn from the examination of possible suspicious transactions are not disclosed. For example, an institution may disclose that cooperation with the customer may be continued by setting restrictions on payment countries and limits, as the risk associated with transactions with increased-risk jurisdictions will be managed.

Example

An incoming transaction performed on the customer's account, the amount of which significantly exceeds the monthly limit of transactions specified for the customer, requires research to obtain information on the nature of the transaction and assess the legal and economic purpose of the transaction. The institution shall explain to the customer that, taking into account the size of the transaction, it is necessary to obtain more information in order to ascertain that the transaction complies with the legal and economic purpose specified in the requirements of regulatory enactments. The institution shall ask the customer to submit the required documents, giving examples of the documents to be submitted. The institution may explain to the customer the need for information on the nature of the transaction (contract, parties to the transaction, other circumstances surrounding the transaction). The institution shall not disclose information about the risks inherent to the transaction (indications that may indicate a suspicious transaction) as well as the circumstances of the transaction, which it shall further examine. If an institution finds that the circumstances for reporting to the Financial Intelligence Unit have occurred, it shall not disclose the fact of reporting or the risks it has identified, but shall indicate to the customer that the information provided is insufficient to obtain assurance on the legal and economic purpose of the transaction.

4. Information technology solutions for management of MLTPF and sanction risk

317. The institution shall use IT solutions to assess the scope of its services and, consequently, the need to automate and improve effectiveness of MLTPF and sanction risk management measures. The customer due diligence regulations set out general principles for IT solutions for

credit institutions that may be applied by other institutions in proportion to the risks inherent to their operations.

318. To meet MLTPF and sanction risk management requirements, IT solutions streamline and ensure the processing of customer information, the operation of a customer risk scoring system, compliance with the term of customer due diligence processes, transaction monitoring processes, compliance with sanctions lists or identification of politically exposed persons.

319. Automated control over the completion of mandatory fields of information necessary for the identification of the customer, its owner, beneficial owner, authorised representative and other customer and for the management of economic and personal activities, as well as solutions for checking correctness (for example, control of the value of the number of the year of birth, control of the existence of the country of residence, etc.) provides the necessary information to identify the risk factors inherent to the customer and to assess the MLTPF and sanctions risk. Automated alerts on the expiry of the identity documents of the customer and its authorised person allow the institution to identify the need to update the customer's data and to take risk management measures in accordance with a risk-based approach.

320. In order to ensure the collection of historical information about the customer and the due diligence conducted by the institution, the institution shall provide solutions for the storage and availability of this information for further customer due diligence.

321. Depending on the size and specifics of the business, the institution uses technological solutions to identify interconnected customers and to assess the economic activity of customers (for example, to analyse customer cash flow schemes and document results). Credit institutions, depending on the scale of their activities, need automated solutions after BO to determine connected customers. Automated solutions for the selection of connected customers facilitate the identification of the customer-related group, but it is necessary to further assess whether the relationship is also substantive.

322. In order to ensure customer due diligence in accordance with the customer's MLTPF and sanction risk, IT solutions are required for the availability of information on the risk categories and application of risk mitigation measures, as well as ensuring compliance with risk mitigation measures (e.g., partners, countries, limits).

323. In addition to transaction monitoring IT solutions for customer relationship monitoring, it is necessary to provide solutions for keeping the suspicious transaction reports and correspondent bank requests in order to be able to select and evaluate them.

324. As part of the additional measures for MLTPF risk monitoring, the institution, depending on the size and specifics of the activity, shall establish and maintain the lists of internal customers and potential customers, their beneficial owners and authorised representatives, for whom information is available in connection with involvement in MLTPF, including lists of persons with whom a business relationship has not been initiated or is terminated in accordance with the procedures prescribed by law (indicating why the business relationship has been terminated or has not been initiated). The institution shall verify the compliance of the institution's customers,

beneficial owners and authorised persons with those lists when entering into the business relationship and during the business relationship.

325. The regulation provides for credit institutions' automated screening of customers and their beneficial owners, authorised persons and participants against sanctions, lists of politically exposed persons, their family members or persons closely associated with politically exposed persons prior to entering into a business relationship and creating alerts if a match is identified. During the business relationship, to check the risk of sanctions in a timely manner, the lists of sanctions should be checked at least once a day; in turn, the institution shall check the lists of politically exposed persons, their family members or persons closely related to politically exposed persons to the extent appropriate to the risk, and its regularity may be less frequent for lower risk customers. With regard to the verification of payment information for the management of the sanction risk, it is permissible that in cases where the customer sanction risk is low (low-risk domestic payments, such as utility payments), the verification of payment information shall be performed by the institution in a risk-based manner, checking the originator or payee against the lists of sanctions.

326. The requirements for the performance of an independent external audit (Commission Regulation No. 148 of 01.09.2020 "Regulations on Conducting an Independent Assessment of an Internal Control System for the Prevention of Money Laundering and Terrorism and Proliferation Financing") also include an independent evaluation of IT solutions. Before carrying out an audit, the institution shall agree with the Commission on the scope of the audit and may set a longer term for the audit of IT solutions. When deciding on the harmonisation of the term, the Commission shall take into account the conclusions of the Commission's most recent due diligence and the steps taken by the institution[33] to remedy the deficiencies, if any.

5. Reporting to the Commission (quarterly reports, requests)

327. Frequently asked questions of the credit institutions and responses of the Commission regarding the preparation of the "Report on the MLTPF Risk Exposure Description" (hereinafter referred to as – the Report) (other institutions shall observe these principles in a manual request report, whenever applicable):

Question	Explanation by the Commission
"On the definition of the "customer":	
a) whether it shall also entail the persons having no deposits in the credit institution	Persons carrying out occasional transactions in the credit institution (for example, currency exchange, payment of public utilities, tax payments, fines, etc. payments without establishing business relationship) in accordance with the Commission Regulations on the MLTPF Risk Management, shall not be considered to be customers.

[33]Institutions covered by Commission Regulation No. 148 of 01.09.2020 "Regulations on Conducting an Independent Assessment of an Internal Control System for the Prevention of Money Laundering and Terrorism and Proliferation Financing".

	Escrow account funds are reflected in the report as follows – an escrow account is opened in the name of a specific person: - it may be an existing customer of a credit institution; - it may be a third party who is not a customer of the credit institution. If the escrow account service is provided to an existing customer of a credit institution, then the movement or balance of funds in the escrow account shall be reflected in the Report as transactions between the accounts of one customer. If the escrow service is provided to third parties who are not customers of the credit institution, then: - the person, in whose name the escrow account is opened, until all the conditions of the transaction have been met, the transaction is not completed and the escrow account is not technically closed, shall be considered a customer and shall be presented in the Report; - the movement and the balance of funds in the escrow account must also be shown in the Report, i.e., the money transferred to the escrow account (in the name of a third party) will be the customer's *credit turnover*, as well as *financial assets*, *incl. deposit* until the transaction is completed and the credit institution accepts the transfer of funds from the escrow account to another third party with another credit institution.
b) whether the number of customers includes customers whose accounts in the credit institution have been closed, but there is an account balance remaining	The Report must also specify data about the customers, with respect whereto the credit institution has taken a decision to terminate the cooperation (customers, whose accounts are closed, but there is an account balance remaining).
c) credit obligations and the assignment agreement taken over from other credit institutions – should they be included in the number of customers (i.e., a person has no current account in the credit institution, a separate loan repayment account is being opened for each customer and the credit institution gains income)	If the credit institution has taken over the credit obligations from another credit institution or under the assignment agreement, and henceforth the credit institution performs the supervision of repayment of such loans, the borrowers taken over shall be regarded as the customers of the credit institution and data about them shall be specified in the Report.

d) whether the number of customers entails customers with temporary accounts	The customer having accounts opened for the registration of a share capital before the enterprise is being registered with the ER and where the amount of the share capital has been paid into (it is not possible for the enterprise to perform any outgoing payments before the enterprise is registered in the ER), shall be reflected in Annex No. 1 to the Report both in the total number of the customers and in the assets and turnover thereof, but the country of the BO of such customers may be specified in Annex No. 6 to the Report according to the country of registration of the enterprise.
e) whether the group companies of the credit institution with the accounts opened in the credit institution are considered to be customers	The group companies of the credit institution shall be considered to be customers.
Regarding deposit platform customers – such customers shall be identified by the credit institution of the EU Member State and they shall only have deposit accounts opened, without access to any other services of the credit institution. Must the deposit balances of such customers be disclosed in the Report as "customers identified by intermediaries"?	Deposit balances of the customers identified by the credit institution of the EU Member State must be specified in the Report in the Section "Customers identified by intermediaries" (also specifying data in the relevant fields of row 010 "Total customers" of Annex No. 1).
Income disclosure in column 110–140 of Annex No. 1 to the Report	Income gained from the customers/customer transactions shall be disclosed (income from economic activity of the credit institution shall not be included in the Report).
What should one do, if the customer has changed the country of residence during the reporting period – which country must the relevant customer be referred to?	The institution shall assess the country of residence of the customers/BOs of the customers, as well as the legal form of the customers at the end of the reporting period and must specify the relevant data (number, balance, turnover, income). For example, if during the reporting period the customer has changed the legal form and at the end of the reporting period the customer has become a financial institution, the turnover (and income) for the entire reporting period shall be referred to the financial institution.
Completion of Annex No. 6	Annex No. 6 to the Report is comprised of three separate tables with different information, using the county code as the uniting element, to be specified in

	column 010. The first table, where information about the BO is to be specified in breakdown by countries, contains column 020-040. The second table, where (irrespective of the data in the first table) information about the PEP shall be specified, contains column 050-070. The third table (irrespective of information specified in the first two tables) shall specify information about the enhanced due diligence customers in breakdown by countries.
Disclosure of BOs and PEPs in Annex No. 6 in the Report	When disclosing data about the number of BOs of the customers-legal persons and, correspondingly, assets and credit turnover, the proportionality principle shall be applied, namely: - if one customer (legal person) has one BO, the credit institution shall indicate 1 in the Report for the relevant country of registration; - if one customer (legal person) has two BOs from different countries of registration, the credit institution shall proportionately indicate 0.5 in the Report for the relevant country of registration (for example, RU 0.5 and LV 0.5); - if one customer (legal person) has three BOs from different countries of registration, the credit institution shall proportionately indicate 0.33333 in the Report for the relevant country of registration (for example, RU 0.33333, UA 0.33333 and LV 0.33333), etc. The sum of all decimal parts shall be specified in the Report opposite the relevant country. The assets and volumes of turnover shall also be disclosed in an analogous way. Column 050, 060, 061, 070 of Annex No. 6 to the Report (customers based on the PEP status) shall disclose data in breakdown by countries of registration about the customers – natural persons, who shall themselves be considered to be PEPs, or family members of PEPs, and/or persons closely related to a PEP, as well as about the BOs (natural persons) of the customers legal persons and legal arrangements, which are to be considered to be PEPs, in breakdown by countries, applying the same proportionality principles as the one applied to the BOs of the customers.
Completion of Annex No. 7	The credit institution, when completing (filling out) Annex No. 7 to the Report, shall provide information

	about the customers (shell arrangements and other) at the end of the reporting quarter, with respect whereto it has adopted the decision on termination of the business relationship (after assessing the MLTPF risk) and who still have the balance, namely, with respect to all (closed accounts with the balance), irrespective of whether the decision was adopted in the first, second or another reporting quarter.

6. Sanctions and prevention of financing of terrorism and proliferation

This section explains the types of sanctions and lists the signs of breaches. Practical examples and principles of good practice have been compiled, which institutions can use as a model for conducting customer due diligence and monitoring customer transactions in order to identify and prevent the risk of breaches of sanctions in a timely manner. The objectives, risks and characteristics of terrorism and proliferation financing are also explained in order to help institutions manage these risks and ensure compliance with regulatory requirements.

6.1. General information on sanctions

328. **Sanctions** are restrictions set in accordance with regulatory enactments regarding the subject of sanctions. Sanctions shall be imposed by an international organisation or state in relation to the state, territory, legal or natural persons or other specifically identifiable subjects (hereinafter referred to as – a subject of sanctions).

329. The purpose of sanctions is to restore international peace and security and to change the behaviour of the subject of sanctions in order to achieve the objective of the sanctions. Consequently, the purpose of sanctions is to restore the legal situation, to prevent the possible deterioration of the situation, as well as to terminate the illegal activities of the subject of sanctions. The purpose of sanctions is not to penalise the subject of sanctions.

330. According to the regulations in the field of sanctions in Latvia, the institution shall comply not only with international and national sanctions (terminology in accordance with the International and National Sanctions Law of the Republic of Latvia (hereinafter referred to as – the Sanctions Law)), but also the restrictions imposed by the sanctions of the North Atlantic Treaty Organization (NATO) and the EU member state, which significantly affect the interests of the financial and capital markets. The purpose of the Sanctions Law is to ensure peace, security and justice in accordance with Latvia's international obligations and national interests by introducing international sanctions, imposing national sanctions or applying sanctions imposed by a member state of the EU or the North Atlantic Treaty Organization in the cases specified in this law[34].

[34] Law On International Sanctions and National Sanctions of the Republic of Latvia, available at: https://likumi.lv/ta/id/280278-starptautisko-un-latvijas-republikas-nacionalo-sankciju-likums.

! *General information on sanctions, including their types and application, a list of sanction databases and other detailed information is available on the website of the Ministry of Foreign Affairs*[35].

NB! *The Ministry of Foreign Affairs is the competent institution for communication with international organisations and other competent institutions regarding the determination, implementation of sanctions and application of exceptions in Latvia. The competent institution for the supervision of financial market participants (including the issuance of the necessary authorisations and advice on the application of sanctions) is the Commission. The competent institutions for reporting violations of sanctions are the State Security Service (violations of sanctions and circumvention) and the Financial Intelligence Unit (circumvention, considering that there may also be a risk of MLTPF in these cases), as well as the Commission in the context of supervision.*

6.2. Types of sanctions

331. According to the Sanctions Law, there are five different types of sanctions that can be imposed on any subject of sanctions. Prohibitions that institutions shall comply with may include the obligation to block (freeze) the assets of the subject of sanctions or not to provide financial services. According to the Sanctions Law, the following types of sanctions are possible:

331.1. **financial restrictions** – restrictions regarding financial instruments and financial resources that are owned, possessed, held or controlled by the subject of sanctions, including the provision of financial services to the subject of sanctions;

331.2. **civil law restrictions** – a prohibition to acquire and dispose of tangible and intangible things in respect of which property rights or other economic rights are to be registered, confirmed or disclosed in public registers in accordance with the specified restrictions;

331.3. **entry restrictions** – restrictions on the subject of sanctions to enter, stay in Latvia or cross the territory of Latvia in transit;

331.4. **Restrictions on the movement of goods of strategic importance and other goods** – prohibition on the subject of sanctions to sell, supply, transfer, export or otherwise dispose of or allow access to certain types of goods of strategic importance or other statutory goods, if an arms embargo or a prohibition on the import, export, transit or brokering of other goods is imposed on the subject of sanctions;

331.5. **Restrictions on the provision of tourism services** – a prohibition on the provision of tourism services for travel to specific areas.

6.2.1. Types of sanctions directly binding on market participants

6.2.1.1. Financial restrictions

332. According to the Sanctions Law, one of the most important types of sanctions enforced by an institution is financial restrictions. According to the Sanctions Law, if a person is subject to financial restrictions, the institution is obliged to:

[35] Ministry of Foreign Affairs of the Republic of Latvia, website: https://www.mfa.gov.lv/lv/sankcijas.

332.1. freeze all funds and financial instruments that are owned, held or controlled, directly or indirectly, in whole or in part, by the subject of sanctions, incl. the financial resources and financial instruments transferred to third parties;

332.2. deny the subject of sanctions access to financial resources and financial instruments;

332.3. not provide the financial services specified in the international or national sanctions to the subject of sanctions (including by using authorisation).

333. The institution is obliged to check whether its customers include persons whose name, surname and other identifying information coincide with the information provided in the sanctions databases, and to take the necessary actions in accordance with the scope of the specific sanctions regulation. If the regulation in question provides for the immediate freezing of all funds and economic resources (hereinafter referred to as – the funds), the funds shall be frozen as soon as the United Nations (hereinafter referred to as – the UN) Security Council (hereinafter referred to as – the SC) resolution, EU regulation or national sanctions entered into force, i.e., all funds belonging to, owned, held or controlled by the persons listed on the sanctions lists shall be frozen. The frozen funds will be released when the sanctions are lifted. Freezing does not change the ownership of the frozen funds.

! *Definitions of "ownership", "control" and "indirect" are given in the European Commission's document on EU best practice for the effective implementation of restrictive measures "Update of EU Best Practices for the Effective Implementation of Restrictive Measures"*[36].

Example

Situation No. 1

Using a risk-based approach, the institution finds that its customer A initiates a transaction in which the beneficiary is a foreign-based company B, which has a person subject to sanctions in its structure (it owns 17% of company B) that imposes the obligation to freeze all its assets.

Example of insufficient control: the institution does not maintain specific programmes and lists that can be used to establish that the subject of sanctions or its subsidiary or affiliate is indirectly involved in the transaction.

Good practice example: An institution uses extended lists of sanctions for the screening of payments, which contain information on the possible control or participation of the subject of sanctions, and accordingly verifies that the participation of the subject or subjects of sanctions in the payee's structure is only 17% and no more than 50%. Payment accepted.

Example of excessive control: the institution does not conduct an enhanced due diligence of the transaction, does not execute the transaction and reports to the competent institutions.

[36] *Council of the European Union "Update of the EU Best Practices for the effective implementation of restrictive measures",* Chapter VIII, available at: https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf; https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/lv/pdf.

Situation No. 2
The customer, company A, receives the incoming payment from company B. Company C owns 51% of the shares in company B, and is on the EU sanctions list and is subject to financial restrictions.

Example of insufficient control: the institution does not maintain specific programmes and lists that can be used to establish that the subject of sanctions or its subsidiary or affiliate is indirectly involved in the transaction.

Good practice example: the payment is withheld in the institution's screening system due to the coincidence and an investigation is carried out, as a result of which a decision is made to freeze the funds in a separate account and send a report to the Commission and the State Security Service. For customer A, the institution applies the risk-increasing factor and initiates an enhanced due diligence to assess the identified risk of sanctions arising from the business partner, Company B, and to apply the necessary risk mitigation measures accordingly.

Example of excessive control: an institution freezes funds received and terminates a business relationship with customer A.

Situation No. 3
The customer, company A, receives the incoming payment from company B. Company B is controlled by a natural person C, which is included on the EU sanctions list and is subject to financial restrictions. Pursuant to the articles of association of company B, person C is entitled or authorised to appoint and remove a majority of the members of the management body of company B.

Example of insufficient control: the institution does not maintain specific programmes and lists that can be used to establish that the subject of sanctions or its subsidiary or affiliate is indirectly involved in the transaction.

Good practice example: the payment is withheld in the institution's screening system due to the coincidence and an investigation is carried out, as a result of which a decision is made to freeze the funds and send a report to the Commission and the State Security Service. For customer A, the institution applies the risk-increasing factor and initiates an enhanced due diligence to assess the identified risk of sanctions arising from the business partner, Company B, and to apply the necessary risk mitigation measures accordingly.

Example of excessive control: an institution freezes funds received and terminates a business relationship with customer A.

6.2.1.2. Sectoral sanctions

334. Sectoral sanctions are prohibitions on goods and services that include various restrictions on the provision of services, the movement of certain goods, transactions in financial instruments, lending, and so on. Sectoral sanctions are not linked to the obligation to freeze the funds or financial

instruments of specific individuals, they are intended to restrict access to finance, imports and exports of goods, services and technology for certain sectors and can therefore only be identified through customer transaction due diligence (for more information on sectoral sanctions, see Sub-section 5.5).

Example

The economic activity of the institution's customer A is the provision of logistics services (groupage, mainly from Europe to a country subject to sectoral sanctions restricting the supply of a wide range of goods). The company institution customer is a limited liability company registered in the Republic of Latvia.

Example of insufficient control: given that customer A is a company registered in Latvia that operates in accordance with the laws of the Republic of Latvia, the institution does not apply control to customer A's operations.

Good practice example: the institution conducts a risk assessment and, taking into account the sanction risk and transaction size of the customer's business partner, requests documentation and verifies that the customers or the recipients of the goods involved in the transaction are not subject to sanctions, whose activities are linked, for example, to those provided for in sectoral sanctions, and who have the potential to order the supply of such goods (related to sectoral sanctions, dual-use goods, luxury goods).

Example of excessive controls: Given that EU sanctions prohibit the supply of a wide range of goods in a country subject to sectoral sanctions, the institution will require the customer, without a risk assessment, to indicate not only the consignee of the goods but also the subsequent movement of the goods (subsequent purchasers) for all deliveries in the country against which the sectoral sanctions have been imposed, including for non-sanctioned goods, although this is not under the control of the institution's customer.

6.2.1.3. Other types of sanctions

335. With regard to other types of sanctions and ensuring their observance, the institution shall ensure the observance of restrictions in accordance with the scope of the regulatory enactment which prescribes sanctions, as well as assess their impact on the fulfilment of the task of compliance with financial restrictions. In addition to financial restrictions, it may be useful for an institution to consider other types of sanctions when assessing the customer sanctions risk. This can also help to assess and identify situations of circumvention of financial restrictions. The institution shall draw attention to the circumstances that may indicate a violation of sanctions.

6.3. Hierarchy of sanctions regulations

336. In accordance with the Sanctions Law, the financial and civil sanctions specified in the UNSC resolutions and the sanctions specified in the EU regulations are binding and directly applicable in the Republic of Latvia.

337. In accordance with Section 3 of the Sanctions Law The Cabinet of Ministers may, on its own initiative and on the basis of a proposal of the Minister for Foreign Affairs or the National Security Council, impose national sanctions. Sanctions are determined in accordance with Cabinet of Ministers Regulation No. 327 of 09.07.2019 "Procedures for Initiating and Enforcing International and National Sanctions"[37]. In turn, financial and capital market participants shall additionally comply with the Sanctions Rules[38].

6.3.1. Breakdown of sanctions

338. Pursuant to Section 1 of the Sanctions Law, sanctions may be divided according to their determinant:

338.1. **international sanctions** – are restrictions imposed in accordance with the international law in relation to subjects of sanctions, which have been adopted by the UN or the European Union, or another international organisation, to which the Republic of Latvia is a member state, and which are directly applicable or introduced in Latvia in accordance with the procedures laid down in this Law;

338.2. **national sanctions** – are restrictions imposed in accordance with the laws and regulations of Latvia and international law in relation to subjects of sanctions, which have been stipulated by the Cabinet in accordance with the procedures laid down in this Law;

NB! ***United States of America (hereinafter referred to as – the USA) Office of Foreign Assets Control*** *(hereinafter referred to as – OFAC))* *sanctions are neither national nor international sanctions – they are North Atlantic Treaty Organization Member sanctions.*

339. At present, the national sanctions imposed by the Cabinet of Ministers are in force, which have been applied to natural and legal persons in accordance with Cabinet of Ministers Regulation No. 419 of 25.07.2017 "Regulations Regarding the Imposition of National Sanctions in Relation to Subjects Connected with the Nuclear Programme and Political Regime Implemented by the Democratic People's Republic of Korea"[39].

340. UN sanctions are imposed by UNSC resolutions. They are binding and directly and immediately applicable in the Republic of Latvia[40].

6.3.2. EU Sanctions

341. The EU is taking over or implementing UNSC sanctions with a time lag, as well as adopting autonomous sanctions regimes. Sanctions are adopted by the EU through a Council Decision and a Council Regulation (e.g., publication of 17.12.2020 In the Official Journal of the European Union[41]).

---

[37] Available at: https://likumi.lv/ta/id/308141-starptautisko-un-nacionalo-sankciju-ierosinasanas-un-izpildes-kartiba.
[38] Available at: https://likumi.lv/ta/id/316774-sankciju-riska-parvaldisanas-normativie-noteikumi.
[39] Available at: https://likumi.lv/ta/id/292535-noteikumi-par-nacionalo-sankciju-ottieciba-uz-subjektiem-kas-saistiti-ar-korejas-tautas-demokratiskas-republikas.
[40] Available at: https://www.un.org/securitycouncil/sanctions/information;
https://www.un.org/securitycouncil/sanctions/information.
[41] Available at: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=OJ:L:2020:426I:FULL&from=EN.

! EU sanctions are directly and immediately applicable in the Republic of Latvia.

342. The interactive Sanctions Map indicates the types of sanctions imposed by the EU and the UN, the legislation or resolution that adopted the specific restrictive measures, provides an advanced search mechanism, as well as detailed explanations, such as which goods are banned from entering the country, and so on. The Sanctions Map also contains information on EU sectoral sanctions, which is obtained by entering the name of the subject of the sectoral sanctions – the relevant regulation setting these sanctions is indicated. The sanctions map is maintained and developed by the European Commission. The interactive Sanctions Map is available here: https://www.sanctionsmap.eu/#/main.

NB! *Only legal publications in the Official Journal of the European Union are legally binding*[42].

6.3.3. Sanctions imposed by a Member State of EU or the North Atlantic Treaty Organization

343. Sanction regulations stipulate that sanctions imposed by an EU or North Atlantic Treaty Organization Member State whose official currency (other than the euro) is the main source of settlement in international trade and financial markets, and which, if non-compliance with the established sanctions, may significantly impede the access of financial and capital market participants to the international financial settlement system, shall be deemed to have a significant effect on the interests of the financial and capital markets.

344. The institution shall assess the sanctions adopted by the Member States of the EU or the North Atlantic Treaty Organization and the impact of those sanctions on the institution itself or on the materiality assessment of all financial and capital markets.

345. In a situation where the institution finds that the impact of sanctions is significant, it shall assess the risks associated with the imposed sanctions and set appropriate restrictions for the assessment, incl. states that:

345.1. an institution shall not provide services to a person for whom financial restrictions have been imposed (for exceptions, see Sub-section 6.6);

345.2. an institution shall not execute transactions if the party involved is a person subject to financial restrictions.

346. The purpose of these measures is to manage the risk associated with ensuring that the institution cooperates with other financial institutions.

! *Given that compliance with OFAC sanctions significantly affects the interests of the financial and capital market, OFAC sanctions in Latvia are observed both in public procurement in accordance with the Sanctions Law and in financial transactions, taking into account the guidelines of the Latvian Financial Industry Association*[43] *(For more on OFAC sanctions, see Section 6.4.2).*

---

[42] Available at: http://eur-lex.europa.eu/homepage.html?locale=lv.

[43] Available at: https://www.financelatvia.eu/wp-content/uploads/2020/10/AML_CFT_vadlinijas_2020_06_10.pdf.

6.4. Imposition of financial sanctions
6.4.1. National, UN and EU sanctions

347. EU regulations usually impose precise financial restrictions, such as the freezing of all funds and economic resources belonging to, owned, held or controlled by natural persons or natural or legal persons, entities or bodies associated with them (e.g., Section 2 of EU Regulation 269/2014[44]).

348. More information on EU best practices for the effective implementation of restrictive measures is available at https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf.

349. The current opinion of the European Commission on the control of a person over a unit is available on the website https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200619-opinion-financial-sanctions_lv.pdf.

350. If all financial instruments are to be frozen under the sanctions regime, the institution will:

350.1. complete the settlement of all transactions concluded before the entry into force of the sanctions and freeze the funds obtained from the transactions;

350.2. all transactions in derivative financial instruments at market price on the date on which the sanctions came into force shall be closed to prevent fluctuations in the security deposit, which is the collateral for the derivative financial instruments (if open positions are not closed, the money pledged may be lost and the institution may need to compensate the counterparty for losses related to the customer's open position);

350.3. if a customer's transfer of securities order (FOP) has been received before the sanctions take effect, the institution shall revoke the order because the financial instruments held by the institution are still in the customer's possession; if a customer on the sanctions list receives an incoming financial instrument transfer (FOP) after the sanction has taken effect, the institution must execute the transaction and the incoming financial instruments shall be frozen;

350.4. the conclusion of new agreements after the entry into force of sanctions is only permitted after authorisation by the Commission.

! *During the freezing of financial instruments, the financial instruments themselves (number of shares, nominal value of bonds, number of fund units) are considered frozen, but their market value may change depending on market prices.*

351. If the financial instrument is profitable (e.g., dividends, interest income), then the freezing of profits shall also be ensured. If a customer-independent corporate event occurs that results in a change in the type of financial instrument (for example, bonds are converted into shares as a result of a recapitalisation), the institution shall process the event and freeze the new financial instrument (the new financial instrument is a replacement). The owner of financial instruments is not restricted from participating in shareholders' meetings and other corporate events that are not related to the

[44] Available at: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32014R0269.

change of ownership. If an issuer of financial instruments is removed from the list of issuers (bankruptcy of the issuer), the funds received for the financial instruments, if any, are frozen.

352. The institution shall evaluate the relevant international or national sanctions legislation and, in a situation where it provides for the possibility to charge a fee for the financial services provided (e.g., servicing of financial instruments, servicing of a current account containing a person's frozen funds), the institution may implement it in accordance with the terms of the transaction after approval by the Commission.

Example Information is published that the institution's customer is included in the list of EU subjects of sanctions, according to which all financial resources must be frozen. The institution reacts immediately by settling transactions that were concluded before the sanctions came into force and freezes the person's financial resources, as well as closes (suspends) all transactions in financial instruments. As the customer uses an account with an institution, the institution applies to the Commission for separate authorisation to charge commission for maintaining a current account. With the authorisation of the Commission, the institution may continue to maintain the account by charging a fee in accordance with the price list.

6.4.2. OFAC sanctions

353. In a situation where a customer due diligence, including an enhanced due diligence, has revealed information to the institution indicating the possibility of OFAC sanctions being imposed on a person involved in the business, the institution is required to conduct enhanced customer due diligence to confirm or deny that allegation and assess participation.

NB! *Subject of OFAC sanctions directly or indirectly has a 50% participation (an explanation of the 50% principle is available at https://home.treasury.gov/system/files/126/licensing_guidance.pdf).*

354. If, in the due diligence assessment, the institution finds that the customer is owned by a subject of OFAC sanctions, but the participation does not reach the 50% threshold, the institution shall assess the MLTPF and sanctions risk for cooperation with the customer and decide on appropriate risk management measures. These may include cooperating with the customer through enhanced supervision, including the imposition of due diligence measures, restrictions on the provision of services or a decision to terminate the cooperation with the customer if the institution determines that the risk inherent to the customer does not comply with the institution’s risk policy or it cannot manage the risk inherent to the customer.

Example Situation No. 1

The customer, company A, receives the incoming payment from company B. Company C owns 50% of the shares in company B, and is included on the OFAC sanctions list. The payment is withheld in the institution's screening system due to coincidence.

Example of insufficient control: the institution refunds the payment without further evaluation. The institution does not conduct a sanction risk assessment for customer A.

Good practice example: The institution carries out an evaluation and as a result decides to transfer the payment back and send a report to the Commission. For customer A, the institution applies the risk-increasing factor and initiates an enhanced due diligence to assess the identified risk of sanctions arising from the business partner, Company B, and to apply the necessary risk mitigation measures accordingly.

Example of excessive control: the institution transfers the payment back and terminates the business relationship with customer A.

Situation No. 2
Institution's customer A – a legal person engaged in the sale of liquefied gas in Latvia. Customer A makes a current payment to Company B, a company incorporated in the Russian Federation, whose parent company is subject to OFAC sanctions (prohibition on supplying equipment to companies listed in the OFAC Enforcement Order).

Example of insufficient control: the institution's payment screening system did not detect the involvement of customer partner B in sanctions when checking customer A's outgoing payment, as customer B is not on any sanction list and the institution has executed the payment without verification.

Example of good practice: The payment system of the institution's payments has suspended the payment because the payee is a company owned by the subject of sanctions and the payment has reached the institution's employee for verification. The employee of the institution, by checking the match, has verified that the match is true, as well as that the customer has declared this partner at the time of opening the account, and the institution already has a contract previously submitted by customer A with customer B for the purchase of liquefied gas and the employee made sure that customer A regularly makes outgoing payments to customer B and that the contract number is always mentioned in the payment purposes. The employee of the institution sends the transaction to the sanctions analyst for verification without requesting additional documents from customer A. The Sanctions Analyst examines the direct restrictions on customer B and, by making sure that the purchase of liquefied gas is not linked to the supply of equipment to customer B, allows customer A's outgoing payment to be executed without requiring additional explanations or documents from customer A.

Example of excessive control: the payment system of the institution's payments has suspended the payment because the payee is a company owned by the subject of sanctions and the payment has reached the institution's employee for verification. By checking the match, the institution's employee made sure that the match is true and, given that the payee is subject to sanctions, customer A is asked to provide supporting documents (invoice, contract, transport documents,

documents of origin) before making the payment, and customer A is asked to submit a sanctions policy that describes the ICS for compliance with customer A's sanctions. After customer A has submitted all the documents, the transaction is sent to a sanctions analyst for review. The Sanctions Analyst examines the direct restrictions on customer B and, by making sure that the purchase of liquefied gas is not linked to the supply of equipment to customer B, allows customer A's outgoing payment to be executed without requiring additional explanations or documents from customer A.

! *The OFAC Sanctions Database is available at https://sanctionssearch.ofac.treas.gov/, and a list by Sanctions Programme is available at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.*

! *Information on persons subject to OFAC sectoral sanctions is available on the OFAC website https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/sectoral-sanctions-identifications-ssi-list.*

! *In certain situations, OFAC allows derogations from the established sanctions by issuing a so-called General licence indicating the derogations allowed. A list of General Licences can be found at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx in the specific sanctions programme description.*

! *According to the OFAC website https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx#licenses, OFAC issues two types of licences:*

- *General Licence*

General Licence is normally issued by OFAC without the application of the subject of sanctions. *The General Licence* allows financial transactions with the subject of sanctions to be subject to special conditions specified in the relevant *General Licence.* ***An example is provided at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/glomag_gl1.pdf.***

- *Specific Licence*

Specific Licence is a document that OFAC may issue at the request of a subject of sanctions authorising certain financial transactions. The decision of OFAC is not subject to appeal, but a person may make a confirmatory application if there is a significant change in circumstances. ***Specific Licence*** only applies to funds blocked in U.S. financial institutions. *You can apply for a* ***Specific Licence at https://www.treasury.gov/resource-center/sanctions/Pages/licensing.aspx***.

Example

The institution notes that customer A has submitted a payment in favour of its Belarusian partner B. Company B is included on the list of subjects of OFAC sanctions. Examination of the information on OFAC's website reveals that OFAC has issued a time-limited General Licence, which allows financial transactions with subjects of sanctions to be carried out under the specific conditions set out in the relevant General Licence.

The institution finds that the payment corresponds to OFAC General Licence conditions and the General Licence is valid at the time of payment. The institution allows the customer to make the payment.

355. In addition to OFAC's financial sanctions, US sectoral sanctions are also imposed on certain sectors and industries in specific countries, such as the Russian defence and intelligence sector, investment in and financing of energy projects, and are enforced by the US Department of State. For example, Section 231 (e) of the ***Countering America's Adversaries Through Sanctions Act*** (hereinafter referred to as – the CAATSA) establishes a list of persons who are considered to be working in the Russian defence and intelligence sector. Information on Section 231 (e) of the CAATSA list is available at *https://www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation/.* The U.S. Department of State has prepared an explanation of sanctions in the energy sector, available at *https://www.state.gov/key-topics-bureau-of-energy-resources/*.

356. The Commission recommends that market participants pay attention to and assess the need to comply with sanctions imposed by other US authorities.

357. There are no single registers listing persons held by subjects of OFAC sanctions. The Commission has received requests for an explanation as to whether a person should be considered subject to OFAC sanctions. The Commission is not in a position to answer such questions because, firstly, the Commission does not have ownership and control of information obtained from the customer's due diligence and, secondly, the Commission is not empowered by law to provide such an explanation.

358. The Commission is entitled to issue an authorisation for the provision of financial services (authorisation for a specific transaction or type of transaction) on the basis of information obtained from the institution's customer due diligence and submitted to the Commission, if the institution has established that the person is subject to OFAC sanctions and the financial services meet the basic needs of a natural person or the basic economic activity of a legal person.

! *In the event of any questions or concerns, any person may contact OFAC at ofac_feedback@treasury.gov to clarify whether and what restrictions on financial services apply in a particular situation.*

NB! *EU sanctions apply to persons who meet the terms "ownership" (more than 50% ownership) or "control", while the ownership is at least 50% decisive in the application of OFAC sanctions.*

6.5. Sectoral sanctions and the movement of strategic goods

6.5.1. Sectoral sanctions

359. Sectoral sanctions are various prohibitions on goods and services, such as:

359.1. a prohibition to import goods originating in certain regions (e.g., Crimea, Sevastopol) into EU;

359.2. restrictions on trade and investment related to certain economic sectors and infrastructure projects;

359.3. restrictions on the access of certain financial institutions to capital markets;

359.4. the prohibition to export goods and technology specified in the EU Regulation (for example, dual-use goods);

359.5. the prohibition to sell, supply, transfer or export to Russia, directly or indirectly, dual-use goods;

359.6. the prohibition to export, supply, transfer to the People's Democratic Republic of Korea, or import and purchase from it, the goods specified in the Regulation;

359.7. a prohibition to open an account and establish a correspondent relationship with a credit or financial institution for persons domiciled in the Democratic People's Republic of Korea.

360. Specific bans and restrictions are specified in the relevant regulatory enactment, for example, in an EU Regulation and its annexes. The institution shall, in accordance with the relevant general provisions of the laws and regulations governing sectoral sanctions, ensure that it does not provide, directly or indirectly, financial services for the acquisition, supply, transport or export of such goods or services.

361. Information on EU sectoral sanctions is not included on the Consolidated Sanctions List of the Financial Intelligence Unit, but information on persons subject to EU sectoral sanctions is available on the EU Sanctions Map.

362. In order to ensure compliance with sectoral sanctions, the institution shall, on the basis of a sanction risk assessment, assess the information available in the payment document, taking into account the type of payment concerned (perform the screening of incoming and outgoing transactions (payee, payer, their address, screening) prior to their execution) to determine whether the subject of sectoral sanctions is not involved in the transaction and no payment is made or received for goods and equipment subject to sanctions.

363. Under a risk-based approach, an institution may, for example, impose stricter requirements for the verification (screening) of payment information for SWIFT cross-border payments than, for example, for SEPA payments where the geography of the payment movement is limited.

! *The Institution shall pay close attention to clients whose business activities are related to countries or territories associated with the export of goods and services subjected to sectoral sanctions, or are carried out in the vicinity of such countries or territories, and shall ensure that the services provided by the Institution are not used for the supply of prohibited goods and services to persons subject to sectoral sanctions. The institution shall assess those considerations when entering into cooperation with new customers or before providing any new financial services to customers (for example, when attracting a time deposit, given that it may also be the source of income from cooperation with the subject of sanctions, the institution should carry out a risk assessment of the customer's sanctions risk in order to identify appropriate customer due diligence measures).*

Example

<u>Situation No. 1</u>

The customer of the institution, company A, is engaged in gas metering, distribution and filtration reduction technologies. Customer A purchases gas filtration units from Italian manufacturer B and supplies and installs the equipment on the basis of an agreement between customer A and Swiss company C. Place of delivery – Serbia. Project – main gas pipeline on the Hungarian-Bulgarian border.

Example of insufficient control: an institution requests additional information about a transaction, performs due diligence of the party of the transaction against the sanction lists and approves the transaction, given that the parties of the transaction are not on the international sanctions lists.

Example of good practice: the institution requests additional information about the transaction, clarifying the technical specification of the product, the name of the pipeline project, the operator, end users and other necessary information, incl. documentation, and the presence of potential subjects of sanctions in the project and their percentage participation, requesting the consultation of the Ministry of Foreign Affairs and the Commission, if necessary. The institution shall make decision based on the facts and on the views of the competent authorities, taking into account any restrictions imposed by a Member State of the North Atlantic Treaty Organization.

Example of excessive control: an institution fails to execute a transaction and terminates the business relationship with company A.

Situation No. 2
The economic activity of the institution's customer, company A, is the sale of machinery used in various industries. The most important cooperation partner of customer A is company B registered abroad.

Company B is established in a locality in the immediate vicinity of a country subject to extensive sectoral sanctions. Information on the economic activity of company B is not available in public resources.

Example of insufficient control: given that customer A is a company registered in Latvia that operates in accordance with the laws of the Republic of Latvia, the institution does not apply control to customer A's operations.

Example of good practice: After checking the registration addresses of customer A's business partners, the business partner's connection with a populated area in the immediate vicinity of the sanctioned state has been established, the institution will verify the economic activity of company B by requesting additional information, as well as that the end users of the goods supplied to company B are not subject to sanctions whose activities involve the use of goods distributed by customer A in areas subject to sectoral sanctions.

Example of excessive control: institution requires customer A to submit documents of all transactions, incl. those carried out domestically by well-known companies.

Situation No. 3

The economic activity of customer A of the institution is the repair and sale of aircraft engines and parts. Customer A leases two aircraft engines to Turkish company B with the possibility of further subleasing. Turkish company B is a non-aviation company.

Example of insufficient control: an institution requests information about a transaction and checks the parties to the transaction against sanction lists. Upon the receipt of information from customer A that customer A is not responsible for the further use of the goods, the institution shall not apply any additional controls.

Example of good practice: The institution assesses, when requesting documents, whether company B involved in the transaction is the end-user of the product. If there are reasonable doubts about the end-user, the institution shall identify the supply chain of the goods and the final consignee to ensure that the consignees are not subjects of sanctions, the transaction is not linked to a sanctioned country or otherwise inconsistent with international sanctions. If necessary, the institution shall seek consultations from the Export Control Division of Strategic Goods of the Ministry of Foreign Affairs.

Example of excessive control: Given that customer A's economic activity involves the sale of a high-risk product, the institution requires customer A to provide a list of all business partners, indicating the supply chain for each planned transaction and the authorisation of the Ministry of Foreign Affairs' Strategic Goods Export Control Division for each transaction.

Situation No. 4
Negative information is available about the cooperation partner, company X, of customer A in the public sources, that company X has a potential business relationship with companies from Iran.

Example of insufficient control: the institution does not take into account available negative information. Payment for the goods is made from Company X's partner in the United Arab Emirates – Company Z. No transaction documents are required.

Good practice example: An institution requests documents or information on a transaction, the end use and end user of a product, the delivery route, etc., as well as additional information from customer A on company Z's role in the transaction and the applicable sanctions compliance measures for the due diligence of its partners within the framework of the Sanctions Law.

Example of excessive controls: a potential violation of sanctions is reported to the Commission. Payment is declined due to an excessive risk of sanctions. Cooperation with the customer is terminated.

Situation No. 5
The economic activity of the institution's customer A involves the sale of deepwater oil extraction equipment (strategic goods). Sanctions for these strategic goods are linked to a ban on their sale to certain companies subject to sanctions and import into certain countries. Customer A informs the institution that it has a new buyer B from Hungary who intends to purchase the product for a significant amount.

Example of insufficient control: Given that Hungarian purchaser B is not included on the sanctions lists, the institution allows the payment in question without further control.

Good practice example: Given that there is no space in Hungary for the use of deepwater oil production equipment, the institution assesses the geographical risk of customer A, verifies (by requesting customer A's documents) who the final consignee is and decides whether or not to accept payment. The institution shall contact the Ministry of Foreign Affairs to ascertain the necessary permits for the trade and export of goods.

Example of excessive control: an institution, given that the object of the payment is strategic goods, requires customer A to provide the institution with a list of all counterparties of consignee B and an account statement to ensure that consignee B has not received any payments from subjects of sanctions.

6.5.2. Movement of goods of strategic importance

364. With regard to the ban on the export of certain goods and technologies, it should be taken into account that the Ministry of Foreign Affairs controls the circulation of goods of strategic importance in Latvia, which also includes dual-use goods. In the case of import, export or transit of goods of strategic significance, a licence is required that can be obtained by submitting an application to the Ministry of Foreign Affairs. More information is available on the website of the Ministry of Foreign Affairs[45].

! *In order to easily verify that a product is not a dual-use good, the Institution may use, within the framework of client due diligence, the* ***Register of Latvian Customs Integrated Tariff Management System****:*
https://itvs.vid.gov.lv/itms/.

365. Indications that may indicate an increased risk of sectoral sanctions or strategic goods:

365.1. the customer or the customer's business partners are related (for example, operating or registered) to a territory or state border subject to sectoral sanctions, the customer's economic activity is related to the trade, production, export or import of equipment or goods that can be used for military purposes and can be considered as dual-use goods;

365.2. the customer, its beneficial owner or business partner is related to a specific sector, such as the military industry, or specialised foreign agencies (military design bureaux, space technology research agencies, etc.);

365.3. the customer’s economic activity may be related to the military industry (for example, aviation) or the trade in goods (such as coal, grain, flour), which can be used to conceal the operation with prohibited goods;

365.4. the customer has the typical features of a front company (for example, the customer acts as an intermediary in the importation and exportation of goods or raw materials, the extraction of which is specific to a territory or country that is subject to sectoral sanctions; several clients with an elevated risk of sanctions have the same owners, managers, employees or contact details (for

[45] Ministry of Foreign Affairs of the Republic of Latvia, export control of strategic goods, website: https://www.mfa.gov.lv/arpolitika/ekonomiskas-attiecibas.

example, telephone numbers); the customer makes or receives payments for an economic activity that is unusual for the client or region);

365.5. instead of the customer's business partner, the payments are made by third parties who are residents of the territories or countries subject to sectoral sanctions, or the client makes payments instead of the third parties who are residents of the territories or countries subject to sectoral sanctions;

365.6. the customer cooperates with a goods transportation service provider transporting goods in the frontier zone of the territories or countries subject to sectoral sanctions and for which the publicly available information indicates that it provides transport services to companies operating in a territory or country subject to sectoral sanctions (for example, servicing ships in prohibited ports);

365.7. the customer cooperates with a goods transportation service provider transporting goods in the frontier zone of the territories or countries subject to sectoral sanctions and for which the publicly available information indicates that it provides transport services to companies operating in a territory or country subject to sectoral sanctions (for example, servicing ships in prohibited ports);

365.8. the carriage of goods involved in the customer's transactions takes place in regions of high risk on routes that are not precisely traceable in publicly available internet resources **(for example, *Marine Traffic: https://www.marinetraffic.com*)**;

365.9. the price of the goods or services involved in the transactions does not correspond to the average price level in the market, the type of transport or storage of the goods involved in the transaction, the route, packaging or other characteristics do not correspond to the general practice in the sector;

365.10. the customer submits the same documents to justify several unrelated transactions;

365.11. the documents supporting transactions submitted by the customer contain indications of fraud;

365.12. the customer imports and exports the same goods;

365.13. Within the framework of non-cash remittance, funds are transferred or received from countries or territories associated with the export of prohibited goods and services subject to sectoral sanctions or transfers carried out in the vicinity of such countries or territories.

Example

Situation No. 1
Customer, Company A, receives an incoming payment from Company B located in Thailand. Information for the purpose of payment: for goods – spectrometer.

Action by the institution: the payment is suspended in the institution's screening system due to a match with an entry in the dual-use goods list. In its examination of the transaction, the institution concludes that:

- Company A is engaged in the manufacture of special machinery, measuring, testing and navigation instruments and devices;
- Company B is engaged in research and experimental development in biotechnology.

Given that the information on the purpose of the payment indicates the possible involvement of a dual-use item in the transaction, Institution A sends a request for information to the customer with a request to submit:

- an explanation of the nature of the transaction;
- product code and technical specification;
- a special permit or licence, if such is required for the export of goods;
- end-user certificate;
- information regarding the final consignee of the goods;
- contract, invoice, transport documents, if available;
- customs documents.

Customer A submits a strategic goods licence, an end-user certificate, a contract, an invoice, as well as a technical specification and code for the goods.

The institution shall contact the Export Control Division of Strategic Goods of the Ministry of Foreign Affairs to ascertain whether the strategic goods licence is valid.

As a result of the due diligence, the institution decides to accept the payment, as customer A has submitted all the necessary documentation. The institution shall apply the risk increasing factor to the customer A and initiate an enhanced due diligence to assess the risks associated with the customer's economic activity and business partners and to apply the necessary risk mitigation measures accordingly.

Situation No. 2

Customer Company A receives an incoming payment from Company B located in Russia. The purpose of the payment is information: prepayment for the purchase of a machine tool and payment for spare parts. The payment is withheld in the institution's screening system because there was a partial match with a person on the sanctions list, which was a false positive match. The investigation of the transaction concluded that:

- Company A operates in the field of transport services;
- Company B is engaged in the manufacture of fabricated metal products.

Action by the institution: Given that the information on the purpose of the payment indicated the possible involvement of the dual-use item in the transaction, a request for information is sent to the customer with a request to submit:

- an explanation of the nature of the transaction;
- product code and technical specification;
- a special permit or licence, if such is required for the export of goods;
- end-user certificate;
- information regarding the final consignee of the goods;
- contract, invoice, transport documents, if available;
- customs documents.

Customer A submits the technical specification and code of the goods, transport documents, customs documents, contract and invoices.

The transport documents state that the consignor is the Italian company LLL, which manufactures machine tools (CNC Machines) and spare parts, and company B in Russia is mentioned as the consignee. Comparing the goods indicated in the transport documents, it can be seen that only

spare parts have been shipped and the customs documents indicate that the goods are not goods of strategic importance, but the amount of payment is both for spare parts and prepayment for the machine tool. Although Customer A's explanation states that a special permit or licence is not required for the export of the machine tool, the institution still contacts the Export Control Division of Strategic Goods of the Ministry of Foreign Affairs to ascertain the need for a licence. The institution clarifies that the machine tool is a strategic good and that an export licence is required. The institution decides to reject the payment and send the report to the Commission, despite the fact that it was a prepayment and the machine tool had not yet been actually exported. The institution shall apply a risk-increasing factor to customer A and shall conduct enhanced due diligence to assess the identified risk of sanctions arising from its economic activity and business partner company B, and to apply the necessary risk mitigation measures accordingly.

Situation No. 3

The customer, Company A, makes an outgoing payment to Company B, located in France. Information specified for the purpose of payment: drone.

Action by the institution: the payment is suspended in the institution's screening system due to a match with an entry in the dual-use goods list. The investigation of the transaction concluded that:

- Company A's economic activity is related to the agents specialised in the wholesale of other particular products
- Company B is engaged in the wholesale of electronic equipment, telecommunications equipment and parts.

Given that the information on the purpose of the payment indicates the possible involvement of the dual-use item in the transaction, a request for information is sent to the customer with a request to submit:

- an explanation of the nature of the transaction;
- product code and technical specification;
- a special permit or licence, if such is required for the export of goods;
- end-user certificate;
- information regarding the final consignee of the goods;
- contract, invoice, transport documents, if available;
- customs documents.

The customer submits a technical specification of the product, which shows that the drone can fly for more than 30 minutes, as well as can fly in winds of more than 50 km/h. According to the explanation of the Export Control Division of Strategic Goods of the Ministry of Foreign Affairs, such drones are classified as goods of strategic importance. According to the information provided by the customer, the goods are exported from France to Pakistan. As supporting documents for the transaction, the customer has attached an agreement with Pakistani company C, a French strategic goods licence, an end-user certificate mentioning Pakistani company C, as well as transport documents, a contract and other information.

As a result of the due diligence, a decision is made to accept the payment. Given that the goods move from France to Pakistan, the goods licence shall be obtained from the country of exportation of the goods.

The institution shall apply a risk-increasing factor to customer A and initiate enhanced due diligence to assess the identified risk of sanctions arising from its economic activity and business partners Company B and Company C, and to apply the necessary risk mitigation measures accordingly.

! ***More information is available on the website of the Ministry of Foreign Affairs in the section "Control of Goods of Strategic Importance"[46].***

6.6. Application of financial sanctions, violation, circumvention, reporting obligation

6.6.1. Application of Financial Sanctions

366. EU regulations imposing financial restrictions also state that the inflows may be credited to an account of subject of sanctions (crediting of frozen accounts) provided that these inflows are frozen in that account. The institution shall notify the Commission of those transactions without delay. If an institution receives a transfer of funds from a subject of sanctions addressed to its customer, the institution should freeze those funds in a separate account, as rejecting an incoming payment would allow the subject of sanctions to access its own funds.

367. Action of the institution in the execution of transactions, if it finds a coincidence with the subject of sanctions:

367.1. if the party to the transaction is a customer of the Institution – a subject of sanctions – the Institution shall not execute the transaction requested by the customer, repaying funds in the customer's account, and shall ensure freezing of the funds;

367.2. if the beneficiary of the funds involved in the transaction is a customer of the Institution – a subject of sanctions, but the party to the transaction is a person who is not a subject of sanctions – the Institution shall execute the transaction and freeze the funds received in the customer's account;

367.3. if the customer initiates a transaction in which the beneficiary is a person – a subject of sanctions – the Institution shall not execute the transaction and shall repay the funds in the customer's account;

367.4. if the transaction has been initiated by a person who is a subject of sanctions and the beneficiary is a customer who is not a subject of sanctions – the Institution shall ensure the freezing of incoming funds in an account other than the customer's account (for example, in a special account).

368. The conduct of the Institution in executing a casual transaction when[5]:

368.1. the person who wishes to carry out the transaction is a subject of sanctions – the Institution shall refuse to execute the transaction and freeze the funds involved in the transaction in a special account;

368.2. the person who initiated the outgoing transaction is not a subject of sanctions and the beneficiary is a person who is a subject of sanctions – the Institution shall not execute the transaction, returning the funds to the initiator of the transaction.

---

[46]Ministry of Foreign Affairs of the Republic of Latvia, control of goods of strategic importance, website: https://www.mfa.gov.lv/tautiesiem-arzemes/aktualitates-tautiesiem/20440-strategiskas-nozimes-precu-kontrole?lang=lv-LV.

369. The EU Sanctions Regulations provide in certain cases for the possibility, with the authorisation of the competent institution (in Latvia it is the Commission), to allow the release of certain frozen funds or economic resources or to make them available under conditions that the competent institution deems appropriate, if the competent institution finds that the relevant funds or economic resources comply with the provisions of that Regulation. That authorisation shall be given to the institution which frozen the funds.

6.6.2. Violation of financial sanctions, circumvention, reporting obligation

370. According to the Sanctions Law, the institution is obliged to immediately, but not later than the next working day, notify the State Security Service of the violation or attempted violation of international or national sanctions and the resulting frozen funds and inform the relevant competent institution thereof.

371. If there is a suspicion of circumvention of international and national sanctions or an attempt to circumvent the financial restrictions, the institution is obliged to report it to the Financial Intelligence Unit in accordance with the procedures prescribed by law.

NB! *Paragraph 14 of the Commission's Sanctions Regulation sets out the institution's reporting obligations to the Commission.*

372. Although the applicable laws, regulations of the Cabinet of Ministers and regulations of the Commission are binding on the territory of Latvia, for the purpose of managing the risk of sanctions, credit institutions would be required, in accordance with the procedures referred to in the Sanctions Law and the Sanctions Regulations, in addition to the obligation to report to the supervisory institution of the relevant home country, to also report on the circumvention of the sanctions established in the foreign branch or foreign subsidiary of the credit institution or the attempt to circumvent the financial restrictions, if a link with Latvia is established for the sanction event.

NB! *Circumvention of OFAC sanctions* ***should only be reported to the Financial Intelligence Unit if the sanction event is linked to the financing of terrorism or proliferation***.

6.7 Exceptions to sanctions

373. With regard to compliance with sanctions by a Member State of the EU of the North Atlantic Treaty Organization, the Sanctions Rules set out the cases in which the Commission may authorise individual payments to meet the basic needs of those subject to sanctions.

374. In order to obtain a separate authorisation, the Commission shall, after examining the application of the institution and the assessment performed by the institution, issue an authorisation to perform a certain transaction or certain types of transactions to the institution and not to the customer itself.

375. The Commission may, in accordance with the requirements of the Sanctions Regulations, provide general consent to Latvian financial market participants, allowing financial and capital market participants referred to in paragraph 1 of the Sanctions Regulation who have received a relevant application for a financial transaction, to provide financial services without the separate authorisation of the Commission and to carry out financial transactions for persons subject to financial restrictions under the sanctions regime of a Member State of the EU or the North Atlantic Treaty Organization necessary for the basic needs of such natural persons and their dependent family members or for the basic economic activity of legal persons. In this case, the general harmonisation applies to both the making and the receipt of payments. The general harmonisation applies to payments claimed by certain subjects of sanctions.

Example
The institution, carrying out enhanced customer SIA B due diligence, finds that the customer is 50% owned by the subject of OFAC sanctions and applies to the Commission for authorisation to provide financial services to SIA B. The Commission, having assessed the information submitted by the institution, in accordance with the requirements of the Sanctions Regulations, issues an authorisation to the institution to provide financial services to SIA B. A few months later, as a result of the enhanced customer's due diligence, the institution finds that the ownership structure of SIA B has changed and that its owner is no longer considered a subject of OFAC sanctions. The institution informs the Commission that it will continue to provide financial services to SIA B without applying the authorisation granted by the Commission.

6.8. Sanctions risk management internal control system

376. When determining the material effect of financial restriction specified in sanctions imposed by a Member State of the EU or the North Atlantic Treaty Organization on the institution or on the financial and capital market interests, the institution shall assess and take into account at least the following circumstances:

376.1. the currencies in which the institution provides services and products;

376.2. the institution's contractual obligations with other financial institutions or correspondent banks;

376.3. the institution's activities and service provision region, including the country in which the institution’s structural unit operates and provides services – a subsidiary, a branch, a representation;

376.4. countries of operation of the institution's customers.

377. If, in the light of the risk assessment of the sanctions, the institution finds that sanctions imposed by an EU or North Atlantic Treaty Organization have a material effect on the institution or the financial and capital market interests, the institution shall ensure appropriate risk management of sanctions imposed by that EU or North Atlantic Treaty Organization Member State.

378. An institution shall use a risk-based approach to the provision of financial services, taking into account the level of risk specified in the institution's internal regulations that the institution is

prepared to assume in order to determine the range of persons with whom it is prepared to enter into a business relationship and who may be related to the subjects of sanctions.

Example

One institution, when conducting an enhanced due diligence of the subject of sanctions relative's (wife's), may find that the relative may be using financial services for the benefit of the subject of sanctions, exposing the institution to the risk of violating the sanction, and it is necessary to decide to terminate the relationship with the customer. On the other hand, another institution, finding that a relative may be using financial services in the interests of the subject of sanctions, may decide to continue cooperating with the customer by applying enhanced due diligence to the customer's transactions.

379. In order to avoid possible circumvention, an institution shall ensure that a customer of another institution who receives or sends payments to a customer of the institution as a result of the provision of financial services is not directly subject to sanctions or is not under the control of such a person.

Example

Situation No. 1
The institution’s customer A, a natural person, is included on the EU sanctions lists. EU sanctions impose financial restrictions on person A.

Example of insufficient control: the institution only checks customers for sanction lists at the time of the establishment of the business relationship and does not repeat the checks.

Example of good practice: The institution checks all customers regularly (at least once a day) for sanction lists. The institution's due diligence has established that customer A has a match with the EU subject of sanctions, checks and, if 100% matched, freezes the funds in customer A's accounts and prepares and sends a report to the Commission and the State Security Service. Subsequent payments shall be made by the institution if they comply with the exceptions provided for in the sanctions.

Example of excessive control: when an institution finds that customer A has a match with an EU subject of sanctions, it freezes the funds in customer A's accounts and prepares and sends a report to the Commission and the State Security Service. The institution shall immediately terminate the business relationship with customer A itself and with all customers who have had a business relationship with customer A.

Situation No. 2
The institution's customer A, a legal person, changes owners and the new owner is a company incorporated in Belarus that is wholly owned by natural person B, which is subject to EU sanctions and is subject to a freezing of funds. At the same time, the authorised persons and the board of customer A do not change.

Example of good practice: The institution has a control mechanism that informs the institution about changes in the ownership structure of customer A. The institution shall inspect the new owners and the new BO. Upon finding that customer A's BO is subject to an EU sanction, the institution shall freeze the funds in customer A's accounts and prepare and send a report to the Commission and the State Security Service.

Example of excessive control: The institution has a control mechanism that informs the institution about changes in the ownership structure of customer A. The institution shall inspect the new owners and the new BO. Upon finding that customer A's BO is subject to an EU sanction, the institution shall freeze the funds in customer A's accounts and prepare and send a report to the Commission and the State Security Service. Without conducting a risk assessment, the institution shall immediately cease to provide services to all of customer A's business partners.

Situation No. 3
As a result of daily screening of customers and persons of the institution, it has been established that the customer is included on the list of sanctions in Russia and the customer's economic activity is related to Russia, incl. its employees are Russian citizens who are paid monthly by the customer.

Example of insufficient control: the institution does not carry out an assessment.

Example of good practice: The institution evaluates the information obtained about the customer and conducts an examination of the limits of sanctions. The institution notes that the restrictions only apply to the assets of the subject of sanctions in Russia, so no restrictions are imposed on the customer's activities in the account. The institution shall take into account the information obtained and the customer's MLTPF risk.

Example of excessive control: An institution makes an assessment and decides to terminate a business relationship with a customer.

6.9. Financial Intelligence Unit

380. The Financial Intelligence Unit is an independent leading institution under the supervision of the Cabinet of Ministers in the prevention of money laundering, the purpose of which is to prevent the possibility of using the financial system of the Republic of Latvia for MLTPF.

381. According to Section 4.1 of the Sanctions Law,[47] the FIU is the competent institution in the fight against the circumvention of international and national sanctions or attempts to circumvent financial restrictions in accordance with the procedures prescribed by law.

382. FIU website[48] information on the subjects of national and international sanctions is maintained – natural or legal persons or other identifiable subjects. A consolidated list of sanctions is published on the FIU website[49]. This includes financial restrictions imposed by both the EU and

[47] Law On International Sanctions and National Sanctions of the Republic of Latvia, available at: https://likumi.lv/ta/id/280278-starptautisko-un-latvijas-republikas-nacionalo-sankciju-likums.
[48] Financial Intelligence Unit website – Sanctions lists (fid.gov.lv).
[49] Financial Intelligence Unit website – Sanctions lists (fid.gov.lv).

the UN, which are binding throughout EU jurisdiction. The consolidated list is designed as an advisory and search tool. The consolidated list does not include information on sectoral sanctions, which can be found on the Sanctions Map on EU sectoral sanctions.

6.10. Terrorism financing

6.10.1. The concept of terrorism financing and its limitation

383. **Terrorism financing** is the direct or indirect collection or transfer of funds or other property, in any form, for the purpose of using it or knowing that it will be used, in whole or in part, to carry out one or more of the following activities[50]:

383.1. terrorism;

383.2. The activities referred to in Section 1 of the Convention for the Suppression of Unlawful Seizure of Aircraft;

383.3. 10.03.1988. The activities referred to in Section 3 of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation;

383.4. Activities referred to in Section 1 of the International Convention against the Taking of Hostages;

383.5. Activities referred to in Section 2 of the International Convention for the Suppression of Terrorist Bombings;

383.6. Activities referred to in Section 7 of the Convention on the Physical Protection of Nuclear Material;

383.7. The activities referred to in Section 1 of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation;

383.8. Activities referred to in Section 2 of the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation;

383.9. Activities referred to in Section 2 of the Convention on the prevention and punishment of criminal offences against internationally protected persons;

383.10. 10.03.1988. The activities referred to in Section 2 of the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf;

383.11. travel for terrorism purposes;

383.12. involvement in, organisation or conduct of a terrorist group;

383.13. recruitment, training or education for terrorism;

383.14. justification of terrorism, incitement to terrorism or threat of terrorism;

383.15. 13.04.2005. Activities referred to in Section 2 of the International Convention for the Suppression of Acts of Nuclear Terrorism.

! *Terrorism financing also includes the direct or indirect collection or transfer of funds or property in any form to a terrorist group or to an individual terrorist.*

384. The risk management tool for terrorism financing is the imposition of sanctions. Sanctions have been imposed by the EU and the UN to curb terrorism financing. The EU's financial constraints on terrorism financing are set out in two programmes: restrictive measures related to

[50]Law On the Prevention of Money Laundering and Terrorism and Proliferation Financing, available at: https://likumi.lv/ta/id/178987-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-un-proliferacijas-finansesanas-noversanas-likums.

ISIL (Daesh) and ***Al-Qaeda (programme name* – EUAQ)** and specific counter-terrorism measures (**programme name –TERR**).

! *Information on these programmes and the people involved is available on the* ***EU Sanctions Guidelines website***[51]*, and information on the persons included in the programmes can be found in the* ***FIU consolidated sanctions database,***[52] *by entering* ***EUAQ*** *and* ***TERR*** *respectively next to the name of the programme.*

385. UN restrictions on terrorist financing have been imposed on ***individuals associated*** with ***AL-Qaeda, ISIL*** and the ***Taliban***.

! *Information is available on the UN website*[53].

! *Information on* ***UN subjects of sanctions*** *is available on the FIU consolidated sanctions list*[54] *and the EU Sanctions Map, entering the* ***Taliban*** *and* ***AL-Qaeda*** *respectively next to the programme name.*

386. The sanctions regime developed by OFAC imposes restrictions on the financing of terrorism and international terrorist organisations, such as the *Global Terrorism Sanctions Regulations* (SDGT), *Foreign Terrorist Organizations Sanctions Regulations* (FTO), *Hizballah International Financing Prevention Amendments Act of 2018, Public Law No.: 115-272* (HIFPAA).

! *Information on the persons included in the specified programmes is available on the FIU consolidated sanctions list* [55]*by* ***entering SDGT, FTO*** *or* ***HIFPAA*** *next to the programme name.*

! *Information on* ***OFAC programmes*** *is available on the OFAC website*[56].

6.10.2. Terrorism financing methods and risk management

387. Terrorists or subjects of terrorist threats are divided into several categories, taking into account:
387.1. the level of coordination of their activities;
387.2. their location;
387.3. their origin and a number of other factors.

388. Terrorist organisations carry out:
388.1. training of combatants;
388.2. attack planning;

---

[51] EU Sanctions Card – https://www.sanctionsmap.eu/#/main.
[52] Financial Intelligence Unit – https://sankcijas.fid.gov.lv/.
[53] List of UNSC sanctions – https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.
[54] Financial Intelligence Unit – https://sankcijas.fid.gov.lv/.
[55] https://sankcijas.fid.gov.lv/.
[56] OFAC Sanctions Programme and Information – https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

388.3. production of propaganda materials;
388.4. weapons preparation.

389. In order to achieve their goals, terrorist organisations need to receive financial support. An effective terrorist group, like any other criminal organisation, needs to establish and maintain its own financial infrastructure. To this end, it is necessary to establish the sources of financing, the means and methods of laundering the obtained funds, as well as the ways and means by which the materials and other aids necessary for the organisation and conduct of terrorism acts will be obtained from these funds.

390. Terrorism financing is not a direct involvement in terrorism activities, but is one of the activities in support of terrorism, and the term encompasses a variety of activities aimed at obtaining and targeting money, other financial instruments or property in support of terrorism. The activity itself involves not only the acquisition of funds or property, but also its diversion (e.g., transfer), physical delivery to, for example, terrorist organisations.[57]

391. Different people with different motivations are involved in terrorism financing activities. The most frequently identified subjects of terrorism financing are:
391.1. radicalised people who want to support terrorism;
391.2. representatives of terrorist organisations who have a task to obtain funding;
391.3. money laundering intermediaries profiting from terrorism financing transactions;
391.4. relatives and friends of persons involved in terrorism activities who support their activities or wish to provide financial support to a particular person (often money is received from terrorist relatives);
391.5. persons and organisations who agree to pay a ransom for, for example, a captured person or group of persons.

392. Terrorism financing is characterised by transactions of any size, from very small payments. Institutions that provide international money remittance services or offer customers the opportunity to make cross-border payments may be at increased risk of terrorism financing. Therefore, an institution's ICS should include adequate management of the risks inherent to the service and its geography.

393. Terrorism financing also uses anonymous prepaid cards to pay for the purchase of goods used in terrorism activities on the internet. It is therefore essential to pay attention to ensuring that transactions or business relationships are properly monitored in order to detect suspicious transactions and that a limited number of anonymous payment instruments can be used by one person.

NB! *In assessing the risk of terrorism financing, institutions should take into account the risks identified in the national and European Commission transnational risk assessments.*
Attention needs to be paid to various charitable organisations and campaigns for obtaining resources, as these funds can be used to finance terrorism.

[57] Financial Intelligence Unit "Strategy for the Prevention of the Financing of Terrorism 2019-2021": https://www.fid.gov.lv/lv/darbibas-jomas/vadlinijas-tipologijas-riki.

394. FATF[58] points to the possible use of non-governmental organisations to fund terrorist organisations or activities[59], with a particular emphasis on public benefit organisations, religious organisations, charitable organisations and social assistance organisations.

395. The FATF points to a number of possible factors that need to be addressed when working with non-governmental organisations:

395.1. the organisation has a large flow of funds (including cash flow);

395.2. the organisation has a comprehensive and unspecified scope;

395.3. there are tax payment exemptions;

395.4. the organisation's income consists mainly of donations and gifts;

395.5. the organisation's activities relate to countries in military conflict or to their neighbouring countries.

396. The institution shall pay attention to the purpose and nature of the activities of non-governmental organisations and shall assess the risk of terrorism financing and, based on the risk assessment, take appropriate risk mitigation measures. In assessing the risk of sanctions, the institution shall also take into account national sanctions imposed by the countries and territories in which it operates or in which its customers or partners operate, in so far as this may affect the functioning of the institution.

NB! *The Sanctions Law also provides the Cabinet of Ministers with the right to impose national sanctions, including for the purpose of combatting international terrorism.*

! *Additional information on the sources and types of financing of terrorism is available in the guidelines developed by the FIU, which are available at https://www.fid.gov.lv/uploads/files/Dokumenti/Vadl%C4%ABnijas%2C%20rekomend%C4%81cijas/TF_un_PF_nov_vadlinijas.pdf.*

Example

Situation No. 1

The customer natural person (pensioner of the Republic of Latvia) rents an individual safe deposit box at the institution. After preparing the safe deposit box, it never visits it, but registers as an additional user, a young person from the country with a high or increased risk of terrorism crimes who periodically starts visiting the safe deposit box with heavy bags. During the identification procedure, the additional user shall present a residence permit of the Republic of Latvia with a minimum term (one year).

Example of insufficient control: the institution does not pay attention to the specified circumstances and does not initiate a due diligence.

[58] FATF – https://www.fatf-gafi.org/about/.

[59] FATF "*Risk of terrorist abuse in non-profit organisations*": https://www.fatf-gafi.org/documents/documents/risk-terrorist-abuse-non-profits.html.

Good practice example: An institution requires a customer who has drawn up a contract to use a safe deposit box to provide documentary evidence on its connection to an additional user and to provide additional information about his or her employment. In the case of suspicion, the institution shall request confirmation of the existence of employment and perform an additional analysis of the user's potential income level and living conditions and compare it with the information provided by the main user of the safe deposit box. If necessary, report to the Financial Intelligence Unit or the State Revenue Service about concerns that the contents of the safe-deposit box may be related to any illegal activities.

Example of excessive control: the institution prohibits the use of a safe-deposit box by an additional user without further investigation.

Situation No. 2

The customer makes several significant payments (10,000 euros) for jewellery to a seller who is located in a country with a high or increasing risk of terrorism crimes or on the border of such a country and about which information is not publicly available. Proof of transaction does not provide assurance on the actual delivery of the goods. The customer does not trade in jewellery and explains that it has purchased the product for personal use.

Example of insufficient control: the institution only requires documents for the purchase of the goods.

Example of good practice: the institution asks the customer for explanations on the need for this type of operation, transport documents and evaluates the goods if necessary.

Example of excessive control: an institution terminates cooperation with a customer without conducting enhanced due diligence.

Situation No. 3

The customer (company) has declared a trade activity – receipt of funds for the product, but does not make outgoing payments for the product. The funds received are transferred to companies for which information is not publicly available, or to natural or legal persons from tax-free jurisdictions or regions with a high or increasing risk of terrorism financing or the borders of such regions.

Example of insufficient control: the institution only requests documents for key partners.

Good practice example: The institution asks for supporting documents for each payment, together with documentary evidence of the transport of the goods, and evaluates the information obtained to ensure that the transactions are free from terrorism financing.

Example of excessive control: an institution terminates cooperation with a customer without conducting enhanced due diligence.

Situation No. 4

The customer – a payment card user, resident in the Republic of Latvia, regularly makes payments for airline tickets using a payment card. Other card transactions were performed in Latvia. In addition, small payments (up to € 1,000) have been identified for individuals from regions with a high or increasing risk of terrorism financing or the borders of such regions.

Example of insufficient control: the institution does not pay attention to the specified circumstances and does not initiate a due diligence.

Good practice example: An institution asks a customer to provide an explanation for the need to make such frequent payments for airline tickets as well as for payments to individuals in increasing risk jurisdictions.

Example of excessive control: the institution does not conduct an enhanced due diligence and terminates the cooperation with the customer.

Situation No. 5
The customer has been identified as outgoing payments to companies in countries with a high or increasing risk of terrorism financing or within the borders of such countries, which, according to public information, may offer the services of an unlicensed payment institution (so-called hawala). Payments to such regions are not typical for the customer, taking into account its economic activity.

Example of insufficient control: the institution does not pay attention to the specified circumstances and does not initiate a due diligence.

Good practice example: An institution applies enhanced transaction monitoring to a customer and requests information on business partners.

Example of excessive control: an institution terminates cooperation with a customer without conducting enhanced due diligence.

6.11 Proliferation financing

6.11.1. The concept of proliferation and its financing methods

397. According to the FATF definition[60] Proliferation is the illicit transfer and export of nuclear, chemical, bacteriological, biological, toxic or other weapons of mass destruction (WMD), the transfer and export of their means of delivery and related materials (for example, technology, goods, software, services or expertise).

398. Proliferation financing is the collection or transfer of funds or other property for the illicit manufacture, acquisition, storage, development, export, transhipment, brokering, transportation, transfer or use of WMD and its supplies, as well as related materials.

[60] FATF Report on Combatting Proliferation Financing, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

399. Proliferation financing differs from terrorism financing mainly in that the main sources of the financing system are used:

399.1. banks and payment institutions, not cash;

399.2. cryptocurrencies;

399.3. *hawala.*

400. This makes it significantly more difficult to detect proliferation, as most transactions are similar to other legal transactions in order not to differ from the overall picture. Virtually all proliferous use complex financial schemes and many front companies to operate in jurisdictions where financial institutions have little understanding of customer research and risk.

401. There are three stages in the financing of proliferation:

401.1. the state or organisation initially raises funds, sometimes illegally;

401.2. the obtained funds are injected into the international financial system (by performing currency exchange, various operations of financial instruments or financing legal business). This is not a problem for non-sanctioned countries, but countries with different restrictions tend to take various measures to circumvent sanctions at this stage;

401.3. The funds in circulation are used to finance proliferation by purchasing various materials and technologies and paying for transportation services.

402. Companies established in EU Member States are often used as intermediaries for proliferation, as well as re-exports of consignments, which makes it significantly more difficult to detect proliferation. Intermediary transaction with goods of strategic significance is common, involving the international illicit movement of such goods, including to countries at risk of terrorism and conflict zones:

402.1. weapons;

402.2. ammunition;

402.3. civil and military aviation equipment;

402.4. maritime transport;

402.5. other techniques.

403. The main risk factor for proliferation is countries that have developed or are developing illicit biological, chemical or nuclear weapons systems. Among the countries directly identified as being at high risk of proliferation financing are the Democratic People's Republic of Korea and Iran.

404. Subject to the restrictions and enhanced supervision measures, no direct payments will be made to the Democratic People's Republic of Korea or Iran, using their border states or countries where MLTPF regimes are incomplete and ineffective for their intermediary transactions.

405. Proliferation financing uses sources of the financing system from legal transactions and is not usually implemented by natural or legal persons on the sanctions lists, but most often front companies and shell companies are used in transactions to obtain funds for proliferation. Proliferation financing could be implemented by a person or entity not on the sanctions list, executing a transaction for the benefit of another person subject to financial restrictions.

Insufficient customer due diligence and transaction supervision create the possibility that proliferation financing can be hidden through complex transactions and ownership structures.

406. Shipping and maritime transport has been used for the proliferation financing purposes, to supply various goods from Asian countries with a high risk of sanctions to customers abroad. In this way, coal, sand, seafood, rare earth minerals and other natural resources available in these countries are transported, and the proceeds of trade are diverted to nuclear and missile programmes.

6.11.2. Proliferation financing risk management

407. The institution should pay increased attention to transactions with countries which are not members of the EU and North Atlantic Treaty Organization and whose industry and economy are closely linked to the military sector, and that cooperate with other sanctioned countries, which poses an additional risk of being indirectly involved in the circumvention of sanctions. This circumstance does not in itself pose a direct risk of sanctions, however, it must be assessed together with other factors that increase the risk of sanctions. The institution shall take into account the link with such a country when assessing the overall economic activity of the customer and the risk of sanctions inherent to it.

408. Restrictive measures to prevent proliferation financing have been imposed by the EU, the UN and OFAC. The Sanctions Law also provides for the right of the Cabinet of Ministers to impose national sanctions for the purpose of combatting the manufacture, possession, transfer, use or distribution of weapons of mass destruction. At present, the national sanctions imposed by the Cabinet of Ministers are in force, which have been applied to natural and legal persons in accordance with Cabinet of Ministers Regulation No. 419 of 25.07.2017 "Regulations Regarding the Imposition of National Sanctions in Relation to Subjects Connected with the Nuclear Programme and Political Regime Implemented by the Democratic People's Republic of Korea"[61].

409. To prevent involvement in the financing of proliferation, an institution should take the following steps when initiating and maintaining business relationships with customers:

409.1. identify customers operating in the field of military or dual-use goods;

409.2. enhanced due diligence should be performed in order to find out the customer's business partners, regions of operation, end recipients of the product or service, incl. to make sure that the customer has received all the necessary licences (authorisations) for the performance of commercial activities, as well as for the import and export of goods outside the borders of the Republic of Latvia;

409.3. if necessary, apply to the Export Control Division of Strategic Goods of the Ministry of Foreign Affairs for an opinion on whether the goods involved in the transaction are subject to special export control and whether the customer has received the necessary authorisation.

Example

[61]Cabinet Regulation No. 419 of 25.07.2017 "Regulations on the imposition of national sanctions of the Republic of Latvia in respect of subjects related to the nuclear programme and the political regime of the People's Democratic Republic of Korea", available at: https://likumi.lv/ta/id/292535-noteikumi-par-nacionalo-sankciju-noteiksanu-attieciba-uz-subjektiem-kas-saistiti-ar-korejas-tautas-demokratiskas-republikas.

Customer A sells dual-use items to partner B, which, according to public information, engages in non-dual-use activities or has the status of a charity, and partner B is located in a country or region adjacent to a sanctioned country.

Example of insufficient control: When monitoring customer A's payments, no enhanced due diligence is provided for each payment.

Good practice example: In the analysis of each payment of customer A, the request for transaction documents and the collection of public information about the business partner are provided in order to know the final ownership and use of the subject of the transaction or the need according to the buyer's needs. The institution shall contact the Ministry of Foreign Affairs to ascertain the necessary permits for the trade and export of goods.

Example of excessive control: If partner B is duly licensed or authorised by the regulatory institution of its country to purchase the specified goods and the partner is from a European Economic Area country, it would be excessive to perform the in-depth collection of public information.

410. A description of the proliferation typologies and sectors most at risk of proliferation financing is provided in the UN Panel Report[62].

Additional information on the risks of financing terrorism and proliferation and their prevention is available in the FIU material available at https://www.fid.gov.lv/images/Downloads/materials/proliferation/TF_un_PF_nov_vadlinijas.pdf.

6.12. Publicly available sources that can be used to manage the risk of sanctions (the list is illustrative and non-exhaustive)

General information on sanctions on the website of the Ministry of Foreign Affairs	https://www.mfa.gov.lv/lv/sankcijas
European Commission clarification on sanctions	https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf
Sanctions database (information on sectoral sanctions not included)	Consolidated database published on the website of the Financial Intelligence Unit (https://sankcijas.fid.gov.lv/)
Information on the control of goods of strategic importance on the website of the Ministry of Foreign Affairs	https://www.mfa.gov.lv/lv/strategiskas-nozimes-precu-kontrole

[62] UN SC report "Report of the Panel of Experts established to resolution 1874 (2009)", available at: https://undocs.org/S/2020/151.

Topicalities of OFAC sanctions	https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions
List of Section 231 (e) of the CAATSA	https://www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation/
US Department of State clarification on sanctions in the energy sector	https://www.state.gov/key-topics-bureau-of-energy-resources/
Information on persons subject to OFAC sectoral sanctions	https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/sectoral-sanctions-identifications-ssi-list
Sanctions in force in the United Kingdom on the UK Financial Sanctions Office website	https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation
Sanctions in force in Canada on the Office of the Superintendent of Financial Institutions website	https://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/Pages/default.aspx
UN restrictions on terrorism financing on the UN website	https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list un https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban.xsl
Report of the UN Panel of Experts on Proliferation Typologies and Sectors Most at Risk of Proliferation Financing	https://undocs.org/S/2020/151
Information on the risks of financing terrorism and proliferation and their prevention on the FIU website	https://www.fid.gov.lv/images/Downloads/materials/proliferation/TF_un_PF_nov_vadlinijas.pdf
National MLTPF risk assessments published on the FIU website	https://fid.gov.lv/lv/darbibas-jomas/nacionalais-risku-novertejums

7. Processing of data of natural persons in the field of AML/CTPF and sanctions compliance[63]

7.1. Basic principles and legal basis for processing data of natural persons in the context of the Law, Sanctions Law and other related laws and Data Regulation[64]

411. In accordance with Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, protection of natural persons with regard to the processing of personal data is a fundamental right.

412. Data Regulation is an EU regulatory act on the processing and protection of data of natural persons, and its Article 6(1) defines the following general legal bases for the processing of data of natural persons: consent, conclusion and performance of a contract, legal obligation, public interest, protection of vital interests, observance of legitimate interests. These legal bases also apply to the collection and processing of data necessary for the purposes of AML/CTPF and sanctions compliance.

413. According to Section 2 of the Law, the purpose of the Law is to prevent money laundering and terrorism and proliferation financing, while according to paragraph one of Section 2 of the Sanctions Law, the purpose of this Law is to ensure peace, security and rule of law in accordance with the international obligations and national interests of Latvia, when introducing international sanctions.

414. The Data Regulation defines the following data processing basic principles which must be followed when processing data of natural persons: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability.

415. A risk-based approach and the principle of proportionality must be followed when processing data of natural persons for the purposes specified in the Law.

416. In its operation, the institution must achieve a balance between the necessary measures to implement the general interests of the customer and the goals of AML/CTPF, as well as respect for privacy and other fundamental rights of the individual. Compliance with AML/CTPF requirements must be ensured while complying with the provisions of the Data Regulation and other data protection requirements in general.

417. In the context of compliance with the Law, the Sanctions Law and other related laws of the Republic of Latvia and the EU, processing of personal data of customers (including potential customers) who are the subjects of these laws is only lawful if one of the following legal bases is applicable and to the extent permitted by these bases:

417.1. **legal obligation** – Article 6(1)(c) of the Data Regulation, which allows the processing of personal data "for compliance with a legal obligation to which the controller is subject" to ensure compliance with the requirements of the Law, the Sanctions Law and other related laws of the Republic of Latvia and the EU. This is the primary legal basis for data processing resulting from the Law, the Sanctions Law and other related laws of the Republic of Latvia and the EU, as it obliges the subjects of these laws to perform certain data processing, for example, to conduct customer due diligence or enhanced due diligence in accordance with the Law, and in the performance of such an obligation, the controller is not given discretion.
Thus, Article 6(1)(c) of the Data Regulation does not apply to voluntary unilateral relationships and public-private partnerships where data is processed beyond what is required by the law.
In addition, the legal obligations themselves must be sufficiently clear about the processing of personal data they require. Therefore, Article 6(1)(c) of the Data Regulation is applicable on the basis of legal norms, which clearly state the type and object of processing, and the controller is not granted disproportionate discretion regarding compliance with its legal obligations.

Laws may sometimes only set a general objective, but more specific obligations are defined at another level, for example, either in secondary law or by a binding decision of a public authority in a specific case. This may also create legal obligations in accordance with Article 6(1)(c) of the Data Regulation, if the type and object of processing are properly defined and have an appropriate legal basis[65];

417.2. **public interest** – Article 6(1)(e) of the Data Regulation, which allows the processing of personal data "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" in accordance with the laws of the Republic of Latvia or the EU.
For the application of this legal basis, as well as for the application of Article 6(1)(c) of the Data Regulation, the processing basis is determined by: (a) EU laws; (b) laws of the Member State applicable to the controller.
For the application of Article 6(1)(e) of the Data Regulation, the law may contain specific provisions to adjust the application of the provisions of the Data Regulation, including: general conditions governing the lawfulness of the processing carried out by the controller; types of data to be processed; relevant data subjects; entities to which personal data may be disclosed and the purposes for which they may be disclosed; processing purpose limitations; storage periods; processing activities and processing procedures, including measures to ensure lawful and fair processing, for example in other specific data processing situations provided for in Chapter IX of the Data Regulation. The laws of the EU or a Member State correspond to the objective of the public interest and are proportionate to the stated legitimate objective.
Recital 45 of the Data Regulation also explains that where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. The Data Regulation does not require a specific law for each individual case of processing. It may be sufficient to have a law on which several data processing activities are based, based on a legal obligation that the controller is required to fulfil, or where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
Thus, Article 6(1)(e) of the Data Regulation has similarities with Article 6(1)(c), since the task carried out in the public interest is often based on or derived from legal provisions. However, the scope of application of Article 6(1)(c) of the Data Regulation is strictly limited compared to Article 6(1)(e) of the Data Regulation. Therefore, the main difference when applying these legal bases is that the controller does not have discretion in the application of Article 6(1)(c) of the Data Regulation, as the processing of personal data will be determined by law.
Therefore, it can be concluded that this legal basis is applicable to data processing in order to achieve the objectives of the Law, as defined in Section 5^2, paragraph one of the Law.
This legal basis is also appropriate for the application of the Sanctions Law in the context of personal data processing, because the subject of this Law performs the task or delegation specified in this Law. Therefore, it can be considered that the processing of personal data is necessary for the protection of public interests.
Taking the above into account, in practice, situations should be distinguished when data processing is carried out on the basis of Article 6(1)(c) and (e) of the Data Regulation. Paragraph 1(e) of this article is applicable in cases where the law does not determine either the scope or type of data processing and does not impose a specific legal obligation. For example,

this legal basis applies to data processing carried out in accordance with Section 44 of the Law, which determines the right of credit institutions and financial institutions to mutually exchange information (see Sub-chapter 5.7 of the Handbook). This basis can also be applied in a situation where a credit institution evaluates the data of its customers using a credit reference database or a database for the prevention of money laundering and terrorist financing or fraud. On the other hand, in situations where the controller does not have discretion, because a legal obligation must be fulfilled, data processing must be carried out on the basis of paragraph (c);

417.3. **legitimate interests** – Article 6(1)(f) of the Data Regulation, which allows the processing of personal data "for the purposes of the legitimate interests pursued by the controller or by a third party", justifying each case separately. This legal basis can be relied upon, for example, to: establish, exercise or defend legal claims; store data in addition to the term specified in Paragraph two of Section 37 of the Law (see Paragraph 461 of the Handbook); exchange data for the purposes of compliance with sanctions.
In order to process personal data on this legal basis, the controller needs to assess whether and which specific legitimate interests of the controller or a third party in the specific case of data processing will be valued higher than the fundamental rights, fundamental freedoms and interests of the data subject. When balancing interests, controllers are invited to use Article 29 of Data Protection Working Party's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC[66]. Information on the right of data subjects to object to data processing based on this legal basis is provided in Sub-chapter 7.5 of this Handbook.
The assessment of the balancing of interests must be carried out in each individual case, taking into account the balancing of the interests of the data subject and the controller.
In order to ensure the observance of the principle of accountability, it would be advisable to document the assessment. At the same time, if the controller has developed internal regulatory acts or guidelines at its disposal which describe the necessity and procedure for personal data processing, an individual assessment is not necessary.
The balancing of interests must be carried out by initially defining the purpose for which data processing is necessary (the purpose must be lawful, clear and real), an assessment must be made as to why personal data processing is necessary to achieve the specified purpose (for example, why it is not possible to achieve this purpose using means which are less intrusive on personal privacy), an initial balance assessment must be carried out (the type of interests of the processor (commercial interests, public interests, fundamental rights, etc.)), as well as the potential harm if processing is not carried out, the status of the data subject (for example, minor, pensioner, employee), the type of data processing, the rights of the data subject must be assessed, the extent of the infringement of the rights of the data subject, the justified expectations of the data subject, the balance of the impact with the benefit, the additional security measures applied (data minimisation, implemented technical and organisational measures, etc.), ensuring transparency, ensuring other rights of the data subject (including whether and how the data subject can object to the processing of his/her personal data in accordance with Article 21 of the Data Regulation) must be assessed. If the balancing assessment has not been carried out, or if the above-mentioned aspects have not been taken into account when carrying out the assessment, the processing of personal data will not comply with the requirements of the Data Regulation.

In addition, according to Article 21(1) of the Data Regulation, the controller should provide the data subject with the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her. The controller should ensure that, in the case of objection, the personal data is no longer processed unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Information on the right of data subjects to object to data processing based on this legal basis is provided in Sub-chapter 7.5 of the Handbook;

417.4. **consent** – Article 6(1)(a) of the Data Regulation. For example, the customer gives consent to receive various bank news. It is the duty of the data controller to ensure that the customer gives consent in accordance with the requirements of the Data Regulation and that all necessary information is available to him/her before giving the consent.
The customer's consent is not required for updating (rectifying) the customer's personal data, if the credit institution obtains data from official registers that have public credibility, for example, from the Population Register. If possible, the credit institution may ask the customer whether the information it has is accurate. According to Article 5(1)(d) of the Data Regulation, personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay, taking into account Article 19 of the Data Regulation, which requires the controller to communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

7.2. Processing of special categories of personal data

418. In accordance with Article 9(1) of the Data Regulation, processing of special categories of personal data, namely, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, shall be prohibited. However, this paragraph does not apply if one of the exceptions specified in Article 9(2), or Article 9(4) of the Data Regulation is applicable, if a certain EU Member State has provided for a different procedure regarding the processing of health, genetic or biometric data. These exceptions apply in addition to the legal basis to be determined according to Article 6(1) of the Data Regulation (see Sub-chapter 7.1 of the Handbook). For example, if the processing of ordinary personal data takes place in the public interest (Article 6(1)(e) of the Data Regulation), the processing of special categories of personal data can take place on the basis of the additional condition referred to in Article 9(2)(g) of the Data Regulation if such data processing arises from the laws of the EU or its Member State. It is considered that the public interests contained in the Law and the Sanctions Law are essential.

419. Before data processing, the controller must check whether special categories of personal data are processed in the given case. In practice, the processing of such data may also not take place if there is no direct intention to obtain and process such data. For example, when checking the origin of funds, the controller obtains information that the funds are transferred from a

country where one religious belief prevails. Consequently, a wrong impression may arise that data about the religious belief of a natural person are being processed. This conclusion is drawn from information about the country, not directly from the fact that the particular person has religious belief X. Therefore, information about the country cannot automatically be considered as information about a particular person's religious beliefs.
However, when checking the status of a politically exposed person, a special category of personal data can be indirectly obtained – data about this person's political views (in connection with belonging to a certain political party) – but their processing depends on the existence of the intention and whether there is an appropriate legal basis for the processing of such data.

Processing of biometric data
420. Regarding the processing of biometric data, it should also be noted that according to Article 4(14) of the Data Regulation, "biometric data" means "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

421. The processing of biometric data as a special category of personal data is possible if at least one of the legal bases mentioned in Article 6(1) of the Data Regulation exists and, in addition, any of the conditions referred to in Article 9(2) or (4) of the Data Regulation.
As an example, Paragraph 9 of Cabinet Regulation No. 392[67] of 03.07.2018 can be mentioned, which stipulates that in the case of off-site (remote) identification, using video identification or comparing the photo of the identity document and the electronic photo of the self-portrait by technical means, the subject of the Law performs the recognition and comparison of the personal biometric data obtained from the person. Taking into account the fact that the processing is determined by the regulatory framework, the legal basis for the processing of biometric data derives from Article 6(1)(c) and Article 9(2)(g) of the Data Regulation. Sub-clause "b" of Clause 1 of Paragraph two of Section 22 of the Law provides that the subject of the Law shall apply enhanced customer due diligence, including upon establishing and maintaining a business relationship or executing an occasional transaction with a customer who has not participated in the onsite identification procedure in person, except for in the case when the following condition is fulfilled: the customer identification, by means of technological solutions including video identification or secure electronic signature, or other technological solutions, is being performed to the extent and in accordance with the procedures stipulated by the Cabinet; Paragraph three of Section 22 of the Law stipulates that in accordance with Paragraph two, Clause 1, Sub-clause "b" of this Section, the Cabinet shall determine the extent of and procedures for customer identification by means of technological solutions including video identification or secure electronic signature, or other technological solutions. Accordingly, Cabinet of Ministers Regulation No. 392 of 03.07.2018 provides for the possibility of using technological solutions such as video identification (Sub-chapter 7.2) or comparison of the photograph in a personal identity document and electronic self-portrait photograph (Sub-chapter 7.4), etc., to determine the risk of MLTPF. Clause 9 of the above Regulation provides that in the case referred to in Sub-paragraphs 7.2 and 7.4 of this Regulation, the subject of the Law, by using solutions (including technological), shall ensure the verification of such security features of an identification document that can be and are needed to be technically verified remotely, and shall also carry out the recognition and comparison of the biometric data of a person obtained from

the person during off-site (remote) identification. When applying Sub-paragraphs 7.2 and 7.4 of this Regulation, a screenshot of a personal identity document shall be regarded as being equivalent to the copy of a personal identification document within the meaning of the Law. Hence, it can be concluded that if the subject of the Law carries out off-site (remote) identification, then such an obligation arises upon it from the regulatory framework (Article 6(1)(c) of the Data Regulation).
(According to the wording of FCMC Recommendation No. 77 of 24.05.2022)

422. According to recital 51 of the Data Regulation, "the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are only covered by the definition of biometric data when processed through specific technical means allowing the unique identification or authentication of a natural person".

Example
Processing of biometric data is a case when the subject of the Law, in order to fulfil the requirements of the Law for customer identification, processes biometric data by technical means to uniquely identify the specific customer. This is most often performed by using templates created by extracting the most relevant features from biometric raw data, such as facial measurements from an image (such a template is called a "biometric matrix"). Identification in the specific case may not be the identification of a person's name, surname or personal identity number, but a unique separation of a person from other persons and the possibility of recognising the person in a repeated contact. On the other hand, if the purpose of information processing is to separate one category of data from another, but unique identification of a natural person by technical means is not carried out in this process, for example, in cases where an employee of a credit institution visually compares a sent-in photo of a customer's self-portrait with the personal image of the sent-in identity document, then it does not count as biometric data processing.

423. Filmed material in which an individual can be seen cannot be considered as biometric data in itself according to Article 9 of the Data Regulation, if it has not been specially processed technically in order to facilitate the identification of the individual. In order for it to be considered a special category of personal data processing (Article 9 of the Data Regulation), biometric data must be processed "for the purpose of uniquely identifying a natural person".

424. Guidelines 3/2019 on the processing of personal data through video devices[68] of the European Data Protection Board set out, in Paragraph 76 of Chapter 5.1 "General considerations when processing biometric data", the criteria which must be considered as regards the application of Article 4(14) and Article 9 of the Data Regulation:
424.1. Nature of data: data relating to physical, physiological or behavioural characteristics of a natural person.

Example
A person's photo is compared to a person's self-portrait photo or video image in real time – this clearly refers to the person's physical characteristics (facial points).

424.2. Means and way of processing: data "resulting from specific technical processing".

Example
When performing off-site (remote) identification, a person's photo (personal identity document image and a person's self-portrait photo or a real-time video image of a person's face) is processed by technical means to obtain information that the person depicted in the photo of the document is the same person using, for example, a mobile app.

424.3. Purpose of processing: data must be used for the purpose of uniquely identifying a natural person.

Example
There would be unique identification in the event that, after submitting photos in the mobile application, it would be possible to identify a specific natural person by technical means, that is, if this person were to be recognised as, for example, Jānis Bērziņš from the photo.

425. If it is established that biometric data will be processed using the planned, especially new, technology, then, taking into account the nature, scope, context and purposes of the processing, in accordance with Article 35(1) of the Data Regulation, the need for a data protection impact assessment must be considered, unless the exceptions mentioned in Paragraph 10 of this article apply (see Sub-chapter 7.4 of the Handbook).

426. The Law stipulates that the subject of the Law must conduct customer due diligence in the cases specified by the Law. For example, Section 11^1, Paragraph one, Clause 5 of the Law stipulates that customer due diligence measures are a set of risk assessment-based activities within the scope of which the subject of the Law "ensures the storage, regular assessment and updating of the documents, personal data and information obtained during the course of the customer due diligence according to the inherent risks, but at least once per each five years". Therefore, it can be concluded that biometric data should also be stored if they have been obtained as part of customer due diligence.
Paragraph 14 of Cabinet of Ministers Regulation No. 392 of 03.07.2018 states that "if the type of remote identification provided for in Sub-paragraph 7.4 of this Regulation may be applied in accordance with the requirements of this Regulation, the subject of the Law shall provide the recording of the image audit trail with a fixed time stamp, given name and surname, and also the IP address of the internet connection of the remotely identified natural person". Section 37, Paragraph two of the Personal Data Processing Law (hereinafter referred to as the "PDPL") states: "If an obligation is imposed on the controller to ensure the storage of audit trails of the system, they shall be stored for not longer than one year after the making of an entry, unless laws and regulations or the nature of processing stipulates otherwise." Considering the fact that data processing is determined by Law, the term of data storage should be determined in accordance with the Law.

427. Further information on the processing of biometric data is also explained in the following resources:
https://www.dvi.gov.lv/lv/dviskaidro-biometrijas-datu-apstradi-mazumtirdznieciba;
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf;
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

7.3. Processing of personal data relating to criminal convictions and offences

428. Pursuant to Article 10 of the Data Regulation, processing of personal data relating to criminal convictions and offences or related security measures shall be carried out based on any of the legal bases laid down in Article 6(1) of the Data Regulation (see Sub-chapter 7.1 of the Handbook) and only under the control of an official authority or when the processing is authorised by Union or Member State law.

"Under the control of official authority" means that processing relating to criminal convictions or offences can only be carried out by those authorities for whom this processing is justified, for example, as defined in a regulatory act, or by competent authorities, if it is carried out in the field of criminal law. Official authorities cannot make personal data publicly available without requiring the person requesting access to justify the acquisition of this data with specific interests. For example, in order to receive a statement on a person's criminal record, the person or company should apply to the Information Centre of the Ministry of the Interior as the holder of the Punishment Register and justify their request.

In accordance with Section 41, Part two, Clause 4 of the Law, in order to fulfil the obligations specified in the Law, credit institutions shall obtain data from the Punishment Register, as the above clause states that credit institutions and insurance merchants, insofar as they are carrying out life insurance or other insurance activities related to the accumulation of funds, have the right, in order to fulfil the obligations specified in this Law, to request and receive free of charge, as well as store and otherwise process information from the Punishment Register – data on the criminal record related to criminal offences in the national economy which has not been extinguished or set aside of a customer, the beneficial owners and representatives thereof, as well as of a person who has expressed a wish to establish a business relationship with the credit institution or insurance merchant, the beneficial owners and representatives of such a person, when carrying out the MLTPF risk assessment of the customer, as well as in the cases when the necessity of reporting to the Financial Intelligence Unit of Latvia on a suspicious transaction or the necessity to refrain from executing a suspicious transaction is being evaluated.

Considering the fact that the Law provides a clear basis for the processing of data on criminal convictions and offences, this processing can be performed.

If the controller does not have access to information from the official database about a criminal record or if a court judgment that has entered into force is not available, there can be no question of processing of data relating to criminal convictions.

At the same time, it should be emphasised that the Court of Justice of the European Union has ruled in its judgment in case C-439/19 that penalty points imposed on drivers for road traffic offences are to be considered as personal data relating to criminal convictions and offences within the meaning of Article 10 of the Data Regulation, by indicating that they constitute the processing of

personal data regarding “offences”. Hence, data on criminal convictions and offences refer to both criminal and, in certain cases, administrative offences.

429. If law enforcement authorities request information from a credit institution and the information request contains, for example, information about an initiated criminal case or administrative case or applied security measures, such data should not be considered as personal data relating to criminal convictions and offences. However, if law enforcement authorities request certain actions, such as blocking an account, the data in the request should be considered data relating to security measures. Data obtained from law enforcement authorities may be considered as received under the control of official authority.

430. In cases where customer due diligence is carried out within the framework of the Law, it is allowed to use information publicly available in the media, including negative information, evaluating the relevance of information relevant to each individual situation and avoiding excessive data processing. It is the responsibility of the data controller to use authoritative sources and avoid those that could provide misleading or false information about an individual. Depending on the specific situation, information, which is as old as it could be useful according to the actual circumstances and compatible with the purpose of the data processing, should be taken into account.

7.4. Ensuring the compliance of internal processes defined in the Data Regulation

431. Observing the legal hierarchy of regulatory acts between the Law and the Data Regulation, in the event of a conflict, the Data Regulation prevails.

432. In accordance with Article 24(1) and (2) of the Data Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

433. Pursuant to Article 35(1) of the Data Regulation, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, namely, data protection impact assessment (hereinafter referred to as the “DPIA”).

434. The Data State Inspectorate has drawn up a list of “Types of processing activities for which it is recommended to carry out a data protection impact assessment in accordance with Article 35(4) of the Data Regulation”[69]. Some examples from this list of when a controller should carry out the DPIA:

- where a credit institution evaluates the data of its customers using a credit reference database or a database for the prevention of money laundering and terrorist financing or fraud (see Paragraph 417.2 of the Handbook);

- processing of biometric data (see Sub-chapter 7.2 of the Handbook) with the aim of identifying a natural person together with at least one of the criteria;

- automatic processing of personal data on a large scale and data processing based on profiling (see Sub-chapter 7.7 of the Handbook).

435. An exception is defined in Article 35(10) of the Data Regulation, which provides that where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, Paragraphs 1 to 7 of Article 35 of the Data Regulation shall not apply (refers to how and when the DPIA should be carried out).

Recital 93 of the Data Regulation provides that in the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out a DPIA prior to the processing activities.

From the above, it can be concluded that the initial general impact assessment should be carried out by the legislator during the process of developing the regulatory act, while the controllers should only carry out a DPIA in relation to the processing of personal data mentioned in the regulatory act if it is separately stipulated in the regulatory act.

7.5. Exercise of the rights of data subjects

436. Every controller is responsible for observing the principles set out in the Data Regulation in their activities. The principle of transparency is particularly important, as the controller is obliged to provide the data subject with transparent, understandable, comprehensive information about the existing or planned processing of personal data. By starting the processing of personal data and not ensuring the availability of clear and understandable information to the data subject, the exercise of the data subject's rights and compliance with the provisions of the Data Regulation are endangered.

437. Regarding the provision of information, Article 29 Data Protection Working Party has emphasised in its Guidelines on Transparency under Regulation 2016/679[70] that the purposes of, and legal basis for, processing the personal data should be clear, information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. Article 12(1) of the Data Regulation stipulates that the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 of the Data

Regulation and any communication under Articles 15 to 22 and 34 of the Data Regulation relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided, and the data subject's rights shall be enforceable, unless there are restrictions on the data subject's rights (see Paragraphs 442-449 of the Handbook).

438. The controller shall provide information in writing or in another form, including, if necessary, in electronic form, for example on its website. At the request of the data subject, information may be provided orally, including, if necessary, identifying the data subject prior to providing the information. Full identification of the data subject is not required for the provision of general information about data processing, unless it is provided for by laws or the rules of the controller's internal procedures. It is recommended for credit institutions to train employees who communicate directly with customers about the purposes and justification of data processing, so that employees can explain the need for data processing.

439. It is considered that the controller has provided the necessary information in accordance with Articles 12-14 of the Data Regulation if the controller includes in its privacy policy or other document (for example, in the contract with the customer) general information about the fact that data processing is carried out in the field of AML/CTPF, based on a legal obligation or public interest. Regarding data processing purposes based on other legal grounds (for example, the legitimate interests of the controller), information must be provided separately, but it is permissible to do so in the same documents.

440. The principle of accountability is particularly important precisely because, without providing the data subject with transparent, understandable, comprehensive information about the existing or planned processing of personal data, the data subject cannot properly exercise his/her data protection rights, unless they are limited.

441. Regarding the provision of information, Article 29 Data Protection Working Party has emphasised in its Guidelines on Transparency under Regulation 2016/679[71] that the purposes of and legal basis for processing the personal data should be clear, information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. Thus, the responsibility of the controller is to provide the data subject with information about the purpose and legal basis of data processing in such a way that the data subject clearly understands both the purpose and the legal basis of the personal data processing. The purposes of each case of processing should be separated, following the principles of personal data processing set out in the Data Regulation, including the principles of "purpose limitation" and "data minimisation".

442. Article 12(2) of the Data Regulation stipulates that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22.

443. In accordance with Article 12(3) of the Data Regulation, the controller shall provide information on action taken on a request under Articles 15 to 22 of the Data Regulation to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

444. The controller shall provide the answer in writing; for example, sending it to the data subject in electronic form (in an e-mail message or as a message in the internet bank), providing it at a branch or sending it through a postal merchant. According to Article 12(3) of the Data Regulation, where the data subject makes the request by means of electronic form, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. At the request of the data subject, information can be provided orally on the condition that before the information is provided, the identity of the data subject has been verified in the ways provided for by law or the controller's internal procedures.

445. Article 23(1) of the Data Regulation stipulates that Union or Member State law to which the data controller or processor is subject may restrict, by way of a legislative measure, the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security (point (d)), other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security (point (e)).

446. Section 26 of the PDPL provides that in accordance with Article 23 of the Data Regulation, rights of a data subject may be restricted in cases provided for in other laws and regulations. Whereas in accordance with Paragraph one of Section 27 of the PDPL, a data subject does not have the right to receive the information specified in Article 15 of the Data Regulation if it is prohibited to disclose such information in accordance with the laws and regulations for the purpose of ensuring public financial interests in the areas of tax protection, prevention of money laundering and terrorism financing or of ensuring the supervision of financial market participants and functioning of guarantee systems thereof, application of regulation and macroeconomic analysis.

447. The aforementioned restrictions on the rights of the data subject are set in Section 5^2, Paragraph two, which states that the subjects of the Law, the providers of the closed or open shared Know-Your-Customer utility service, supervisory and control authorities, the Financial Intelligence Unit, the Enterprise Register, and the administrators of the registers referred to in Section 41 of this Law shall not provide information to the data subject on the processing of

data performed within the framework of this law in the field of AML/CTPF, except for the publicly available data. Paragraph two of Section 5^2 of the Law should be read in conjunction with Article 23 of the Data Regulation, and it should be considered that the limitation mentioned in the Law only applies to the access rights of the data subject.

Accordingly, the Law limits the data subject's right to access personal data which the credit institution processes with regard to him/her in order to achieve the purposes of the Law. Considering the fact that the restriction itself contains an exception – "except for publicly available data" – it should be understood so that the data subject nevertheless has access to a certain part of the personal data and has access rights for a certain category of personal data. Publicly available data are personal data that are equally available to both the subject of the Law and the data subject. For example, data provided by the data subject itself to the subject of the Law about him/herself and information that is available free of charge in the state's publicly available registers (for example, data available in the Enterprise Register, which are not considered to be the data of a legal entity), can be considered to be publicly available data. Personal data obtained as a result of customer due diligence by gathering information from both publicly available and non-publicly available sources cannot be considered publicly available data. The data subject's right of access is enforceable in accordance with Article 15 of the Data Regulation and should be separated from the issuance of copies of documents.

A copy of personal data is not the same as a copy of a document. The purpose of the data subject's rights set out in Article 15 of the Data Regulation is to determine the data subject's control over the use of personal data; therefore, the data subject has the right to know what data the controller is processing about him/her, but the rights do not apply to any copies of the materials that are at the controller's disposal, which may contain commercial secrets, third party data, etc.

The controller's obligations specified in the Data Regulation, namely the approval of access to the relevant personal data and the provision of a copy of the personal data, are equally related to the data subject's control over his/her personal data, incl. the possibility to correct errors or inaccuracies in the data, rather than to the data subject's right to control the controller and the information at the controller's disposal.

The exercise of the rights of data subjects is related to the purpose of including said rights in the Data Regulation, that is, recital 7 of the preamble of the Data Regulation mentions that natural persons should have control of their own personal data. Therefore, the exercise of the rights of the data subject also applies to measures that the data subject would take to ensure control over the processing of his/her data (1. whether the particular person processes my data; 2. whether any decisions are made regarding me based on the data; 3. whether the data being processed are accurate; 4. whether my data are transferred to someone else, etc.). Hence, the question of issuing a copy of personal data is not related to receiving copies of documents from the controller's accounting system or another system of the controller, because a copy of personal data is not a copy of documents. In other words, a data copy is understood to be information that reflects the

data subject's personal data held by the controller in the form and manner in which they are processed; for example, the controller has the following personal data at its disposal: name, surname (Jānis Bērziņš), place of birth (Aizkraukle), etc.

Regarding the application of other data subject rights, the application of the exercise of the right of access to data and the legal basis for each specific processing of personal data should be taken into account. The exercise of the rights of the data subject should be evaluated in connection with the legal basis of personal data processing and the prerequisites for ensuring the rights of data subjects established in the Data Regulation.

When evaluating the right to data deletion, it should be noted that this right cannot be used if the condition referred to in Article 17(3)(b) of the Data Regulation occurs, according to which data deletion is not possible if the data must be processed in accordance with EU or Member State law, e.g., the Law.

The legal basis of each person's data processing must also be evaluated in order to assess whether the right to data portability and the right to object to the processing of own data can be exercised in accordance with Articles 20 and 21 of the Data Regulation. The right to data portability cannot be exercised if, with regard to customer due diligence, the legal basis for data processing is not Article 6(1)(a) or (b) of the Data Regulation, but Article 6(1)(c), (e) or (f) of the Data Regulation.

Also, the right to object cannot be extended to data processing that is carried out on the basis of law (Article 6(1)(c) of the Data Regulation). The right to object could only be used in relation to the processing of data carried out on the basis of Article 6(1)(e) or (f) of the Data Regulation; besides, in such a case, the data subject would have to justify his/her particular situation and circumstances.

The right to rectify personal data may be applied to those personal data that the data subject has submitted him/herself or for which the data subject has provided reasonable information about their inaccuracy. The data subject's right to rectify data can be exercised by submitting a request to the subject of the Law, or the data subject can rectify the data him/herself, using electronic tools created by the subjects of the Law, for example, in the internet bank, every customer can change his/her contact address, phone number, e-mail, workplace, etc. Upon receiving clarified data from the data subject, the controller does not need to make amendments to the historically conducted customer due diligence files, as these data were correct and up-to-date until the rectifications were submitted. The right to rectify data applies to the future processing of personal data, starting from the date of rectification. If the personal data have been obtained from another controller, the data subject must initially contact the controller responsible for the accuracy of the particular data. For example, with regard to data maintained in the registers of the Register of Enterprises, one should contact the Register of Enterprises, while with regard to data maintained in the Register of Natural Persons – the Office of Citizenship and Migration Affairs.

448. If the limitation of rights is not stipulated in a law, the data subject should be able to exercise his/her rights. For example, the Sanctions Law does not specify the limitations of the data subject's rights; therefore, the data subject may exercise his/her rights. However, if data processing within the scope of the Sanctions Law is carried out in conjunction with the Law, restrictions on the rights of the data subject shall apply.

449. In cases where the data subject's rights are not limited and the data subject may exercise the right to data deletion (Article 17 of the Data Regulation), it should be taken into account that this right can only be exercised after expiration of the data storage period established by the Law (see Sub-chapter 7.8 of the Handbook), unless other regulatory enactments specify a longer storage period or there is another basis for storing the data longer (e.g., for the establishment, exercise or defence of legal claims).

7.6. Processing of data of natural persons in cooperation with other subjects of the Law (at national and international level)

450. Exchange of data of natural persons in the context of Section 44 of the Law is allowed for the implementation of the purposes set out in the Law. It shall be considered that the legal basis for such data exchange is public interest.

451. According to Section 44 of the Law, data exchange is allowed for several purposes:

451.1. upon the request of the correspondent bank or another payment institution or electronic money institution involved in the making of the payment, "a credit institution, payment institution or an electronic money institution shall provide the information and documents applying to the transaction in relation to which the payment is being made, obtained during the course of identification and due diligence of its customers and their beneficial owners or authorised persons" (Paragraph one of Section 44). Transfer of this data to the correspondent bank is permissible on the basis of Article 49(1)(b) of the Data Regulation (the transfer is necessary for the performance of a contract between a controller and a data subject), if the correspondent bank is located outside the EU or the European Economic Area and the European Commission has not, in this regard, taken a decision on the adequacy of the level of protection and appropriate safeguards for data transfer have not been provided. In the above case, the credit institution would not transfer the information if the customer did not initiate the payment. However, it is important to remember the duty of the data controller to ensure the provision of clear and understandable information to the customer before concluding a contract and the observance of the principle of accountability (see Sub-chapter 7.5 of the Handbook);

451.2. "for the implementation of the purposes of this Law, credit institutions and financial institutions have the right to mutually exchange, directly or with the intermediation of the authorised bodies of the abovementioned institutions, the information and documents obtained during the course of identification and due diligence of their customers and the beneficial owners or authorised persons thereof, as well as the information on persons in relation to whom a business

relationship has not been established or has been terminated in accordance with the procedures laid down in this Law" (Paragraph two of Section 44);

451.3. "for the implementation of the purposes of this Law, credit institutions and financial institutions or the authorised bodies thereof, including within the scope of a group, have the right to create, maintain, and electronically process the personal data, to create and maintain personal data processing systems regarding the customers and persons in relation to whom a business relationship has not been established or has been terminated in accordance with the procedures laid down in this Law, the beneficial owners and authorised persons of such persons. In such cases the right of a data subject to request information on data processing, including its purposes, recipients, source from which it has been obtained, right to access his or her data and request their amending, destruction, discontinuation or prohibition of the processing thereof shall not apply to the personal data processing performed" (Paragraph three of Section 44).

As an example of data exchange within the scope of a group of controllers within the EU, the following situation can be mentioned: a parent company as the controller transfers data to a subsidiary company as another controller.

7.7. Automated decision-making

452. According to Article 22(1) of the Data Regulation, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In accordance with Chapter 2 and other sections of the Commission's Customer Due Diligence Regulations[72], a credit institution, a licensed institution and a licensed electronic money institution shall ensure the automated calculation of the risk assessment, which, using a risk assessment-based approach, reflects the MLTPF risk inherent to the customer (data subject) in numerical expression (scoring system). Besides, depending on the applicable technological solution, the numerical evaluation can also be the basis for making an automated decision (Paragraph 13 of the above-referred Regulations). In exceptional cases, the credit institution, licensed payment institution and licensed electronic money institution may not apply automated numerical assessment of the risk. This must correspond to the institution's risk, and the written consent of the Commission must be received. In such cases, the credit institution, licensed payment institution and licensed electronic money institution is obliged to prove that it will objectively ensure the evaluation of the risk inherent to the customer and will determine the extent of customer due diligence measures which is appropriate to the risk inherent to the customer.

453. In the described case, a decision based on automated processing may be taken which produces legal effects concerning the data subject or similarly significantly affects the data subject (Article 22(1) of the Data Regulation), for example, the data subject may be refused the opening of a current account, or enhanced due diligence has been carried out regarding the data subject.

454. Considering the fact that the purpose of the numerical evaluation is to evaluate specific personal aspects related to the data subject, which could indicate a risk related to the possible involvement of the data subject in AML/CTPF, such an evaluation is considered profiling (Article 4(4) of the Data Regulation).

455. In the case described, automated decision-making may include profiling. Taking into account the fact that such data processing is carried out on the basis of a legal act issued by the Commission, the exception referred to in Article 22(2)(b) of the Data Regulation is applicable, according to which such data processing is permitted and is not covered by the data subject's right not to be the subject of such a decision.

7.8. Data storage

456. In accordance with Article 5(1)(e) of the Data Regulation, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

457. Personal data can be stored for longer if the personal data will only be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Data Regulation, provided that appropriate technical and organisational measures are implemented which are provided for in the Data Regulation to protect the rights and freedoms of the data subject ("storage limitation").

458. Personal data shall be considered to be deleted when they cannot be restored or otherwise recovered. If data are deleted from a system (for example, when their further storage in the system is no longer necessary or in accordance with the Data Regulation), then the duplicated data in the subsystems of the system or elsewhere must also be deleted, unless there is another (new) legal basis for this separate processing within the meaning of the Data Regulation. Instead of data deletion, it is permissible to perform the anonymisation of data in such a way that, as a result of this action, the data subject is no longer identified or identifiable.

459. Data of natural persons shall be deleted when the purpose of their storage has been reached and irrespective of the form in which they are stored.

460. Regarding the storage of the customer's file, taking into account the fact that the customer's file (customer's documents that are stored both together and separately) may consist of documents with different storage periods, it shall be considered that the institution has the right to store the entire set of documents, incl. contracts, for 10 years after the termination of any business relationship with the customer (in accordance with the general prescription period for the right of obligations established in Section 1895 of the Civil Law, in order to protect one's legitimate interests in the event of a claim).

461. In the wording of Paragraph two of Section 37 of the Law, which was in force until 08.11.2017, the subject of the Law was required to store customer data in a certain amount for at

least five years after the termination of the business relationship. Whereas, with the law "Amendments to the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing" which entered into force on 09.11.2017 (hereinafter referred to as the "amendments of 09.11.2017"), Paragraph two of Section 37 of the Law is expressed in new wording, stipulating that the subject of the Law shall store the customer's data in a certain amount for five years after the termination of a business relationship or execution of an occasional transaction. At the same time, with the amendments of 09.11.2017, Section 37 of the Law has been supplemented with Paragraph 2.[1], which provides for the obligation of the subject of the Law to destroy the documents and information about the person in its possession after the end of the period of storage of documents and information specified in this Section. Hence, it is to be considered that with the entry into force of the amendments of 09.11.2017, the subjects of the Law no longer have the legal obligation to store customer data for more than five years, unless there is another purpose and legal basis for data storage. The subjects of the Law, who had set the storage period of customer data as longer than five years after the termination of the business relationship, with the entry into force of the amendments of 09.11.2017 were obliged to review the data storage period, as well as, upon the expiry of the storage period, to destroy the documents and information in their disposal about the customer, which have been created in fulfilling the requirements set out in the Law, unless there is another purpose and legal basis for data storage. Besides, it should be taken into account that with the entry into force of the Data Regulation, controllers also had to review personal data processing processes and set storage periods in accordance with the requirements of the Data Regulation. Also, in accordance with Clause 11 of Paragraph one of Section 7 of the Law, when creating the ICS, the subjects of the Law shall provide for at least the requirements and procedures for regular reviewing of the functioning of policies and procedures according to changes in the laws and regulations or the operational processes of the subject of the Law, services provided thereby, governance structure, customer base or regions of operations thereof.

462. In accordance with Paragraph two of Section 37 of the Law, information obtained during the course of customer due diligence shall be stored for five years after the termination of a business relationship. After the expiry of the specified period, said information (documents) must be destroyed, unless the subject of the Law has received the instruction referred to in Paragraph three of Section 37 of the Law to extend the storage period or another case has occurred (see Paragraphs 463-465 of the Handbook).

Example If a credit institution terminates the business relationship with the customer, but the customer's obligations regarding the issued loan remain, i.e., the loan agreement is valid, then the credit institution will store the documents necessary for securing the rights of obligations arising from the loan agreement in accordance with the prescription period provided for in the Civil Law (10 years) or, in the case of loan recovery, until the complete discharge of the obligations or recognition thereof as invalid, while the customer's due diligence file will be stored for the period

prescribed by Law, namely five years after the termination of the business relationship, if no instructions for extension have been received or there is no other basis for data storage. The exception is data obtained within the framework of the Law and related to the issuance of the loan – they should be stored until the termination of the business relationship arising from the loan agreement and for the additional time period specified in Section 37 of the Law, unless there is another basis for data storage.

The date when all customer accounts have a zero balance and the credit institution has closed the customer's last account should be considered the date of termination of the business relationship.

After the termination of the business relationship and in connection with the loan agreement, newly acquired data in the field of AML/CTPF should be stored in accordance with Section 37 of the Law, unless there is another basis for data storage.

463. A credit institution may have compelling legitimate interests in continuing the processing (including storage) of the customer's due diligence documents (materials) for an additional time period of five years in cases where the instructions referred to in Paragraph three of Section 37 of the Law have not been received. Besides, it does not contradict the provisions of Article 40 of the AML IV Directive[73]; however, the credit institution should carry out a thorough assessment of the necessity and proportionality of the storage before extending the storage period (risk assessment-based approach).

Example

The storage period of a "know your customer" file could be extended for high MLTPF risk customers.

464. If investigation or legal proceedings have been initiated against a credit institution, it is permissible to store the data for as long as it is necessary just for this purpose, i.e. more than five or 10 years as provided for in Section 37 of the Law. The justification for the storage period should be subject to a thorough assessment.

465. The storage period of data that are only processed in accordance with the Sanctions Law shall be determined by the controller independently, observing the principle of storage limitation referred to in Article 5(1)(e) of the Data Regulation.

7.9. Training of staff

466. It is the responsibility of each controller to regularly (for example, once a year) conduct staff training, taking into account the official duties and work specifics of each employee. The controller shall have the duty to assess whether the relevant employee faces data protection issues in his/her daily work, serves customers and is able to provide the relevant information to every customer in a clear, understandable and simple language, thus implementing the principle of accountability. Only the controller him/herself is able to analyse the specifics of his/her business, the level of

knowledge of the employees involved and the necessary skills to determine how much in-depth training is needed. It is impossible to define uniform and specific requirements for each controller; however, basic skills would be useful and desirable in practice, such as, for example, concepts of data protection, categories of personal data, distribution of roles in personal data processing (controller or processor), basic principles of processing, determination of the legal basis, data subject rights (especially for employees who work directly with customers), risk assessment in data processing, controller responsibility, data protection violations, data transfer to third countries. A controller may consider grouping employees according to job duties and providing training content that is tailored to a specific group of employees, for example one group may be provided with more in-depth training than another.

7.10. Transfer of data outside the EU or the European Economic Area

467. Article 44 of the Data Regulation is explained in its recital 101, which states that where personal data are transferred from the EU to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the EU by this Regulation should not be undermined.

At the same time, in order to ensure the processing of personal data in accordance with the Data Regulation, the very fact of data transfer is essential. If the person involved in the processing is one of the controller's internal recipients (for example, employees), then control over personal data is not changed, as the internal recipient continues to process personal data within the framework of the controller's authorisation.

Thus, if the controller's internal recipient (for example, a seconded employee) performs data processing in a third country, then no element of transfer can be established (there is no exchange of information between the controller and any other legally distinct entity). A different case is where the controller's employee performs functions in the controller's establishment (for example, a subsidiary company) in a third country or if the controller's employee's stay in the third country is characterised by a certain degree of independence. In such a case, the exchange of information between the controller and the employee could be considered a transfer of personal data to a third country.

In accordance with Article 24 of the Data Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures, hence, if it can be expected that the duties of employees will include data processing in third countries, it is necessary to consider and implement such measures that will reduce or even eliminate the additional risk factors associated with the processing of personal data in third countries.

The employee's work e-mail, first name, last name, work telephone number, IP addresses of the employer's devices are considered information of a legal person in accordance with recital 14 of the Data Regulation.

7.11. Competence of the Data State Inspectorate and the Commission

468. The competence and tasks of the Data State Inspectorate are determined by Articles 55, 57 and 58 of the Data Regulation and Sections 4 and 5 of the PDPL. General supervision of personal data processing falls within the competence of the Data State Inspectorate. The competence of the Commission is the implementation of the monitoring measures specified in the Law and the Sanctions Law, and the Commission can advise the Data State Inspectorate on whether the processing of personal data results from the AML/CTPF and laws in the field of sanctions.

The Data State Inspectorate and the Commission shall cooperate, including when necessary, exchange views and provide mutual assistance to ensure the consistent application and enforcement of the Data Regulation and other laws and regulations.

When obtaining and otherwise processing information from the subjects of the Law, the Data State Inspectorate observes confidentiality, as well as Paragraph one of Section 14 of the PDPL, which states that it shall be prohibited for the staff working in the Inspectorate to disclose information (except for the publicly available information) which they have obtained with regard to the performance of tasks in the Inspectorate.

7.12. Data protection officer

469. When processing data within the framework of AML/CTPF and sanctions compliance, the appointed data protection officer should be consulted if necessary. The duties of the data protection officer are to:

469.1. inform and advise the subject of the Law and its employees, who perform data processing, about their obligations;

469.2. monitor compliance with the Data Regulation and other laws (including internal regulations) on data protection, including ensure the distribution of responsibilities, information and training of employees involved in processing activities, and related audits;

469.3. collect information to identify processing processes, analyse and check the compliance of processing processes with the Data Regulation, inform, give advice and recommendations to the credit institution in connection with data processing;

469.4. provide advice on data protection impact assessment upon request and monitor its implementation;

469.5. cooperate with the supervisory authority;

469.6. be the supervisory authority's point of contact in matters related to processing, incl. in connection with prior consultation and other issues;

469.7. advise data subjects who have contacted the data protection officer.

More detailed information on the role and status of the data protection officer is provided in the Latvian Financial Industry Association's "Recommendations for the Application of the General Data Protection Regulation"[74].

Final provisions

With the entry into force of these Recommendations, the following are repealed:

(1) Commission Recommendation No. 100 of 17.07.2020 "Recommendations for the Establishment of the Internal Control System for Anti-Money Laundering and Countering Terrorism and Proliferation Financing and Sanctions Risk Management, and for Customer Due Diligence";

(2) Commission Recommendation No. 111 of 28.06.2018 "Recommendations to credit institutions and licensed payment and electronic money institutions to reduce the risks associated with the failure to comply with sanctions".

---

[1] Guidelines on 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 ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849, which repeal and replace Guidelines JC/2017/37, available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016934/Guidelines%20ML%20TF%20Risk%20Factors_LV.pdf.

[2] The risk level the institution accepts and is able to manage.

[3] For example, for 2019, it is available at: https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

[4] The turnover of incoming payments of the customer; in cases when the activities of, and the services provided by the institution, do not include the performance of payments, the credit turnover shall be understood to mean the amount of the customer's transactions.

[5] The Institution shall determine them if its activities are subject to risks or risk increasing factors that are not covered by the EBA Guidelines, typologies developed by law enforcement authorities, international or national risk assessments or the Law.

[6] The institution shall prescribe such requirements, if there are risks inherent to its activities or risk increasing factors, not included in the Customer Due Diligence Regulations or the Law.

[7] Senior management is the Executive Board (board of directors) of the institution, if any is established, or a member of the Executive Board, official or employee specially appointed by the Executive Board, who has sufficient knowledge of the exposure of the institution to the AML/CTPF risks and holding a position of a sufficiently high level to take decisions concerning exposure of the institution to the abovementioned risks.

[8] The institution may additionally refer to the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders" (EBA/GL/2017/12), available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1972984/43592777-a543-4a42-8d39-530dd4401832/Joint%20ESMA%20and%20EBA%20Guidelines%20on%20the%20assessment%20of%20suitability%20of%20members%20of%20the%20management%20body%20and%20key%20function%20holders%20%28EBA-GL-2017-12%29.pdf?retry=1

[9] It is recommended that the requirements of these Regulations would be, as far as possible, also considered by other institutions with an increased AML/CTPF risk inherent in their activities.

[10] The use of commercial databases is a significant tool for obtaining and verifying customer due diligence information.

[11] Point "a", Clause 2, Paragraph three, Section 11^1 of the Law.

[12] The example includes an EU Member State, but the same principle would also be applicable to a European Economic Area Member State or OECD Member State.

[13] The institution may also prescribe additional criteria.

[14] The Commission has developed Clause 40 of the Customer Due Diligence Regulations in accordance with Paragraph two, Section 21^1 of the Law, and Clause 40 is applicable with respect to the indication "a" of the definition of a shell arrangement.

[15] To solve the current situation, the Commission has filed proposals for introducing amendments to the Law, by supplementing Point "c" of Paragraph 15^1, Section 1 of the Law.

[16] The customers, for the registration whereof the services of the legal incorporation enterprises are used, create an increased risk with respect to the possible formal specification of the BO.

[17] Commission's recommendations for off-site (remote) identification are also expected to be adopted in the near future, and a reference to these Recommendations is planned in the Handbook.

[18] Based on the risk, the institution may also obtain information about the key cooperation partners from public sources; for example, if the activity of the customer corresponds to the declared one and there is public information available about the key cooperation partners (for example, the customer is a farm, ensuring the supply of dairy products to milk processing enterprises).

[19] Enhanced due diligence before and during the business relationship at regular intervals.

[20] If risks are detected during due diligence that require more frequent transaction analysis, enhanced due diligence shall be performed more often. The criterion of significance and the results of the last due diligence must be viewed in a complete way, in order to avoid the situation where under the influence of the significance of various participants of the group, enhanced due diligence for the entire group must be performed disproportionally often.

[21] Ascertaining the existence of a licence shall refer to the cases when the legal nature of the activity of the customer is related to transactions exposed to a higher AML/ACTPF risk (for example, provision of financial services, organisation of gambling, etc.).

[22] In the case of direct shareholding or control, the BO controls the legal person directly, while in the case of indirect shareholding or control, the control is implemented through the intermediation of another – natural or legal – person.

[23] In accordance with Section 195[1] of the Criminal law a person who knowingly commits the provision of false information to a bank which is authorised by law to request information regarding the BO may be held criminally liable and a criminal penalty may be imposed thereto.

[24] In practice, information can also be obtained from websites where up-to-date data from the Register of Enterprises are available.

[25] Please see more about the ways of obtaining information in Sub-chapter 3.1.3.2.

[26] Pursuant to Paragraph seven of Section 18 of the Law, the terms "presumed BO" and "BO" are separable; therefore, the amount of information referred to in Paragraph two of Section 18 of the Law would not apply to the BO within the meaning of Paragraph five of Section 1 of the BO Law.

[27] https://www.ur.gov.lv/lv/patieso-labuma-guveju-skaidrojums/biedribas-arodbiedribas-politiskas-partijas/.

[28] The norm referred to in the legal framework is determined in accordance with Article (3)(6)(ii) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 684/2012 of the European Parliament and of the

Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[29] In accordance with the term "*the natural person(s) who holds the position of senior managing official(s)*" used in Directive 2015/849, as well as the purpose of indicating the person who is considered to be the beneficial owner, in this case the management body shall mean the highest management body of the association, the board.

[30] In accordance with the provisions of Section 37 of the Law.

[31] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf .

[32] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 684/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[33] Institutions covered by Commission Regulation No. 148 of 01.09.2020 "Regulations on Conducting an Independent Assessment of an Internal Control System for the Prevention of Money Laundering and Terrorism and Proliferation Financing".

[34] Law of International and National Sanctions of the Republic of Latvia, available at: https://likumi.lv/ta/id/280278-starptautisko-un-latvijas-republikas-nacionalo-sankciju-likums.

[35] Ministry of Foreign Affairs of the Republic of Latvia, website: https://www.mfa.gov.lv/lv/sankcijas.

[36] *Council of the European Union "Update of the EU Best Practices for the effective implementation of restrictive measures",* Chapter VIII, available at: https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf.

[37] Available at: https://likumi.lv/ta/id/308141-starptautisko-un-nacionalo-sankciju-ierosinasanas-un-izpildes-kartiba.

[38] Available at: https://likumi.lv/ta/id/316774-sankciju-riska-parvaldisanas-normativie-noteikumi.

[39] Available at: https://likumi.lv/ta/id/292535-noteikumi-par-nacionalo-sankciju-noteiksanu-attieciba-uz-subjektiem-kas-saistiti-ar-korejas-tautas-demokratiskas-republikas.

[40] Available at: https://www.un.org/securitycouncil/sanctions/information; https://www.un.org/securitycouncil/sanctions/information.

[41] Available at: https://eur-lex.europa.eu/legal-content/ENV/TXT/HTML/?uri=OJ:L:2020:426I:FULL&from=EN.

[42] Available at: http://eur-lex.europa.eu/homepage.html?locale=en.

[43] Available at: https://www.financelatvia.eu/wp-content/uploads/2020/10/AML_CFT_vadlinijas_2020_06_10.pdf.

[44] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269.

[45] Ministry of Foreign Affairs of the Republic of Latvia, export control of strategic goods, website: https://www.mfa.gov.lv/arpolitika/ekonomiskas-attiecibas.

[46] Ministry of Foreign Affairs of the Republic of Latvia, control of goods of strategic importance, website: https://www.mfa.gov.lv/tautiesiem-arzemes/aktualitates-tautiesiem/20440-strategiskas-nozimes-precu-kontrole?lang=lv-LV.

[47] Law of International and National Sanctions of the Republic of Latvia, available at: https://likumi.lv/ta/id/280278-starptautisko-un-latvijas-republikas-nacionalo-sankciju-likums.

[48] Financial Intelligence Unit website – Sanctions lists (fid.gov.lv).

[49] Financial Intelligence Unit website – Sanctions lists (fid.gov.lv).

[50] Law on the Prevention of Legalisation of Criminal Proceeds and Financing of Terrorism and Proliferation, available at: https://likumi.lv/ta/id/178987-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-un-proliferacijas-finansesanas-noversanas-likums.

[51] EU Sanctions Card – https://www.sanctionsmap.eu/#/main.

[52] Financial Intelligence Unit – https://sankcijas.fid.gov.lv/.

[53] List of UNSC sanctions – https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.

[54] Financial Intelligence Unit – https://sankcijas.fid.gov.lv/.

[55] https://sankcijas.fid.gov.lv/.

[56] OFAC sanctions programmes and Information – https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

[57] Financial Intelligence Unit's "Terrorism Financing Prevention Strategy for 2019-2021": https://www.fid.gov.lv/lv/darbibas-jomas/vadlinijas-tipologijas-riki.

[58] FATF – https://www.fatf-gafi.org/about/.

[59] FATF "*Risk of terrorist abuse in non-profit organisations"*: https://www.fatf-gafi.org/documents/documents/risk-terrorist-abuse-non-profits.html.

[60] FATF Report on Combating Proliferation Financing, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

[61] Cabinet of Ministers Regulation No. 419 of 25.07.2017 "Regulations Regarding the Imposition of National Sanctions in Relation to Subjects Connected with the Nuclear Programme and Political Regime Implemented by the Democratic People's Republic of Korea", available at: https://likumi.lv/ta/id/292535-noteikumi-par-nacionalo-sankciju-noteiksanu-attieciba-uz-subjektiem-kas-saistiti-ar-korejas-tautas-demokratiskas-republikas.

[62] UNSC report "*Report of the Panel of Experts established to resolution 1874 (2009)"*, available at: https://undocs.org/S/2020/151.

[63] The content of the chapter is coordinated with the Data State Inspectorate.

[64] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[65] Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[66] Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_env.pdf.

[67] Cabinet of Ministers Regulation No. 392 of 03.07.2018 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer". Available at: https://likumi.lv/ta/id/300147-kartiba-kada-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-finansesanas-noversanas-likuma-subjekts-veic-klienta-neklatienes-identifikaciju.

[68] Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.

[69] Available on: https://www.dvi.gov.lv/lv/media/92/download.

[70] Available on: https://www.dvi.gov.lv/lv/media/72/download.

[71] Available on: https://www.dvi.gov.lv/lv/media/72/download.

[72] Available on: https://likumi.lv/ta/id/320289-klientu-izpetes-klientu-padzilinatas-izpetes-un-riska-skaitliska-novertejuma-sistemas-izveides-un-informacijas-tehnologiju.

[73] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 684/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[74] Available at: https://www.financelatvia.eu/wp-content/uploads/2021/02/Ieteikumi_datu_aizsardzibas_regula-1.pdf.

Chairperson of the Financial and Capital Market Commission *S. Purgaile*