COUNCIL OF EUROPE'S COMMITTEE OF EXPERTS ON THE
EVALUATION OF ANTI-MONEY LAUNDERING MEASURES
AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2025)20

Anti-money laundering and counter-terrorist financing measures

Slovak Republic

4th Enhanced Follow-up Report & Technical Compliance Re-Rating

December 2025

Follow-up report

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The 4th Enhanced Follow-up Report and Technical Compliance Re-Rating on Slovak Republic was adopted by the MONEYVAL Committee during its 70th Plenary meeting (16-18 December 2025).

Slovak Republic: 4th Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER)[1] of Slovak Republic was adopted in September 2020. Given the results of the MER, Slovak Republic was placed in enhanced follow-up[2]. Its 1st Enhanced Follow-up Report (FUR) was adopted in November 2022,[3] the 2nd FUR was adopted in December 2023,[4] and the 3rd FUR was adopted in December 2024.[5] This report analyses the progress of Slovak Republic in addressing the technical compliance (TC) deficiencies identified in its MER and/or subsequent FUR, where requested to do so by the country. Re-ratings are given where sufficient progress has been made. Overall, the expectation is that countries will have addressed most, if not all, TC deficiencies by the end of the third year from the adoption of their MER.[6]

2. The assessment of the request of Slovak Republic for technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur team (together with the MONEYVAL Secretariat):

- Azerbaijan
- Bulgaria
- Cyprus

3. Section III of this report summarises the progress made by Slovak Republic in improving technical compliance. Section IV sets out the conclusion and a table showing which Recommendations have been re-rated.

4. In line with MONEYVAL's Rules of Procedure, the follow-up process is desk-based – using information provided by the authorities, including revised legislation. It does not address what progress a country has made to improve the effectiveness of changes introduced by the country.

II. BACKGROUND, RISK AND CONTEXT

5. A number of significant changes have been made since adoption of the MER or subsequent FUR that are relevant for considering Recommendations that have been reassessed.

6. On 15 January 2025, Act No. 387/2024 Coll. entered into force, amending the AML/CFT Act (Act No. 297/2008 Coll.) and 12 other laws to address deficiencies identified in the 5th round MER of the Slovak Republic and align with EU requirements. The amendments covered a wide range of FATF Recommendations, including, Recommendation (R.) 10, R.12, R.13, R.15, R.18, R.19, R.23, R.28, R.29, R.32, and R.35, and introduced measures on customer due diligence (CDD), politically exposed persons (PEPs), correspondent banking, virtual asset service providers (VASPs), internal controls, and supervision.

1. Mutual Evaluation Report 2020, available at: https://rm.coe.int/moneyval-2020-21-5th-round-mer-Slovak Republic/1680a02853.
2. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
3. 1st Enhanced Follow-up Report, available at: https://rm.coe.int/moneyval-2022-16-fur-sk/1680a9211a.
4. 2nd Enhanced Follow-up Report, available at: https://rm.coe.int/moneyval-2023-21-sk-5thround-2ndenhfur/1680ae98c8.
5. 3rd Enhanced Follow-up Report, available at: https://rm.coe.int/moneyval-2024-19-sk-5thround-3rdenhfur/1680b35473
6. Slovak Republic's submission of the country report for this FUR preceded a Plenary decision to amend the Rules of Procedure for the 5th Round of Mutual Evaluations. Therefore, the 2013 version of the Methodology applies to this technical compliance re-rating exercise.

7. The Slovak Republic also promulgated Act No. 248/2024 Coll, which implements certain provisions of Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCAR). The amendments to the AML/CFT Act, effective from January 15, 2025, also amended Act No 171/1993 Coll. on the Police Force, Act No. 199/2004 Coll. Customs Act, and Act No. 372/1990 Coll. Offences Act.

8. For crypto-asset service providers (CASPs), Act No. 248/2024 Coll, empowers the National Bank of Slovakia to act as the prudential supervisor of crypto-asset service providers and issuers of asset-referenced tokens while the amendments to the AML/CFT Act allow the Financial Intelligence Unit (FIU) to be the AML/CFT supervisor for CASPs.

III. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

9. This section summarises the progress made by Slovak Republic to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER and applicable subsequent FUR for which the authorities have requested a re-rating (R.8, R.10, R.12, R.13, R.15, R.18, R.19, R.23, R.28, R.29, R.32, R.35).

10. This report takes into consideration only relevant laws, regulations or other anti-money laundering and combating financing of terrorism (AML/CFT measures) that are in force and effect at the time that Slovak Republic submitted its country reporting template – at least six months before the follow-up report (FUR) is due to be considered by MONEYVAL.[7]

IV. PROGRESS TO ADDRESS TECHNICAL COMPLIANCE DEFICIENCIES IDENTIFIED IN THE MER AND SUBSEQUENT FURS

11. Slovak Republic has made progress to address the technical compliance deficiencies identified in the MER and applicable subsequent FURs. As a result of this progress, Slovak Republic has been re-rated on R.10, R.12, R.13, R.15, R.19, R.23, R.29 and R.32. The country asked for a number of re-ratings for other R.8, R.18, R.28 and R.35 which were also analysed but no re-rating has been provided.

12. Annex A provides a description of the country's compliance with each Recommendation that is reassessed, set out by criterion, with all criteria covered. Annex B provides the consolidated list of remaining deficiencies of the re-assessed Recommendations.

V. CONCLUSION

13. Overall, in light of the progress made by Slovak Republic since its 3rd enhanced FUR was adopted, its technical compliance with the Financial Action Task Force (FATF) Recommendations has been re-rated as follows.

7. This rule may be relaxed in the exceptional case where legislation is not yet in force at the six-month deadline, but the text will not change and will be in force by the time of the plenary. In other words, the legislation has been enacted, but it is awaiting the expiry of an implementation or transitional period before it is enforceable. In all other cases the procedural deadlines should be strictly followed to ensure that experts have sufficient time to do their analysis.

Table 1. Technical compliance with re-ratings, November 2025

R.1	R.2	R.3	R.4	R.5
LC (FUR1 2022) ~~PC (MER)~~	C (MER)	LC (MER)	LC (MER)	LC (MER)
R.6	R.7	R.8	R.9	R.10
LC (MER)	LC (MER)	PC (FUR4 2025) PC (FUR3 2024) PC (FUR2 2023) PC (MER)	LC (MER)	**LC (FUR4 2025)** ~~PC (FUR1 2022)~~ ~~PC (MER)~~
R.11	R.12	R.13	R.14	R.15
LC (MER)	**LC (FUR4 2025)** ~~PC (FUR1 2022)~~ ~~PC (MER)~~	**C (FUR4 2025)** ~~PC (FUR1 2022)~~ ~~PC (MER)~~	LC (MER)	**LC (FUR4 2025)** ~~PC (FUR3 2024)~~ ~~PC (FUR1 2022)~~ ~~LC (MER)~~
R.16	R.17	R.18	R.19	R.20
LC (MER)	LC (MER)	PC (FUR4 2025) ~~PC (FUR1 2022)~~ ~~PC (MER)~~	**C (FUR4 2025)** ~~PC (FUR3 2024)~~ ~~PC (FUR1 2022)~~ ~~PC (MER)~~	C (FUR1 2022) ~~PC (MER)~~
R.21	R.22	R.23	R.24	R.25
LC (MER)	LC (MER)	**LC (FUR4 2025)** ~~PC (FUR1 2022)~~ ~~PC (MER)~~	LC (MER)	LC (MER)
R.26	R.27	R.28	R.29	R.30
LC (FUR2 2023) ~~PC (MER)~~	LC (MER)	PC (FUR4 2025) ~~PC (FUR2 2023)~~ ~~PC (FUR 1 2022)~~ ~~PC (MER)~~	**LC (FUR 4 2025)** ~~PC (FUR1 2022)~~ ~~PC (MER)~~	C (FUR1 2022) ~~PC (MER)~~
R.31	R.32	R.33	R.34	R.35
LC (MER)	**LC (FUR 4 2025)** ~~PC (FUR 1 2022)~~ ~~PC (MER)~~	C (FUR 1 2022) ~~PC (MER)~~	LC (MER)	PC (FUR4 2025) ~~PC (MER)~~
R.36	R.37	R.38	R.39	R.40
LC (MER)	C (MER)	LC (MER)	LC (MER)	LC (MER)

Note: There are four possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC), and non-compliant (NC).

14. As the issues of concern have been adequately addressed with regard to the "big six" recommendation[8] (R.10), in line with Rule 27 of the Rules of Procedure for the 5th Round of Mutual Evaluations, Slovak Republic will be removed from the compliance enhancing procedure.

15. Given that MONEYVAL's onsite visit for the 6th round mutual evaluation of Slovak Republic is scheduled for October 2028, in line with Rule 23 of the Rules of Procedure, Slovak Republic is no longer subject to the 5th Round follow-up process.

8. The "big six" Recommendations are: R.3, R.5, R.6, R.10, R.11 and R.20.

Annex A: Reassessed Recommendations

Recommendation 8 - Non-profit organisations

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (no upgrade requested)
FUR2	2023	PC (upgrade requested, maintained at PC)
FUR 3	2024	PC (upgrade requested, maintained at PC)
FUR 4	2025	PC (upgrade requested, maintained at PC)

1. In the 5th round of evaluations Slovak Republic was rated partially compliant with R.8. The NPO sector was assessed as part of the national risk assessment (NRA) but the subset of NPOs which would fall within FATF definition was not identified. No formal review of the adequacy of measures was undertaken, no systematic and specific outreach was conducted, no best practices were developed. There was no supervision over NPOs, no specific training was provided to relevant authorities.

2. Slovak Republic's compliance with R.8 was reassessed under its 2nd and 3rd enhanced FURs. Slovak Republic retained a rating of PC, and the following deficiencies remained: no identification of sub-categories that are at risk of terrorism financing (TF) abuse; no review of the adequacy of measures related to the subset of NPO sector that may be abused for TF and no risk -based approach in supervision of NPOs applied.

3. **Criterion 8.1** –

(a) Art. 9 (e) of the AML/CFT Act, defines "a corporation" as a customer being a foundation (as regulated by Act 34/2001 Coll), a non-profit organisation providing services of general economic interest (as regulated by Act 213/1997 Coll.), a non-investment fund (as regulated by Act 147/1997 Coll.) and other special-purpose corporations irrespective of their legal personality which manage and distribute funds. The 2nd NRA provides general information on the overall level of risk to TF abuse the NPOs face in Slovak Republic, and gives some examples of activities or characteristics, which are likely to carry a higher risk of TF abuse. The NRA identified the subset of NPOs which would fall within the FATF definition, without detailing the sub-categories which are at risk of TF abuse. According to the Sectorial Risk Assessment (SRA) published in April 2024 and as updated in May 2025, civic associations and organisations with an international dimension are legal forms of NPOs that are not required to keep records of their activities or to publish annual reports. Authorities advised that this lack of oversight limits the ability to assess NPO activities and identify those at higher risk of TF abuse, which is why a new legislation (Act No. 109 of 16 April 2025 amending Act No. 213/1997 on non-profit making organisations providing services of general interest) was introduced, requiring civic associations and organisations with an international dimension, to file annual financial statements, in case their income in a calendar year exceeds EUR 35 000. While the SRA analysed some characteristics of NPOs, current legislation and regulatory measures, accountability and supervision, interrelations with higher risk countries (including limited assessment of risks of NPOs' use of funds from public collections in these countries), it concluded that overall risk level of NPOs TF abuse is low. However, notwithstanding the update of May 2025, the SRA's limited functional analysis of NPOs prevents a clear determination of which NPOs are at risk when engaging in what specific types of activities and how these characteristics are uniquely applicable to Slovak Republic NPO environment.

(b) According to the 2nd NRA, in the period under review (2016-2019), there were no cases where NPOs were used or misused for money laundering (ML) or TF. Similarly, the SRA for 2020-2023

recorded no presence or activities of terrorist organisations in the country, nor any investigations of TF cases involving NPOs. However, absence of such involvement does not equate to the identification of the nature of threats posed by terrorist entities to the NPOs. Whilst the SRA outlines potential threats, such as returnees from conflict regions and radicalisation, these scenarios are general in nature and do not link NPO characteristics to the described scenarios. In 2024, one case of financing of a terrorist organisation was recorded and prosecuted. This enabled the authorities to identify certain vulnerabilities in the NGO sector to TF risk more precisely. However, this analysis is based on a single case and does not provide a basis for the in-depth identification of potential abuses of NPOs. Nonetheless, it must be noted that ways of potential misuse of NPOs for the financing of terrorism are described in the Information for NGOs in the field of combating the financing of terrorism listed on the FIU's website.

(c) Slovak Republic conducted a formal review of the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for terrorism financing support. There were certain shortcomings identified in the oversight and accountability of civil associations and NPOs providing services of general interest, and the necessary recommendations were made accordingly. Furthermore, as concerns remain under 8.1(a) criteria, it is not clear if adequacy of measures has been identified to the full extent. A new legislation's requirement (Act No. 109 of 16 April 2025, as referred under c.8.1(a)) to civic associations and organisations with an international dimension, to file annual financial, does not seem to be relevant for this sub-criterion since these measures target a wide range of civil associations and organisations and not specifically the NPOs likely to be at risk of terrorist financing abuse. The Register of Non-Governmental Non-Profit Organisations became operational from 1st of January 2021 and represents a reliable, up-to-date and unified source register of non-governmental NPOs, including data on the beneficial users of NPOs. However, there is no obvious link between the risks identified and the establishment of the registry. Moreover, its establishment was foreseen before the completion of the NRA.

(d) A general provision was introduced as an amendment to the AML/CFT Act according to which the NRA shall be submitted to the Government for approval at the latest four years after the previous approval.

4. **Criterion 8.2** –

(a) The Slovak Republic has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs, in particular through specific laws regulating the various legal forms of NPOs, where all relevant data on bookkeeping (single-entry or double-entry accounting) are presented in annual reports, in the register of financial statements, in tax returns, in the register of BOs, while meeting the conditions for applying for a share tax. In the area of transparency of NPOs and their publicly available information, legislative changes were performed in the Slovak Republic. The efficiency of the use of public funds is closely related to the record of non-governmental non-profit organisations. The largest organisations in the NPOs sector in terms of financial volume are foundations, which are also the most controlled and regulated by legislation (Act no. 34/2002 Coll. on Foundations and on Amendments to the Civil Code). Obligations of foundations related to funding control include: the obligation to prepare financial statements and the annual report, the obligation to have the financial statements and the annual report audited by an auditor, the obligation to publish the annual report and deposit it in the register of financial statements, obligation to file a tax return if it has revenue subject to tax (Art. 34 and 35 of the Act no. 34/2002 Coll.).

(b) Specific outreach to the NPO sector or the donor community on FT issues has been conducted. The authorities asserted that the NPOs are notified by the FSJ of possible misuse of terrorist

financing in the context of AML/CFT controls that FIU performs in this sector with four such inspections reported in the period under review. In February 2023, the FIU issued the "Information for NGOs in the field of combating the financing of terrorism" to raise and deepen NPOs awareness on potential vulnerabilities of TF abuse and terrorist financing risks, and updated it in May 2024 as result of conducted SRA.

(c) As mentioned above, the FIU's document "Information for NGOs in the field of combating the financing of terrorism" contains best practices to address TF risk and vulnerabilities. It also provides a set of steps to be undertaken by the NPO sector to reduce the risks of being misused for TF. The FIU, with involvement of and in co-operation with NPO sector, updated this document to reflect the conclusions of the SRA NPO (April 2024) and following consultation with NPOs' representatives published on its website an information leaflet "Awareness-raising for NPOs in the area of countering TF".

(d) Foundations are obliged to deposit funds that are part of the foundation assets, to an account at a bank or a branch of foreign bank. Apart from that, "Information for NGO´s in the field of combating the financing of terrorism" is encouraging NPOs to conduct transactions via regulated financial channels, by providing the risk factors increasing the possibility of NGO abuse, inclusively on the increased use of cash transactions. Additionally, information is available on the NBS's website with the recommendation not to enter into business relationships with "problematic" entities and check the authorisation of individual financial market entities on the NBS website.

5. **Criterion 8.3** – The Slovak Republic does not apply a risk-based approach in supervision of NPOs at risk of TF abuse but authorities report a number of measures applied to all main types of NPOs according to the AML/CFT Act or according to sectorial regulation (i.e. Act 34/2002 on Foundations, Act 213/1997 on Non-Profit Organisations Providing Public Benefit Services and Act 147/1997 on non-investment funds).

6. For the purposes of the AML/CFT Act, a foundation, a non-profit organisation providing services of general interest, and a non-investment fund are obliged to carry out the identification of the donor and the identification of the natural person or legal entity whose property association has provided funds under Art. 25 of the AML/CFT Act if the value of the donation or the amount of provided funds reaches at least EUR 1 000.

7. The annual reports of the foundation, a non-profit organisation providing services of general interest and a non-investment fund shall be filed in the Register of Financial Statements. All of those shall keep accounts and shall keep accounting records (including annual reports) for the ten years following the year to which they relate (Art. 35(3) of Act 431/2002 on Accounting). On the basis of that document retention, the competent authorities may, if necessary, subsequently verify transactions in order to establish whether the funds have been received and spent in a manner consistent with the purpose and objectives of foundations, non-profit organisations and non-investment funds.

8. The authorities report that in the context of its rights and obligations, the Ministry of Interior (MoI) may impose fines on foundations for failure to submit an annual report, in line with the Act No. 109 of 16 April 2025 amending Act No. 213/1997 on non-profit making organisations providing services of general interest.

9. The FIU's Methodological Guidance on the selection of the control of obliged entities, amended in April 2024, establishes a risk-oriented supervision of obliged entities and pool of assets, including some types of NPOs, based on the ML/TF risk assessment. According to authorities, when considering individual ML/TF factors, FIU would refer to SRA as strategic analysis and consider its findings to

supervise covered NPOs. However, the guidance serves as a general tool for FIU only, and no information was provided regarding supervisory risk-based measures implemented by other competent authorities overseeing NPOs.

10. **Criterion 8.4** –

(a) The authorities stated that the NPOs sector is monitored according to the annual controls plan used by the FIU when carrying out controls at entities that show the signs of risk. The FIU has implemented a risk-oriented approach to carrying out controls, as referred to in Art. 2.1 of the Order of FIU Director No. 126/2018 and in the Methodological Guidelines on the Procedure for Controlling the Compliance of Obligations of Obliged Persons Pursuant to the AML/CFT Act by Police Officers of the Obligation of Controlled Persons of FIU No. 34/2018. After the establishment of the register of non-governmental non-profit organisations, responsible authorities (MoI and district offices) before and after registering a legal person perform controls of the entities in compliance with the applicable generally binding legal regulation, inclusively by evaluating the Annual Reports. However, as stated under criterion 8.3. Slovak Republic does not apply a risk-based approach in supervision.

(b) The FIU is entitled to conduct controls on NPOs for the purpose of identification of the beneficial ownership (BO) and verification of the veracity and correctness of data about the BO, for the purpose of identifying persons (donors and recipients of donations worth more than EUR 1 000) or for the purpose of checking disposal of property (Art. 25 of the AML/CFT Act). For the non-performance of these obligations, the FIU may impose fines of up to EUR 200 000. (Art. 33 (3) AML/CFT Act). If a foundation fails to perform the obligation to deposit an annual report in the public part of the register of financial statements, the Ministry of the Interior may impose a fine of up to EUR 1 000 (§ 36 of Act 34/2002 Coll. on Foundations). NPOs are legal entities and are subject to Act No. 91/2016 Coll. on Criminal Liability of Legal Entities. As legal entities, NPOs may be criminally prosecuted for committing the offense of ML under § 233 and § 234 of the Criminal Code, and for the offense of terrorist financing under § 419c of the Criminal Code. It results that there is legal base to application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.

11. **Criterion 8.5** –

(a) Slovak Republic is effective in NPO related co-operation, co-ordination and information sharing. If necessary, FIU and law enforcement agency (LEA) are entitled to request information on NPOs from the Register of non-governmental non-profit organisations (including paper documents such as memorandum of association, statutes, annual reports, etc.). NPOs keep accounts according to Act no. 563/1991 on accounting and are subject to control by the tax authorities. Upon request, the tax authorities provide information to FIU/LEA. According to § 25 para. 2 of the AML/CFT Act FIU is authorised to carry out inspections in NPOs also for the purpose of property management. In case of unauthorised disposal of assets in NPOs, the FIU withdraws the LEA information. The FIU shall disseminate the information from the unusual transaction reports (UTRs) regarding NPOs to the competent authorities, for example Financial Administration, LEA, etc.

(b) The National Counter-Terrorism Unit of the National Criminal Agency is a Police Force unit which has its own investigators and operational search activity specialists who are authorised to examine, detect and investigate suspected terrorist financing. The Slovak authorities provided a detailed list of training activities related to TF issues, inclusively with the implication of NPOs, oriented for the National Counter-Terrorism Unit in order to gain sufficient investigative expertise and capability to examine NPOs suspected of TF abuse/ TF support.

(c) Information on the sub-group of organisations that meet the FATF definition of NPOs (mainly non-profit organisations providing services of general interest and foundations) is provided in the Register of non-governmental non-profit organisations maintained by the MoI of the Slovak Republic. Hence, this information can be obtained in the course of an investigation.

(d) The SIS, FIU and Counter-Terrorism Unit - National Criminal Agency Slovak Republic (CTU – NAKA) are competent to receive and analyse information on any form of TF abuse of NPOs. In addition, on January 1, 2013, the National Security Analytical Center (NSAC) was established within the SIS organisational structure, with the aim to make co-operation among security forces more effective. The key tasks of NSAC are the preparation of comprehensive analytical assessments of security incidents based on reports and statements received from state authorities, monitoring security situation in open sources and the provision of analytical products on security threats to designated recipients. Although no statistics or examples of NPO abuse information sharing were presented to the AT, from the general scope of NSAC one can deduce that such would fall under the attributions of NSAC.

12. **Criterion 8.6** – The FIU uses the procedures and mechanisms for international co-operation that are provided under the AML/CFT Act, to handle information requests regarding to NPOs. Joint investigation teams (JITs) and the Joint Customs Operations (JCO) are mechanisms which can be used by the National Counter-Terrorism Unit in the area of the fight against TF under the applicable legislation, including in case a NPO would be involved. JITs and JCOs have not been used in practice, given that no direct activity by terrorist groups has been recorded so far, and no persons or groups have been localised that would prepare to commit a terrorist offense.

Weighting and Conclusion

13. The NPOs sector was assessed as part of the 2nd NRA and recently in 2024 as a part of Sectorial Risk Assessment, which was updated in May 2025, and the authorities to some extent identified the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse, although without detailing which NPOs are at a higher risk of TF abuse based on their specific activities and characteristics (c.8.1(a) and (b)). A review of the adequacy of measures, including the subset of NPO sector that may be abused for terrorism financing support has been conducted to a limited extent (c.8.1(c)). Specific outreach to the NPO sector or the donor community on FT issues has been conducted and best practices have been developed in co-operation with NPOs to protect them from TF abuse. It seems that there is a legal base to application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs. NPO information exchange is done in the usual manner by the FIU. Overall, Slovak Republic has addressed some of the deficiencies under c.8.1(c) and c.8.2(c), however it still has not identified the NPOs that are at higher risk of TF abuse (c.8.1(a) and (b)) and does not apply risk-based approach in supervision of NPOs at risk (c.8.3). Therefore, **Slovak Republic remains rated PC with R.8**.

Recommendation 10 – Customer due diligence

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ LC (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.10 based on the following deficiencies: absence of full range of CDD measures when carrying out occasional wire transfers over EUR 1 000 (c.10.2(c)); no legal requirement to verify whether persons act on behalf of third person are authorised and verify the identity of that person and the customer (c.10.4); there is no requirement to verify BOs based on reliable source data (c.10.5); no clear information provided regarding FI's understanding the purpose and intended nature of the business relationship (c.10.6); absence of the specific requirement to examine, where necessary, whether transactions of the customer are consistent with the source of funds (c.10.7); there is no obligation to understand the customer's business (c.10.8); identifying the natural person authorised to act on behalf of the legal entity also does not amount to obtaining the names of all relevant persons holding the senior management position (e.g. senior managing directors) (c.10.9(b)); FIs are not required to distinguish the address of the registered office of the legal entity from its principal place of business, and if different, obtain the relevant information (c.10.9(c)); the BO definition of trusts is not in line of the requirements of c.10.11 as it required identification based on a threshold and it does not cover the protector (where applicable) (c.10.11(a)); there are no specific requirements concerning beneficiaries designated by characteristics or class (c.10.11(a)); absence of the similar definition of BOs for other types of legal arrangements (c.10.11(b)); no specific requirement to gather the relevant information in relation to beneficiaries designated by characteristics or class to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the pay-out (c.10.12(b)); lack of information about other investment-related insurance policies and the applicable requirements (c.10.12); no requirement to include the beneficiary of a life insurance policy as a relevant risk factor when determining whether to apply enhanced CDD (c.10.13); absence of legal provisions that would require FIs to apply CDD to existing customers depending on the materiality (c.10.16); simplified CDD measures in low-risk scenarios which are not justified by the findings of the NRA (c.10.18); absence of the requirement to refuse establishing a business relationship or performing a transaction, and to terminate a business relationship where FIs cannot perform other required CDD measures such as conducting ongoing due diligence (c.10.19(a)); obligation to report unusual transactions does not broadly extent to the situation when a financial institution is unable to comply with the relevant CDD measures (c.10.19(b)); the legislation does not contain the permission for the FIs refrain from pursuing the CDD process in case of risk of tipping-off the customer followed by submission of a UTR (c.10.20). Slovak Republic has requested an upgrade in the context of the 1st FUR due to certain changes in legislation, however, no sufficient progress has been made, and the rating remained.

2. **Criterion 10.1** – According to Art. 24(2) of the AML/CFT Act, FIs are prohibited from entering into a business relationship or performing a transaction with an anonymous customer. Furthermore, Art. 89(2) of the Law on Banks prohibits carrying out transactions of customers on an anonymous basis. Although there is no explicit prohibition on keeping accounts in obviously fictitious names, the AML/CFT Act requires verifying the identity of customers when establishing business relations or carrying out occasional transactions over EUR 1 000.

When CDD is Required

3. **Criterion 10.2** – Art. 10(2) of the AML/CFT Act requires to apply CDD, inter alia, when (i) establishing a business relationship, (ii) carrying out an occasional transaction over EUR 15 000 or in case of a cash transaction, over EUR 10 000, carried out in a single operation or in several operations that appear linked, (iii) there is a suspicion that the customer is preparing or performing an unusual transaction regardless of its value, (iv) there are doubts about the veracity or completeness of the previously obtained CDD data, or (v) carrying out an occasional transaction outside a regular business relationship which represents a transfer of funds or a transfer of crypto-assets over EUR 1 000. The definition of an unusual transaction (Art. 4) covers suspicions of ML/TF.

Required CDD measures for all customers

4. **Criterion 10.3** – The requirement to identify the customer and verify that customer`s identity is set out in Art. 10(1) of the AML/CFT Act. The identity of natural persons is verified on the basis of identity documents and with the physical presence of a customer or by non-face to face interaction using technical means that ensure the same degree of reliability (Art. 8(1)(a)). Legal persons including state authorities, are verified based on the data or documents obtained from official corporate registers or other reliable and independent sources.

5. **Criterion 10.4** – Art. 10(7) of the AML/CFT Act stipulate that when carrying out due diligence, the obliged person shall ascertain whether the customer acts in their own name. If the obliged person finds out that the customer does not act in their own name, Articles 7(1)(c) and 8(1)(c) of the AML/CFT Act stipulate the obligation to identify and verify the identity of a person authorised to act on behalf of a customer. The obliged person shall follow the same procedure in case that there are doubts whether the customer acts in their own name. The obliged entity is required to verify the submission of a proof of authorisation of that person- whether the customer is natural or legal person- including its terms of validity and scope (AML/CFT Law, Art. 7(1)(c)). Verification shall be based on documents, data or information obtained from the submitted proof of authorisation, from an official register or other official records, or from another reliable and independent source. When the authorisation is carried out under a power of attorney, the signature of the represented person must be officially certified (AML/CFT Law, Art. 8(1)(c)).

6. **Criterion 10.5** – Art. 10(1)(b) of the AML/CFT Act requires FIs to identify the BO and take adequate measures to verify his/her identity, including measures to establish the customer's ownership and management structure if the customer is a legal entity or an association of assets to verify the information on BO. FIs are also not permitted to solely rely on the data obtained from corporate registries and public authorities. However, the obligation to verify the information relating to the BO identification from an additional reliable source applies only when there is a higher risk of ML/TF (AML/CFT Law, Art. 10(1)(b)). The BO is defined by Art. 6a of the AML/CFT Act as the natural person who ultimately owns or controls the legal entity, an entrepreneur natural person or any other natural person in whose favour a transaction/activity is being conducted. This definition however does not cover all instances when a natural person ultimately controls another natural person.

7. **Criterion 10.6** – Art. 10(1)(c) of the AML/CFT Act requires FIs to obtain and evaluate information about the purpose and intended nature of a business relationship.

8. **Criterion 10.7** – According to Art. 10(1)(g) of the AML/CFT Act, FIs must carry out the ongoing monitoring of business relationships, including the scrutiny of transactions undertaken throughout the course of those relationships to ensure that transactions are consistent with their knowledge of the customer and its business and risk profile, including the source of funds. FIs must also ensure that CDD documents, data and information are kept updated.

Specific CDD measures required for legal persons and legal arrangements

9. **Criterion 10.8** – Art. 10(1)(b) of the AML/CFT Act requires FIs to understand the ownership and control structure of clients (legal entities and trusts) in the process of establishing BOs. REs should obtain and evaluate information about the nature of the client's business in order to understand the nature of the customer's business, ownership and management structure.

10. **Criterion 10.9** –

(a) The data required to identify legal entities and the sources of verification therein are set out in Articles 7(1)(b) and 8(1)(b) of the AML/CFT Act. Thus, FIs are required to obtain the name of the legal entity and address of its registered office. FIs are also required to identify the natural person authorised to act on behalf of the legal entity. These data must be verified based on the information or documents obtained from the official corporate registry or other reliable and independent sources. In case of corporate registries, the proof of existence (e.g. certificate of incorporation, extract) would normally be obtained; however, FIs may also obtain relevant information from other credible sources, which may not contain the information mentioned by authorities.

(b) Identifying the natural person authorised to act on behalf of the legal entity or association of assets also does not amount to obtaining the names of all relevant persons holding the senior management position (e.g. senior managing directors).

(c) FIs are required to distinguish the address of the registered office of the legal entity or association of assets from its principal place of business, and if different, obtain the relevant information (AML/CFT Law, Art.7(b)). Regarding the registered address – the legal entities have one registered address/"seat" listed in Commercial register (Art. 2/ 3 of the Commercial Code). Natural persons have the "place of business" listed in the Trade register (Art. 60/2/d Law No. 455/1991 Coll. on Business). Corporations have "seat" listed in their respective registers, see effectiveness part. (Foundation, non-profit organisation non-investment fund – Art. 2/ 2 / a), b) a c), and Art. 2 / 1 / a) Law No. 346/2018 Coll. on the register, non-governmental organisations.

11. **Criterion 10.10** – BO of the legal person is defined by Art. 6a(1)(2) of the AML/CFT Act and includes the natural person(s) who:

(a) ultimately owns or controls the legal entity through direct or indirect ownership or control of at least 25% of shares or voting rights including through bearer shareholdings, or benefits from at least 25% of the economic activity of the business;

(b) is authorised to appoint, otherwise determine the composition of or withdraw the statutory, managing, supervisory or audit bodies, or controls the legal person in any other way;

(c) is the member of top management in case no other person meets the criteria noted above. The member of top management is defined as the member of the statutory body, procurator or manager under the direct authority of the statutory body. Pursuant to Art. 6(2) of the AML Law, in case that any person does not meet criteria listed in Art. 6a(1) of the law, members of top management shall be considered as the BO of the entity; member of top management means a statutory body, a member of the statutory body, procurator and manager under the direct authority of the statutory body. The authorities explained that where several persons act in those capacities, all of them shall be considered as senior managing officials.

12. **Criterion 10.11** –

(a) According to the Art. 6a (1) (d) in case of a trust or a similar legal arrangement established under the law of another jurisdiction (foreign trust)[9] the BO is: (i) the settlor, (ii) the trustee, (iii) the person supervising the administration of the foreign trust, if appointed (the protector), (iv) a future beneficiary of trust funds, or when not yet determined, the circle class of beneficiaries; and (v) any person with an ultimate control over the assets of trust through direct or indirect ownership or by other means. For beneficiaries that are designated by characteristics or class, the identification is limited to the circle of persons having a substantial benefit from the founding or operation of a trust, which is not consistent with the FATF standard. Moreover, there is no requirement for FIs to obtain sufficient information concerning the beneficiary of foreign trust (designated by characteristics or class) to ensure that they will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

(b) Legal arrangements similar to trusts are referred to as "foreign trusts" under Art. 6a(1)(d) of the AML/CFT Act and are subject to the same BO requirements. However, there is no specific obligation to identify persons having equivalent or similar positions to those in a trust (particularly with regard to the settlor and the trustee as specified in Art. 6a(d)(1) and (2) of the AML/CFT Act). Notwithstanding, the lack of updated statistics on use of foreign trusts and other similar legal arrangements, their use by foreigners appears to be minimal in the Slovak Republic context.[10]

CDD for beneficiaries of life insurance policies

13. **Criterion 10.12** – Beneficiaries of life and investment-related insurance policies must be identified and verified prior to or at the time of payout, or when the beneficiary intends to exercise the rights vested under the policy. Pursuant to Art. 10(8) of the AML/CFT Act, the obliged entity is required to gather the sufficient information to enable identification of the particular beneficiary at the time of the payout, including where the beneficiary is designated by characteristics, class or other means.

14. **Criterion 10.13** – The risk level posed by the beneficiary of a life insurance policy is included as a higher-risk factor for applying enhanced CDD (Annex 2(4) of the AML/CFT Act). When the beneficiary is a legal person, the obliged entities are required to obtain sufficient information to identify the beneficiary at the time of payment of the benefit and verify the identification of the beneficial owner of a beneficiary (AML/CFT Law, Art. 10(8)(b)(c)). There is no such requirement in relation to a beneficiary that is a legal arrangement. However, authorities claim that neither foreign trusts nor other types of legal arrangements can be beneficiaries of a life insurance policy.

Timing of Verification

15. **Criterion 10.14** – Pursuant to Art. 8(2) of the AML/CFT Act, FIs are required to verify the identity of the customer and BO before establishing a business relationship or carrying out a transaction. The verification may be completed after establishing the business relations provided that it is necessary to not interrupt the normal conduct of business, ML/TF risks are low, and the verification is finalised without undue delay (Art. 8(3)).

9. Trust or their equivalent are not recognised under Slovak law and c.25.1(a) and (b) were considered not applicable in the 2020 MER.
10. The 2020 MER indicated that only 1% of the total number of bank customers were non-residents, primarily natural persons from neighbouring countries. Updated statistics confirm that the number of foreign bank customers remains low and continues to be mainly natural persons.

16. **Criterion 10.15** – The AML/CFT Act provides for the general requirement for FIs to put in place the relevant measures to manage ML/TF risks (Art. 20(2)(c)) and verification may be completed after the establishment of the business relationship only if the ML/TF risks are low. In case of bank accounts, including accounts that allow transactions in transferrable securities, only crediting operations are allowed before the customer and BO are duly verified.

Existing Customers

17. **Criterion 10.16** – The transitional provisions of the AML/CFT Act (Art. 36(1)) required obliged entities to conduct CDD (according to new national requirements), depending on the risk, in relation to existing customers within a year from when the law entered into force. According to Art.10(2)(g) and (h) obliged entities shall carry out CDD in the course of the business relationship on the basis of risks identified through the institutional risk assessment and when significant changes have occurred with respect to the customer that might affect the risk of ML or FT. However, there are no provisions that would require FIs to apply CDD to existing customers depending on the materiality and, when determining appropriate times, to also take into account whether and when CDD measures have previously been undertaken and the adequacy of the data obtained.

Risk-Based Approach

18. **Criterion 10.17** – Art. 12(1) of the AML/CFT Act requires FIs to apply enhanced CDD measures based on a risk assessment in every case where higher ML/TF risks have been identified. It further stipulates some higher ML/TF situations where the enhanced CDD is mandatory: for example, (i) cross-border correspondent banking relationships, (ii) transactions or business relations with PEPs and (iii) with persons established in high-risk countries as designated by the European Commission, (iv) non-face to face verification of customers. At the same time, this list is non exhaustive and the decision whether or not to conduct enhanced CDD should be based on the initial risk assessment, the criteria of which are broadly described in the annex of the AML/CFT Act. The AML/CFT Act defines the enhanced CDD as the application of additional CDD measures depending on the ML/TF risk.

19. **Criterion 10.18** – Art. 11(1)(2) of the AML/CFT Act provides for the possibility of applying simplified CDD measures in certain low risk scenarios. The FIs are prohibited from performing simplified CDD measures when there is suspicion of an unusual transaction (Art. 11(3)).

Failure to Satisfactorily complete CDD

20. **Criterion 10.19** –

(a) Art. 15 of the AML/CFT Act stipulates that FIs are required to refuse establishing a business relationship or performing a transaction, and to terminate a business relationship if they cannot carry out all the CDD requirements under the AML/CFT Act.

(b) According to Art. 17(1) of the AML/CFT Act, FIs are required to report an unusual business transaction to FIU without undue delay. This reporting obligation extends to all circumstances in which a financial institution is unable to comply with the relevant CDD measures.

CDD and Tipping-off

21. **Criterion 10.20** – Articles 10(9)(a) and (b) of AML/CFT Act allow obliged entities to refrain from conducting customer due diligence (CDD) if doing so in whole or in part could jeopardise the processing of an unusual business transaction (including by tipping off a customer), or if instructed in writing by the FIU. In such cases, according to Art. 17(1), the obliged entity must promptly submit an UTR to the FIU. Furthermore, under Art. 17(4), the obliged entity must specify the reasons for not performing the CDD and indicate which parts of the procedure were not carried out.

Weighting and Conclusion

22. The Slovak Republic has most of the necessary CDD requirements in place. The remaining deficiencies include: no explicit obligation to verify BO information against reliable sources in situations other than those involving a higher ML/TF risk (c.10.5); and for customers that are legal persons or legal arrangements there is still no requirement to obtain the names of all relevant persons holding the senior management position (c.10.9(b)). Other gaps, such as shortcomings in the identification and verification of BOs of legal arrangements (c.10.13), absence of a specific obligation to identify persons having equivalent or similar positions to those in trust (c.10.11(b)) and limited scope of the identification of beneficiaries designated by characteristics or class (c.10.11(a)) are of limited impact given the minimal use of trust and other legal arrangements by foreigners in the context of Slovak Republic. Similarly, absence of provisions that would require FIs to apply CDD to existing customers depending on the materiality (c.10.16) is considered a minor gap. Therefore, **Slovak Republic is re-rated LC with R.10.**

Recommendation 12 – Politically exposed persons

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ LC (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.12 based on the following deficiencies: there is no specific requirement to put in place risk management systems for identifying PEPs (c.12.1(a)); a manager, who has direct communication with the statutory and supervisory boards, and can access all required information and documents, does not seem to be equivalent to senior manager (c.12.1(b)); there is no specific requirement to take reasonable measures to establish the origin of the entire body of wealth of PEPs (c.12.1(c)); the definition of family members however does not include siblings of PEPs, which is part of the minimum standard provided by the FATF Guidance (c.12.3); persons considered as close associates of PEPs are limited to those who have joint beneficial ownership of the FI's customer, run business together with PEPs or have beneficial ownership of the FI's customer set up in favour of a PEP (c.12.3); there is no requirement for the FIs providing life insurance policies to take reasonable measures to determine whether the beneficiaries or the BO are PEPs (c.12.4); other elements of c.12.4 are also not fulfilled, although the senior management must be informed whenever policy proceeds are paid out as part of the business relationship with PEPs (c.12.4). Slovak Republic requested to upgrade R. 12 in the context of the 1st FUR, however no progress was recorded under the FUR.

2. **Criterion 12.1** – The definition of PEPs is provided by Art. 6 of the AML/CFT Act and is in full compliance with the FATF standards.

(a) Art. 10 (1) (d) of the AML/CFT Act requires FIs to ascertain whether the customer or the BO is a PEP as part of CDD measures. Art. 20 (2) (l) of the AML/CFT Act requires the obliged entities to implement a risk management system for the identification of a customer or a customer's BO who is a PEP or sanctioned person.

(b) Art. 12 (2) (c) (1) of the AML/CFT Act requires FIs to obtain the approval from the management board, a designated person, or a person appointed by them before establishing or continuing a business relationship. The designated person must either be a member of the management board of an FI or a manager with sufficient knowledge of the obliged person's exposure to the ML/TF risks, who is authorised to make decisions to mitigate the risks, has direct communication with the statutory and supervisory boards, and can access all required information and documents. While the law does not explicitly refer to "senior management" and the designated person may not, in all cases, hold a formally senior managerial title, the functions and responsibilities described broadly align with the FATF standard.

(c) Art. 12 (2) (c) (2) of the AML/CFT Act requires FIs to establish the source of wealth and source of funds in business relationships and transactions of customers and BOs identified as PEPs.

(d) Art. 12 (2) (c) (3) of the AML/CFT Act requires FIs to apply enhanced on-going monitoring of the business relationship with PEPs.

3. Art. 12 (3) of the AML/CFT Act provides that FIs must continue applying the measures noted above in relation to persons who are no longer entrusted with a prominent public function for at least 12 months and until such time as the person poses no PEP-specific ML/TF risk based on the risk assessment of an FI. This approach is in line with the FATF Guidance on PEPs, which requires handling

of a customer who is no longer entrusted with a prominent public function based on an assessment of ML/TF risks.

4. **Criterion 12.2** – The AML/CFT Act does not distinguish between the domestic and foreign PEPs, and those who are members of the management bodies of the EU institutions and international organisations. Thus, FIs must apply measures noted in c.12.1 to all types of PEPs.

5. **Criterion 12.3** – The definition of family members of PEPs is provided by the Art. 6 (3) of the AML/CFT Act and includes spouses, parents, children and their spouses and those equivalent to spouses. The definition of family members however does not include siblings of PEPs, which is part of the minimum standard provided by the FATF Guidance on PEPs. Persons considered as close associates of PEPs are limited to those who have joint beneficial ownership of the FI's customer, run business together with PEPs or have beneficial ownership of the FI's customer set up in favour of a PEP. This approach is more restrictive than is called for by the FATF Guidance on PEPs.

6. **Criterion 12.4** – FIs providing life insurance policies are required to take reasonable measures to determine whether the beneficiaries, and where required, the BO of the beneficiary, are PEPs, at the time of payment of the benefit (AML/CFT Law, Art. 10(8)(b)(c)). This requirement does not cover beneficiaries that are legal arrangements. However, authorities claim that neither foreign trusts nor other types of legal arrangements can be beneficiaries of a life insurance policy. If higher risks are identified, FIs are required to apply enhanced due diligence and monitoring of the business relationship and to inform the statutory body, designated person or person appointed by them (i.e. the equivalent of senior management under c.12.1(b)) before paying out the proceeds of an insurance contract (AML/CFT Law, Art. 10(8)(d) and Art. 12(2)(c)(3-4)). There is no explicit requirement to consider making an UTR.

Weighting and Conclusion

7. Slovak Republic implements most of the requirements under R.12, and only minor deficiencies remain. Definitions of family members and close associates of PEPs are restrictive (c.12.3), there is no requirement for the FIs providing life insurance policies to take reasonable measures to determine whether the beneficiaries or the BO of legal arrangements are PEPs (c.12.4) and FIs are not required to consider filling an UTR with the FIU in case of beneficiary or BO of the beneficiary identified as PEP (c.12.4). **The Slovak Republic is re-rated LC with R.12**.

Recommendation 13 – Correspondent banking

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ C (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.13 based on the following deficiencies: the correspondent banking requirements do not apply to EU/EEA countries (c.13.1); there is no requirement to determine if the respondent has been subject to a ML/FT investigation or regulatory action (c13.1(a)); FI's do not clearly understand the respective AML/CFT responsibilities of each institution (c.13.1(d)); with regard to payable-through accounts, this requirement applies to only non-EU/EEA countries (c.13.2). Slovak Republic requested to upgrade R. 13 in the context of the 1st FUR, however no progress was recorded under the FUR.

2. **Criterion 13.1** – The correspondent relationship is defined by the AML/CFT Act (Art. 9(k)). Prior to establishing a cross-border correspondent relationship (with FIs within and outside EU/EEA area), FIs are required to:

(a) Gather information about the respondent institution to fully understand the nature of its business and assess the risk factors (Art. 12 (2)(b)(1) of the AML/CFT Act. Art. 12 (2) (b) (2) requires FIs to collect information from publicly available sources to determine respondent institution's reputation and the quality of supervision, and whether the respondent institution has been a subject to any investigation or regulatory proceedings related to ML/FT.

(b) Assess the respondent institution's AML/CFT controls (Art. 12 (2)(b)(2), the AML/CFT Act).

(c) Obtain the senior management (statutory body or the designated manager with sufficient knowledge of the ML/TF risks, authorised to take risk-mitigation decisions, in direct communication with the statutory body and with access to the information and documents obtained from the obliged person during performing CDD) approval for establishing a new correspondent relationship (Art. 12(2)(b)(3), the AML/CFT Act);

(d) Art. 12(2)(b)(5) require defining and recording the AML/CFT obligations and responsibilities related to the correspondent relationship in order to clearly understand the respective roles and responsibilities of each institution in the given area.

3. **Criterion 13.2** – Art. 12(2)(b)(6) of the AML/CFT Act requires FIs, with regard to payable-through accounts, to ensure that the respondent institution performed CDD obligations in relation to the customer that has direct access to the correspondent account, is able to provide relevant CDD information upon request, and ensures the transmission of information on the payer and the payee in cash transfers.

4. **Criterion 13.3** – Art. 24 of the AML/CFT Act stipulates that FIs must not enter into or continue a correspondent relationship with a shell bank or a bank that is known to have entered into a correspondent relationship with a shell bank.

Weighting and Conclusion

5. All criteria are met. **The Slovak Republic is re-rated C with R.13**.

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	2020	LC
FUR1	2022	PC (upgrade requested)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (upgrade requested, maintained at PC)
FUR 4	2025	↑ LC (upgrade requested)

1. In the 5th round MER, Slovak Republic was rated LC with the R.15, as there was no requirement for FIs to conduct risk assessment prior to the launch or use of new business practices and the new or developing technologies.

2. Given the significant revision to R.15, Slovak Republic was reassessed against the requirements in relation to VASPs, in result of which the rating was downgraded to PC in the 1st FUR adopted in November 2022. The following deficiencies were identified: (i) no explicit requirement for risk management and mitigations in relation to VASPs; (ii) risk-based approach applicable only to entities which have VA/VASPs client in their portfolios; (iii) not all activities provided under FATF definition of VASPs are covered; (iv) the legislation is not clear on the licensing and registration requirements concerning VASPs; (v) no information was provided on the communication mechanisms, reporting obligations and monitoring with respect to Targeted Financial Sanctions (TFS); (vi) lack of market entry requirements in relation to VASPs; (vii) no systemic measures to identify natural or legal persons that carry out VASP activities without the required registration; (viii) no risk-based supervision of VASPs carried out by the FIU; (ix) deficiencies in the VASP risk assessment negatively impact the risk-based supervision; (x) absence of the information regarding the legal processes for withdrawing, restricting or suspending the license for AML/CFT violations; (x) sanctions applicable to VASPs for violations of TFS obligations are not proportionate and dissuasive; (xi) no measures to impose to the directors and senior management of VASPs; no information was provided on how the country ensures travel rule requirements for Virtual Assets (VA) transfers.

3. In March 2024, the FIU has concluded the VA/VASP sectorial risk assessment and analysed to some extent the risks of VASPs operating in Slovak Republic.

4. **Criterion 15.1** – Art. 26a of the AML/CFT Act requires the FIU to assess national ML/TF risks and to take into account a number of risk factors provided in Annex No. 2, which include new products, business practices and delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Similarly, Art. 20a of the Law requires financial institutions (FIs) to assess their business-specific ML/TF risks taking into account at least the very same risk factors. Art. 14(2)(b) further stipulates that FIs must pay special attention to ML/TF risks related to new technologies that favour anonymity.

5. **Criterion 15.2** –

(a) Art. 20 (1) of the AML/CFT Act (as amended by the Act No. 387/2024 Coll.) requires FIs to update their AML/CFT programmes before starting the provision of new products that increase their ML/TF risk exposure. This covers new products, new business practices, new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

(b) Art. 20a(2) of the AML/CFT Act requires FIs to implement measures to manage and mitigate risks identified through their risk assessments, taking into account the results of NRA. Art. 14(2)(b) requires measures to prevent misuse of new technologies favouring anonymity. Art. 8(1)(a) allows non-face to face verification if the technology provides reliability equivalent to physical

presence. Articles 20a(4) and (5) add specific obligations for crypto asset service providers (CASPs) regarding self-hosted addresses.

6. **Criterion 15.3** –

(a) At the EU level, the European Commission conducts and publishes an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Art. 6) that also identifies and assesses the risks emerging from virtual assets and the activities and operations from VASPs. The EU level risk assessment shall be updated by a report at least every two years.

The country has taken actions to identify and assess ML/TF risks. The FIU concluded a VA/VASP sectorial analysis in March 2024. However, only some aspects were covered, and analysis is done to some extent on the risk of VASPs operating in the jurisdiction. The risk assessment is merely based on the questionnaires received from VASPs registered in the Slovak Republic, the information received from banks, payment services and electronic money sector considering VASPs as a customer and other information from National Expert Group on Anti-Money Laundering and its members. The country has taken extensive steps in terms of identifying and assessing risks, but it should be noted that the core analysis is based on limited data, gathered from the registered VASP representatives. The assessment of the relevant part of the VASP sector is constrained due to issues with lack of supervision, statistical data availability and complexity. The Slovak Republic completed the process of the 3rd NRA update,-and it will be approved in September 2025.[11]

(b) Please also refer to c.15.3(a) as this criterion is affected by the incomplete understanding of ML/TF/PF risk of VASPs. The National Bank of Slovakia (NBS) strengthened its risk-based supervisory capabilities by implementing a specialised reporting framework requiring each authorised CASP to submit periodic regulatory returns covering standard prudential and crypto-specific data points such as categories and types of virtual assets offered and number and type of hosted wallets. In addition, the competent authority uses advanced blockchain analytics to map wallet addresses and trace transaction flows. By cross-referencing this information with regulatory returns, the NBS applies continuous, data-driven off-site monitoring and timely risk profiling of individual providers, closing previous gaps in regulation, licensing and ongoing supervision. These measures take into account the findings of the 2nd NRA and relevant supranational risk assessments in line with Art. 7 of Directive (EU) 2015/849, as required by Art. 26a of the AML/CFT Act.

(c) The definition of CASPs (as per the definition found in Regulation (EU) 2023/1114 on markets in crypto-assets (MiCAR)) is largely aligned to the FATF definition of a VASP. CASPs are considered FIs, which are obliged persons under the AML/CFT Act (Art. 5(b)(15), and are subject to all provisions of the Act, including the identification, assessment (Art. 20a(4), management and mitigation (20a(5)) of the ML/TF risks associated with their activities (Art. 20a), and the implementation of internal control procedures to pursuant to Art. 20. Regarding c.1.11 Slovak Republic has not taken any actions to remedy the identified deficiency.

11. The updated 3rd NRA has not been considered in the analysis of this follow-up report, as it was approved after the date on which Slovak Republic submitted its country reporting template.

7. **Criterion 15.4** –

(a) A person providing crypto[12] asset services within the EU is subject to prior authorisation (EU Regulation 1114/2023, Art. 59) by the authority of the member state where it has its registered office. A crypto asset service provider under EU law should be a legal person or other undertaking if the legal form of that undertaking ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if it is subject to equivalent prudential supervision appropriate to their legal form (Art. 59 (3)). These requirements to the legal form of undertakings exclude natural persons from being authorised as crypto asset service providers (c.15.4 (a) (ii) is not applicable).

EU law also subjects some types of offerors to authorisation requirements and differentiates offerors according to the specific assets: A person that issues virtual assets qualifying as asset-referenced tokens (EU terminology for a type of stable-coins) has to be authorised as well (EU Regulation 2023/1114, Art. 16). E-money tokens may only be issued by authorised credit institutions or e-money institutions (EU Regulation 2023/1114, Art. 48). Financial services related to an issuer's offer and/or sale of a virtual asset are covered in the crypto-assets services list under Art. 3 (1)(16) EU Regulation 2023/1114, in line with the provisions of the FATF glossary and the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[13] for limb (v) of the VASP definition in the FATF glossary.

Authorisation processes for service providers and offerors include a fit and proper assessment and authorisations shall only be granted if members of the management bodies and shareholders or members are of sufficiently good repute (Art. 21 (2), 63 (10) EU Regulation 2023/1114.

Slovak Republic has identified the NBS as the national authority responsible to authorise CASPs under EU Regulation 2023/1114. The NBS is also authorised to grant authorisation to issuers of asset-referenced tokens. Act No. 248/2024 Coll. on certain obligations and authorisations in the field of crypto-assets and on amendments and supplements to certain acts (effective from 30 December 2024) contains certain provisions that are necessary to harmonise the Slovak legal order with EU Regulation 2023/1114. All activities that fall within the scope of MiCAR are now covered under Act. No. 248/2024 Coll.

(b) The authorisation process under EU Regulation 2023/1114 includes assessments that members of the management body are sufficiently reputable and competent and that shareholders or members that have a qualifying holding fulfil fit and proper requirements (Art. 62, 63, 64 and 68 for crypto asset service providers). These provisions empower authorities to prevent individuals convicted of offences relating to money laundering or terrorist financing or of any other offences that affect their good repute from assuming relevant functions. Regarding shareholders and members whether direct or indirect, that have qualifying holdings, proof is required that those persons are of sufficiently good repute (Art. 62 (2) (h)).

The NBS has the legal authority to undertake fit and proper tests in line with EU Regulation 2023/1114 (Act 248 2024, Section 7). Under the Slovak MiCAR-licensing procedure, a "member of the management body" applies to anyone sitting on the statutory board or body (board, managing director, administrative board or executive director). Members of the management body and supervisory board must pass a fit-and-proper test covering competence, integrity, time commitment and conflicts of interest. The same assessment applies to every director or indirect

12. In the terminology of the EU Regulation 1114/2023 on markets in crypto-assets 'virtual asset' and 'virtual asset service provider' as per the FATF Glossary are defined as 'crypto asset' and 'crypto asset service providers' respectively. Here, both terms are used depending on the framework referred to.
13. Available at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.

shareholder, including ultimate beneficial owners, who holds a qualifying holding (at least 10% of capital or voting rights) or otherwise exercises significant influence. Owners below that threshold are identified for AML purposes but are not subject to the full test. Accordingly, market-entry requirements now attach both to managers who control the CASP and to any owners or beneficial owners whose stake gives them material influence.

8. **Criterion 15.5** – Regulation at EU level prohibits the provision of services without authorisation (Art. 59 (1) EU Regulation 2023/1114). EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure action is taken to identify persons that carry out VASP activities without licensing or registration and to ensure compliance with authorisation requirements by taking supervisory measures and applying sanctions. EU Regulation 2023/1114, Art. 94 (1) (h) stipulates that competent authorities, in accordance with national law, shall have the power to order the immediate cessation of the activity where there is a reason to assume that a person is providing crypto-asset services without authorisation. The prerequisite of "reason to assume" the provision of service leaves sufficient room to take targeted action at service providers that address the market. At the EU level, the European Securities and Markets Authority assist efforts to ensure compliance by keeping a register of operators found to have provided services in breach of the authorisation requirement (Art. 110 EU Regulation 2023/1114).

9. The authorities have indicated that the NBS has a system in place to identify natural or legal persons conducting CASP activities without authorisation. It employs market-intelligence sweeps, consumer complaint monitoring, and blockchain analytics to proactively identify providers operating without proper authorisation. A graduated response mechanism has been established against operators that lack a trade licence, including cease-and-desist notices, public warnings, and technical measures such as website blocking co-ordinated with the National Cyber Security Authority. Priority cases are referred to law enforcement and relevant foreign NCAs where appropriate (Section 8, Paragraph 1 of Act No. 248/2024 Coll). However, the relevant powers rely on national transposition of MiCAR. During the transition period (30 December 2024 – 30 December 2025) VASPs that have relevant trade licenses may continue to provide their activities without a CASP license. On 30 December 2025, the trade licences for the provision of virtual currency exchange services and virtual currency wallet services will automatically expire. VASPs that fail to obtain authorisation as CASPs by 30 December 2025 and nevertheless continue to carry out crypto-asset services in Slovak Republic will be sanctioned by the NBS after this date.

10. **Criterion 15.6** –

(a) When assessed for market entry, CASPs are required to have mechanisms and controls in place that ensure compliance with AML/CFT requirements (EU Regulation 2023/1114, Art. 63 (2) to (10)). CASPs, as obliged entities, are subject to the AML/CFT requirements (Section 5(1)(b) (15)). The FIU is in charge of monitoring for compliance with AML/CFT requirements. CASPs are also subject to authorisation by the NBS pursuant to Section 7(2) of Act No. 248/2024 Coll., in conjunction with MiCAR. The VA/VASP sectorial risk assessment conducted by FIU in March 2024 is of limited usefulness due to issues with lack of supervision, statistical data availability and complexity. Regarding risk-based supervision, the considerations under R.26 apply, i.e. FIU does not have any ML/TF risk-based procedures that determine the frequency and intensity of onsite inspections, nor a procedure for reviewing the ML/TF risk profile of a financial institution. Moreover, deficiencies in the VASP risk assessment negatively impact the risk-based supervision.

(b) EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure compliance by CASPs with requirements to combat ML/TF. EU Regulation 2023/1114, Art. 94, stipulates that competent authorities in accordance with national law shall have the power to inspect and to compel documents. The withdrawal of the authorisation of

CASPs is regulated at EU level in Art. 64 of EU Regulation 2023/1114 and, alongside other administrative penalties and administrative measures, shall also be implemented at national level (EU Regulation 2023/1114, Art. 111). The FIU has the necessary powers to ensure compliance by CASPs with AML/CFT requirements (Art. 29(1), (9), 26(2)(c), (e), 30, 33a, 33(1), (6) of the AML/CFT Act) such as the power to compel documents, conduct risk-based inspections, order the delay/suspension of unusual transactions, and impose fines. Art. 8 of Act No. 248/2024 Coll. empowers the NBS to impose remedial measures and sanctions in accordance with EU Regulation 2023/1114. The NBS also has the supervisory powers as set out in Act No. 747/2004 Coll. on Supervision over the Financial Market and on Amendments and Supplements to Certain Acts, as amended.

The deficiency identified under R.27 equally applies to CASPs, i.e., absence of the information regarding the legal processes for withdrawing, restricting or suspending the license for AML/CFT violations.

11. **Criterion 15.7** – After amendment by EU Regulation 2023/1113 EU Directive 2015/849 (Art. 18) mandates the European Banking Authority to issue guidelines on risk variables and risk factors to be taken into account by crypto-asset service providers when entering into business relationships or carrying out transactions in crypto-assets. (Guidelines published on 16 January 2024 and to be applied from issued from 30 December 2024).

12. At the national level, the FIU has published a guidance document (last updated in April 2024) for VASPs and a guideline on the fulfilment of obligations under Act No. 297/2008 Coll. for legal and natural entities providing virtual currency wallet services and virtual currency exchange offices. On 9 April 2024, the NBS also organised a workshop for prospective CASP applicants on licensing requirements related to AML and IT security. Apart from these documents no other feedback has been provided by the authorities to VASPs to help them implement national measures against ML/TF. AML Act Section 26(2)(i) obliges FIU to provide feedback to the obliged persons in relation to the quality of submitted report (UTR). Nevertheless, the provision is of a general nature and refers to the procedure that the FIU shall adopt after the receipt of UTRs rather than a form of specific feedback on the quality of the UTRs and the manner in which they have been used by the FIU (see R.34).

13. **Criterion 15.8** –

(a) At the EU level, EU Directive 2015/849 and EU Regulation 2023/1114 require member states to provide competent authorities, in accordance with national law, with the power to apply appropriate administrative penalties and other administrative measures. Art. 111 of EU Regulation 2023/1114 stipulates sanctions for a number of infringements including minimum fines. In addition, Member states are obliged to ensure that where obligations apply to legal persons in the event of a breach, sanctions and measures can be applied to the members of the management body and to other natural persons responsible for the breach (Art. 58 (3) of EU Directive 2015/849). Some of the administrative penalties regulated under EU Regulation 2023/1114, Art. 111, shall also apply to members of the management body of a crypto-asset service provider.

At the national level, the analysis under c.35.1 applies here. The FIU is authorised to impose a fine on CASPs, as an obliged entity, pursuant to Art. 33(2) of the AML/CFT Act of up to EUR 5 000 000 or up to 10% of the total annual turnover, in the event that it fails to fulfil the obligations set forth in Art. 33(1) of the AML/CFT Act (CDD, EDD, assessment of transactions, delay of an unusual business transaction, failure to terminate a business relationship, failure to report an unusual business transaction to the FIU, failure to retain data, failure to provide co-operation to the FIU). In the event of other violations of the provisions of the AML/CFT Act, the

FIU is authorised to impose a fine on CASPs of up to EUR 200 000 (AML/CFT Act, Art. 33(3)). For breaches of targeted financial sanctions, enforcement follows Act No. 289/2016 Coll. in line with EU/UN regimes, and sanctions may also apply to members of the management body and other responsible natural persons pursuant to Art. 58(3) of Directive (EU) 2015/849. Sanctions applicable to VASPs for violations of terrorism and TF related TFS are not proportionate and dissuasive.

Art. 8 of Act No. 248/2024 Coll. empowers the NBS to impose sanctions in accordance with EU Regulation 2023/1114. This power directly extends to AML/CFT breaches through Art. 68(8) of EU Regulation 2023/1114.

(b) At EU level, member states are obliged to ensure that where obligations apply to legal persons in the event of a breach, sanctions and measures can be applied to the members of the management body and to other natural persons responsible for the breach (Art. 58 (3) of EU Directive 2015/849). Some of the administrative penalties regulated under EU Regulation 2023/1114, Art. 111, shall also apply to members of the management body of a CASP.

At the national level, the analysis under c.35.2 applies here. The previously identified deficiency relating to the lack of measures to impose sanctions on directors and senior management of VASPs has been addressed by an amendment to the AML Act, effective from 15 January 2025. Pursuant to Art. 33 (4) of the AML/CFT Act, the FIU may impose on a member of the statutory body, supervisory body, management body or procuration holder of an obliged entity, including CASPs, a fine of up to 10 times the monthly average of their total income for the preceding 12 months from the obliged entity for failure to comply with or breach of any obligations under the Act.

14. **Criterion 15.9** – CASPs are obliged persons under the AML/CFT Law and bound by the AML obligations mirroring the requirements set out in R.10-R.21. For occasional customers, VASPs are obliged to keep all the data and written documents obtained through CDD measures and related to the transaction for 5 years after the execution of an occasional trade (AML/CFT Act, Art.19(2)). The record-keeping requirements cover risk profile assessment records, including supporting analysis, business correspondence, results of any analysis undertaken, records of all actions taken and related obstacles (AML/CFT Act, Art. 19(2)(c), in relation to c.11.2). Other minor deficiencies identified under R.10-21 equally apply to VASPs.

(a) Covered VASPs are obliged to only identify and verify the customer identity when an occasional transfer of crypto assets that amounts to or exceeds 1 000 Euros. (Art. 10(2)(j) AML/CFT Act).

(b) (i)EU Regulation 2023/1113 repeals and replaces EU Regulation 2015/847 formerly regulating the transfer of funds and extends the scope to cover both transfer of funds and transfer of virtual assets. Art. 14 (1) of EU Regulation 2023/1113 requires the originating crypto asset service provider to obtain and hold originator information (Art. 14 (1), (2) and (3)) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Art. 14 (4)). Before transferring crypto-assets, the service provider shall verify the accuracy (Art. 14 (6). In accordance with Art. 24 of EU Regulation 2023/1113, information has to be provided to competent authorities in the Member State in which they are established. The originating crypto asset service provider submits beneficiary information to the beneficiary's service provider in line with Art. 14 (2) of Regulation 2023/1113 and holds it on record according to Art. 26 (1) Regulation 2023/1113.

The distributed ledger address (DLT) information is required for both the originator and the beneficiary. If the transfer does not occur on the DLT, the Regulation requires the crypto-asset account number instead (EU Regulation 2023/1113, Art. 14 (1) (b) and (2) (b)).

EU Regulation 2023/1113 imposes additional requirements to be implemented in the case of transfers being made to self-hosted addresses (where no crypto asset service provider is involved on the originator or beneficiary side), such as individual identification of transfers and ensuring that the address is controlled by the originator/beneficiary.

EU Regulation 2023/1113 does not make a distinction between crypto-asset transfers within and outside the EU, treating all crypto-asset transfers as cross-border.

(ii) Art. 16 of EU Regulation 2023/1113 requires the crypto asset service provider of the beneficiary to implement effective procedures, which may include post-event or real-time monitoring, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (EU Regulation 2023/1113, Art. 16 (1) and (3)). Service providers are obliged to make information available to competent authorities on request according to Art. 24 of EU Regulation 2023/1113.

(iii) EU Regulation 2023/1113 covers the requirements of Recommendation 16 and applies them to virtual asset transfers, especially on monitoring and risk-based procedures (Art. 14 (8) and Art. 16 (1)) as well as freezing action and prohibiting transactions with designated persons and entities (Art. 23).

(iv) FIs are covered by the scope of relevant provision of EU Regulation 2023/1113 through the broad definition of crypto asset service provider in Art. 3 (1) 15 of that Regulation with reference to Art. 3 (1) (15) EU Regulation 2023/1114, including credit institutions that provide crypto asset services in accordance with Art. 59, 60 of EU Regulation 2023/1114.

15. **Criterion 15.10** – TF/PF TFS obligations apply to covered VASPs in the same manner as they apply to other obliged persons (Art. 4(2)(b) ISA, Act 289/2016). The respective communication mechanisms and reporting obligations are provided under International Sanctions Act (ISA, Act 289/2016). Please refer to analysis of criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) as they apply to CASPs.

16. **Criterion 15.11** – EU Regulation 2023/1114, Art. 107, expressly provides that competent authorities should, where necessary, conclude co-operation arrangements with supervisory authorities of third countries concerning the exchange of information with those supervisory authorities of third countries and the enforcement of obligations under this Regulation in those third countries.

17. The Slovak Republic was assessed as compliant with R.37 and largely compliant with R.38-R.40. Consequently, international co-operation and exchange of information can occur with a view to covered VASPs in the extent allowed by the deficiencies identified under R.38 to R.40 in the 2020 MER.

Weighting and Conclusion

18. The Slovak Republic has taken some steps to address and deficiencies under R.15 identified in the 5th round MER. Slovak Republic has undertaken substantial legislative reforms, including amendments to the AML/CFT Act to extend AML/CFT obligations to all VASPs and the transposition of MiCAR and TFR requirements. Notwithstanding these improvements, a number of minor shortcomings remain. In the case of the risk assessment of VASPs and VAs, the risk assessment process relies heavily on self-reported and incomplete data, and lacks sufficient statistical coverage (c.15.3). This affects the ability to take a risk-based approach with regard to supervision (c.15.3 and c.15.6). Concerns also remain as to sanctions for unauthorised VASPs during the transition period (c.15.5) and sanctions imposed for breaches of AML/CFT obligations (c.15.8(a))). Other minor deficiencies include identified deficiencies under R.10-21 that equally apply to VASPs. (c.15.9(a)), no direct reference in the legislation to "monitor" the compliance of VASPs with R.7. (c.15.10), and deficiencies identified under R.38 to R.40 (c.15.11). **R15 is re-rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	PC (upgrade requested, maintained at PC)

1. In its 5th round MER, Slovak Republic was rated PC with R.18 based on the following deficiencies: absence of the obligation for the FIs to take into account the size of the business when designing AML/CFT programmes (c.18.1); there are no requirements that the compliance officer should be at management level (c.18.1(a)); legal provision requiring FIs to screen their employees to ensure high standards when hiring does not exist (c.18.1(b)); there is no specific requirement to put in place an independent audit function for the purpose of testing the AML/CFT system (c.18.1(d)); the requirement to implement group-wide AML/CFT programmes does not extend to branches and subsidiaries in EU member states (c.18.2); the requirement to include procedures for information sharing within the group-wide AML/CFT programme does not extend to branches and subsidiaries in EU member states (c.18.2(a)); There is no specific requirement that the group-wide AML/CFT programs provide for the collection of the relevant customer, account and transaction data at the group-level functions, or the dissemination of those data to members of the group for risk management purposes (c.18.2(b)); limited requirement to include adequate safeguards on confidentiality and prevention of tipping-off in the group-wide AML/CFT programmes (c.18.2(c)); requirements to the FIs' branches and majority-owned subsidiaries in third countries to take AML/CFT measures in line with the domestic and EU legislation do not extend to those who are placed in the EU member states (c.18.3). Slovak Republic requested to upgrade R. 18 in the context of the 1st FUR, however no sufficient progress has been made and the rating remained.

2. **Criterion 18.1** – The AML/CFT Act requires FIs to put in place AML/CFT programs (Art. 20 (1)) taking into consideration its own organisational structure, the size and activity and must be approved by the FI's statutory body (Art. 20a(2)).

(a) Art. 20(2)(h) of the AML/CFT Act requires the designation of the FI's statutory body or its member or a manager in direct communication with the statutory and supervisory bodies, who has sufficient knowledge of the obliged entity's exposure to risk of ML/TF and is authorised to make decisions to mitigate the risks, to be in charge of AML/CFT compliance. The AML/CFT compliance officer/body should be holder of managerial office and should have access to all required CDD information and documents.

(b) Art. 20(2)(k) of the AML/CFT Act requires FIs to implement methods for verifying and ensuring high standards of integrity when onboarding employees and non-employed individuals who perform activities for FI and directly carry out duties under the Act.

(c) The AML/CFT Act requires FIs to ensure professional training of employees in the AML/CFT programme (Art. 20(3)) and the identification of unusual transactions (Art. 20(3)). Such trainings must be held annually and also before assigning a new employee to the job.

(d) Art. 20(2)(k) of the AML/CFT Act requires FIs to monitor compliance with the action programme and the obligations arising from the Act, to review the effectiveness of the strategies and procedures and, when so justified by entity's size and nature, to establish an independent internal audit or internal control unit, directly reporting to the statutory body.

3. **Criterion 18.2** – The AML/CFT Act requires FIs to apply group-wide AML/CFT programs to their branches and majority-owned subsidiaries in third countries (including within the EU/EEA and

outside) (Art. 20a(3)). There are no similar provisions regulating financial groups established in Slovak Republic.

(a) The group-wide AML/CFT programs must include procedures for information-sharing within the group under the AML/CFT Act (Art. 20a(3)).

(b) Art. 20a(3) requires obliged entities which have foreign branches and subsidiaries to apply group anti-money laundering and counterterrorism financing strategies, including procedures for intra-group sharing of customer, account and transaction information and for the protection of personal data and the confidentiality of such exchanged information to the extent allowed by that country's laws. The term intra-group sharing does not specifically cover provision of data between selected group-level functions (compliance, audit, and/or AML/CFT function) and it is not clear that the dissemination of those data to members of the group is required for risk management purposes. Obliged entity is required to share information on the reported attempted or unusual transaction within a group (AML/CFT Law, Art. 18(10).

(c) The group-wide AML/CFT programs must include procedures for the protection of personal data and the confidentiality of exchanged information, to the extent allowed by the host country (AML/CFT Act, Art. 20a(3). There is no specific requirement to include adequate safeguards on prevention of tipping-off in the group-wide AML/CFT programs.

4. **Criterion 18.3** – Art. 21(4) of the AML/CFT Act requires obliged entities with branches, units, or subsidiaries in other jurisdictions (including within the EU) to ensure compliance with host country AML/CFT laws, provided that customer due diligence and data retention requirements, as set out in Articles 10–12 and 19 of the AML/CFT Act, are compliant with the EU law. This obligation is limited in scope, covering as minimum only selected AML/CFT requirements. Moreover, the law does not explicitly require the application of home country AML/CFT measures where host country requirements are less strict, to the extent permitted by host country laws and regulations. If the host jurisdiction's laws prevent implementation of such limited measures, the obliged entity must notify the FIU and apply additional measures. If these are insufficient, the FIU or National Bank of Slovakia may impose supervisory actions, including terminating business relationships or operations in that jurisdiction. All legal obstacles, including those related to intra-group information sharing and data protection, must be considered when assessing the host jurisdiction's legislation.

Weighting and Conclusion

5. The implementation of group-wide AML/CFT programs is required for foreign branches and majority-owned subsidiaries only (c.18.2). The term intra-group sharing does not specifically cover provision of data between selected group-level functions (compliance, audit, and/or AML/CFT function) and it is not clear that the dissemination of those data to members of the group is required for risk management purposes (c.18.2(a) and (b)). FIs are not required to apply home country's AML/CFT measures where the AML/CFT requirements of the host country are less strict which is a moderate deficiency (c.18.3). There are also deficiencies concerning the procedures for information-exchange in the group-wide AML/CFT programs, including lack of adequate safeguards on prevention of tipping-off (c.18.2(c)). **The Slovak Republic remains rated PC with R.18**.

Recommendation 19 – Higher-risk countries

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (upgrade requested, maintained at PC)
FUR 4	2025	↑ C (upgrade requested)

1. In the 5th round MER, Slovak Republic was rated as PC with R.19. There were moderate shortcomings identified, including (i) applicability of enhanced Customer Due Diligence (CDD) measures limited only to high-risk countries that are not part of the European Economic Area (EEA) area; (ii) no authorisation for competent authorities to apply countermeasures either independently or when called for by the FATF; (iii) only European Commission decisions identifying high-risk countries published by the FIU.

2. Slovak Republic requested to upgrade R. 19 in the context of the 1st FUR, however no sufficient progress has been made, and the rating remained.

3. **Criterion 19.1** – FIs are obliged to perform enhanced CDD to a transaction or business relationship with the person established in a high-risk jurisdiction, defined as a country with strategic deficiencies as identified by the EU, an intergovernmental institution or an international organisation that establishes, monitors compliance with, internationally recognised standards for the prevention of money laundering and the financing of terrorism (AML/CFT Act, Art. 9(o) and Art. 12(1)). Art. 9 (p) of the AML/CFT Act defines a "person established in a high-risk country" as: (i) a natural person who is a national of, or resides (permanently or otherwise) in a high-risk country; (ii) a natural person acting as an entrepreneur with a place of business in such a country; or (iii) a legal entity with its registered office, branch, organisational unit, or place of business located in a high-risk country.

4. **Criterion 19.2** – Art. 12(2)(d) requires obliged entities, when dealing with a person established in a high-risk country, to apply enhanced due diligence measures, including obtaining additional information about the customer, beneficial owner, and the purpose of the relationship, verifying the origin of funds and property, gathering data from credible sources, obtaining approval from senior management, and conducting ongoing detailed monitoring of the business relationship. The countermeasures that can be applied by Slovak Republic independently or when called by the FATF according to AML/CFT Act include: (i) application of enhanced supervisory measures for subsidiaries or branches in countries with inadequate AML/CFT systems (Art. 21(4)), (ii) ban on the establishment or termination of operations of subsidiaries, branches, organisational units in such jurisdictions (Art. 21(4)), (iii) prohibition on FIs to rely on CDD conducted by third parties operating in high risk countries (Art. 13(4)), (iv) obligation to review, change or, if necessary, terminate correspondent banking relationship with a partner institution established in high-risk country (Art. 24(4)).

5. **Criterion 19.3** – According to Art. 26(2)(o) of AML/CFT Act, FIU is publishing on its website, in addition to the decisions taken by the European Commission that identify high-risk jurisdictions with strategic deficiencies, a list of high-risk countries identified by FATF.

Weighting and Conclusion

6. All criteria are met. **R.19 is re-rated as C.**

Recommendation 23 – DNFBPs: Other measures

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ LC (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.23 based on the following deficiencies: TCSPs are not required to report suspicious transactions when performing the equivalent function of a trustee for other forms of legal arrangement (c.23.1(c)); shortcomings identified under R.18, 19 and 21 equally apply to DNFBPs (c.23.2, c.23.3, c.23.4). Slovak Republic requested to upgrade R.23 in the context of the 1st FUR, however no sufficient progress has been made and the rating remained.

2. **Criterion 23.1** – DNBFPs, including lawyers, notaries, accountants, auditors, tax advisors, dealers in precious metals or stones, and TCSPs are required to report unusual transactions based on Art. 17 of the AML/CFT Act.

(a) Lawyers and notaries are considered obliged entities when they provide services related to transactions described in c.22.1(d) and thus, are also required to report unusual transactions. Under Articles 22 and 23 of the AML/CFT Act, lawyers, notaries, accountants, auditors and tax advisors are exempted from the reporting requirement where the professional secrecy or legal professional privilege apply. The matters that fall under the professional secrecy or legal professional privilege broadly correspond to FATF standards;

(b) Dealers in precious metals or stones are required to report unusual transactions under Art. 14 of the AML/CFT Act;

(c) According to Art. 9(b) of the AML/CFT Act, the AML/CFT obligations, including the reporting requirements, apply to TCSPs when they provide services related to the activities listed in c. 22.1(e) except for performing the equivalent function of a trustee for other forms of legal arrangement.

3. **Criterion 23.2** – DNFBPs are subject to the same requirements regarding internal controls and foreign branches and subsidiaries as FIs (see R.18).

4. **Criterion 23.3** – DNFBPs are subject to the same requirements regarding higher risk countries as FIs (see R.19).

5. **Criterion 23.4** – DNFBPs are subject to the same requirements regarding tipping off and confidentiality as FIs (see R.21). Art. 35(b) of AML/CFT Act exempts REs and their employees, and any person acting on behalf of the RE under a different contractual arrangement from civil and criminal liability for fulfilling reporting obligations, if they acted bona fide. If lawyers, notaries, accountants, auditors and tax advisors act with a view to preventing the customer from committing an illegal act, it will not be considered as a violation of the tipping-off requirement. Also, for the sole purpose of ML/TF prevention, these DNFBPs may share UTR related information with similar entities under the joint ownership, management or compliance control that operate in other countries with equivalent AML/CFT requirements

Weighting and Conclusion

6. The minor deficiencies identified in relation to FIs under R.18 and 21 are also relevant for DNFBPs. In addition, TCSPs are not required to report suspicious transactions when performing the equivalent function of a trustee for other forms of legal arrangement (c.23.1(c)). **The Slovak Republic is re-rated LC with R.23.**

Recommendation 28 - Regulation and supervision of DNFBPs

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (upgrade requested, maintained at PC)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	PC (upgrade requested, maintained at PC)

1. In the 5th round MER, Slovak Republic was rated as PC with the R.28. The casinos were subject to licensing however the measures did not cover the associates of criminals. The FIU was designated as the AML/CFT supervisor for all the categories of DNFBPs, however there were shortcomings in the sanctioning regime, as well as risk-based supervision. The Slovak Republic had requested to upgrade R.28 in the context of the 1st and 2nd FURs, however there was no sufficient progress to justify the re-rating.

2. **Criterion 28.1** –

(a) Casinos and online casinos are subject to licensing by the Gambling Supervisory Authority.

(b) Pursuant to Art. 48 (4) of the Gambling Act, for obtaining an individual license the applicant must, inter alia, possess integrity ((a) the person who was not sentenced for an economic crime, crime against order public matters or a crime against property; (b) other wilful criminal act.). Integrity must be proved also by legal persons registered in Slovak Republic or in other EU member (using an extract from the Criminal Record or an equivalent document). This applies to natural persons responsible for operating the gambling and natural persons who are members of the statutory body or are the statutory body. It also includes any natural person or legal person belonging to the applicant's group, as well as a natural person who is a member of the statutory body or the statutory body of a legal person belonging to the applicant's group (Gambling Act, Art. 39(2)). The applicant's group is a group of natural persons or legal entities who are in a relationship of control over each other or who are controlled by one natural person or legal entity (Gambling Act, Art. 2(c)). However, other high-level managers are not subject to similar checks. Additionally, a criminal conviction is the only factor that can lead to a licence refusal. There is no provision for the authority to consider other information to prevent accomplices of criminals from being appointed to casino management positions. Lastly, no measure is applied to prevent associates of criminals to hold a managerial function after the licensing period.

(c) The AML/CFT Act designates the FIU as the AML/CFT supervisor for casinos (Art. 29). The FIU has the power to conduct onsite visits and obtain access to any document or electronic systems of the supervised entity (Art. 30). According to Art. 11 of the Law on Gambling Games, the casinos are also supervised by a number of other supervisory bodies such as the Financial Directorate, and the tax and customs services (until 2016 the MoF performed AML/CFT inspections and since 2016 the Tax authorities were in charge of AML/CFT inspections). Pursuant to the Gambling law all the off-site and on-site supervision prerogatives were transferred to the Gambling Regulatory Authority.

3. **Criterion 28.2-28.3** – The FIU is the designated competent authority responsible for monitoring the compliance of all categories of DNFBPs with AML/CFT obligations. As described above, the FIU has adequate powers to conduct onsite inspections and obtain required data.

4. **Criterion 28.4** –

(a) The FIU has adequate powers to monitor compliance of DNFBPs with AML/CFT requirements by conducting onsite inspections and obtaining any required data or documents.

(b) Professional licenses granted by SRBs to auditors, tax advisors, accountants, notaries, lawyers, bailiffs, real estate agents and dealers of precious metals and stones require the absence of criminal record. Additionally, tax advisors and auditors, beneficial owners and members of the statutory body should not be in close business relationship with the person who is not of a good repute and integrity (Act No 78/1992 on Tax Advisors and Slovak Chamber of the Tax Advisors and Act No 423/2015 Coll. on Statutory Audits). However, the examination of the good repute and integrity related conditions for those 2 categories of professionals only refers to the absence of criminal record, which is thereof limited. Consequently, no measures are in place to prevent non-convicted associates of criminals to be professionally accredited or holding (or being a beneficial owner of) a significant or controlling interest or holding a management function in a DNFBP.

(c) The AML/CFT Act provides the FIU with the sanctioning power. Available sanctions include imposing fines up to EUR 1 000 000 (Art. 33), requiring the publication of the legal valid decision/applied sanction (Art. 33a) and requesting the relevant authority to withdraw authorisation/license for serious or consecutive violations (Art. 34). The range of these sanctions appears adequate. The FIU can also impose sanctions on a member of the statutory body of the obliged entity, a member of the supervisory board of the obliged entity, a member of the obliged entity's management body or the obliged entity's holder of the procuration, for failure to comply with, or breach of, any of the AML/CFT (Art. 33(4)). In addition, the SRBs can withdraw the professional licenses granted to auditors, tax advisors, accountants, notaries, lawyers and real estate agents for violating the licensing conditions related to the absence of criminal record. (the gambling law provides sanctioning prerogatives to the gambling authority).

5. **Criterion 28.5** – When planning the frequency and scope of inspections, the supervisory authority, including the Office for Gambling Regulation, shall take into account the risk profile of the obliged entity, the results of the NRA and the risk assessments prepared by the European Union's bodies and other international institutions. The supervisory authority shall update the risk profile of the obliged entity on a regular basis and whenever any significant event or change in the management or operation of the obliged entity occurs (AML/CFT Act, Art. 29(3) and (9)). The Methodological Guideline for the fulfilment of obligations of gambling operators in the field of protection against ML/FT issued by the Office for Gambling Regulation stipulates prescribes risk-based approach per gaming type whereby the obliged entities are required to identify, assess and manage risks specific to them (Methodological Guideline of 15 November 2024, Art. 4). The FIU inspectors are required to understand certain characteristics (size, distribution channels, ownership structure, etc.) and risk factors related to DNFBPs before conducting an inspection (FIU Order No. 297/2008).

Weighting and Conclusion

6. Slovak Republic meets criteria 28.2, 28.3 and 28.5 and partly meets criterion 28.4. There are significant deficiencies remaining: no measures in place to prevent associates of criminals from holding management functions in casinos (c.28.1(b)); absence of the measures to prevent non-convicted associates of criminals to be professionally accredited or holding (or being a beneficial owner of) a significant or controlling interest or holding a management function in other DNFBPs (c.28.4(b)). **R.28 remains as PC.**

Recommendation 29 – Financial intelligence units

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ LC (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.29 based on the following deficiencies: the legislation does not clearly determine the "regulation" setting up the FIU (c.29.1); lack of provision allowing the FIU to "use" the additional information received from the REs (c.29.3(a)); there is no clear legal obligation for the FIU to carry out strategic analyses (c.29.4(b)); wide ranging of dissemination of information creates deficiencies in its protection (c.29.6(a)); no specific legal provision on how the FIU files are handled and stored, and whether this shall be physically distinct from other police units (c.29.6(a)); the Head of the FIU is not able to conclude MOUs independently (c.29.7(b)); the FIU's position and its core-functions definitions are volatile due to repeated changes within the Police structure and the reference made to the FIU in various pieces of legislation is done in an inconsistent manner (c.29.7(c)). R.29 was re-assessed in the 2022 in its 1st FUR but, given that it had only addressed some of the deficiencies, the rating remained PC.

2. **Criterion 29.1** – The Slovak FIU is established through Art. 4(6) of the Act 171/1993 Coll. on Police Force (hereafter the Act on Police) as a specific part of the Financial Police Service of the Police Force, whose responsibility is to carry out tasks in relation to the prevention and detection of money laundering and terrorist financing under special regulation. A legislative reference note specifies that the special regulation is Act No. 297/2008 Coll. (the AML/CFT Act).

3. Art. 26 (2) (a) AML/CFT Act, provides that the FIU fulfils the tasks of a central national unit in the area of preventing and detecting money laundering and terrorist financing. Amongst the powers and responsibilities of the FIU are: receive, analyse, evaluate and process unusual business operations and financial information related to money laundering and terrorist financing, prepare financial analyses, and assign the matter to law enforcement authorities if the facts suggest that a crime has been committed. There are no competences assigned to the FIU related to associate predicate offences. To the latter, the Slovak authorities argued that the competence of the FIU in the environment and conditions of the Slovak Republic cannot be defined only from the point of view of legalisation of proceeds from crime, as FIU employees/police officers are also members of Police Force, who check and detect various criminal activities, especially of economic nature (not only legalisation of proceeds from crime). In the light of the explanations provided by the authorities, corroborated with the findings on the dissemination process (see c.29.5), the AT concludes that the requirement related to the predicate offences is met.

4. **Criterion 29.2** –

(a) As described above the AML/CFT Act (Art. 26(2)(a)) provides that the FIU shall receive, analyse, evaluate and processes reports of unusual business operations and financial information related to money laundering and terrorist financing, filed by the RE. The definition of "financial information" in point (m) of Art. 9 of the AML/CFT Act includes any information or data held by the FIU for the purpose of preventing and detecting ML/FT, such as data on financial assets, movements of funds or business relationships.

(b) Apart from the UTRs, the only threshold reports received by the FIU are customs declarations for cash above EUR 10 000. The transmission of cash declaration data to the FIU is conducted based on Art. 9 of Regulation (EU) 2018/1672. In accordance with this provision, the Financial

Directorate of the Slovak Republic, as the competent authority, centrally ensures the secure and electronic transmission of cash declaration data to the FIU through the "Custom Information System – CIS", a database directly accessible by the FIU, in accordance with Art. 5 of Implementing Regulation 2021/776.

5. **Criterion 29.3** –

(a) Based on the FIU written request and for the purposes of fulfilment of its tasks pursuant to the AML/CFT Act, the obliged person shall provide the FIU with the data on business relationships or transactions, submit documents, and provide information on the persons that took part in the transaction in any way (Art. 21 (1)). The FIU shall provide the time-limit for the completion of the request (which the authorities stated is usually of 7-14 days). This precise period does not follow from any provision of the AML/CFT Act. The FIU can "use" the additional information received from the REs for performance of its tasks, including for carrying out operational and strategic analyses (Art. 26(2)(a) in conjunction with Art. 9, points (m) and (n) of the AML/CFT Act.

(b) According to Art. 76 of the Act on Police, the PF units (which would include the FIU) are entitled to request documents and information from state authorities, municipalities, legal and natural persons when performing their tasks. In practice, the FIU has access to a series of DB such as: Register of investigated cases (DVS), the Commercial Register, the Slovak population register; record of drivers, vehicles; cadastral portal; Register of wanted persons, BO register, Register of public sector partners, Trade register, Register of foundations, non-investment funds and NPO register, Finstat and Register of Financial Statements (see also analysis under IO.6).

6. **Criterion 29.4** –

(a) The FIU is empowered to conduct operational analysis as required by 29.4(a) through Art. 26(2)(a) in conjunction with Art. 9, letter (n) point 1 of the AML/CFT Act. The Order of the Director of the FIU on "The Method of implementation of some provisions of the AML/CFT Act" from 2023 (hereafter The FIU Methodological Order) stipulates the UTR prioritisation mechanism (in three categories depending on the risk) and the steps to be taken in conducting analysis. The analytical process includes further information on the UTRs from REs, search for and identify all transactions, financial flows, natural and legal persons that are relevant for further assessment, ensure other relevant information and evidence through available registers and databases and also open sources, ask foreign FIUs for co-operation, and prepare the analytical report. At the operational level, the FIU uses a number of analytical tools. The analysis is performed by the UTR Department.

b) The FIU is also mandated to perform strategic analysis through Art. 26(2)(a) in conjunction with Art. 9, letter (n) point 2 of the AML/CFT Act. The FIU's Analytical Unit in collaboration with other departments develops strategic analysis on new phenomena of crime, the results of which are published in the FIU's Annual Report.

7. **Criterion 29.5** – The FIU has the ability to disseminate spontaneously and upon request specific information to competent authorities. The spontaneous dissemination provisions are stipulated by four different items in the AML/CFT Act which are not fully clear and overlapping, creating effectiveness issues in practice (see IO.6). The authorities advised that the following distinction between the four items apply:

- According to Art. 26 (2) (b) of the AML/CFT Act, the FIU shall submit information to law enforcement authorities if facts suggest that a crime has been committed. According to the authorities, these concern the cases where the FIU transfers information (matter) to the

departments of the Police Force in the capacity of the authorities acting in criminal proceedings, in the event that the facts established indicate that a crime has been committed.

- According to Art. 26 (2) (l) of the AML/CFT Act, FIU submits information to the Police Force for the purposes of detecting crimes and identifying their perpetrators, co-operating in the detection of tax evasion, illegal financial transactions, money laundering and the financing of terrorism, combating terrorism and organised crime and searching for property pursuant to Council Decision 2007/845/JHA. According to the authorities, these concern the cases where the FIU disseminates information to the departments of the Police Force that require the performance of further verification actions to confirm the fact that a crime has been committed.
- According to Art. 26(2)(j) of the AML/CFT Act, the FIU provides information to the tax administrator and government authorities in the area of taxes, fees and customs if the information is relevant and such provision does not endanger the fulfilment of the tasks of the FIU.
- According to Art. 26(3) of the AML/CFT Act, FIU provides information and documentation it has received under that law to the State authorities which carry out tasks in the field of protection of the constitutional system, internal order and security of the state to the extent necessary for fulfilling their statutory tasks in the fight against terrorism and organised crime. According to the authorities, these cases concern the dissemination of information and documents by the FIU to other authorities, within the meaning of this provision, which are not part of the Police Force. Upon request, the FIU shall also provide information and documents to authorities having jurisdiction over international sanctions for the performance of their duties.

The requirement for the use of dedicated, secure and protected channels for disseminations is covered with explicit obligation for the FIU to apply in its activities such organisational, personnel, technical and other measures in its operation so as to guarantee that no unauthorised person may come into contact with the information obtained through its activities under the AML/CFT Act (Art. 26 (9)). All information obtained from UTR reports and the results of their analysis are collected in the FIU's system goAML. The system provides end-to-end encryption capability and a secure data transfer protocol to recipients of FIU information. Regulation of the Ministry of the Interior of the Slovak Republic No. 159 on the goAML information system from 2024 (hereinafter referred to as "Regulation No. 159) defines the tasks and responsibilities of the manager of the information system, which is the FIU, and defines the conditions relating to access rights, permits and registration of authorised persons.

8. **Criterion 29.6** –

(a) According to Art. 18(4) of AML/CFT Act the obligation of secrecy shall apply to everyone who becomes familiarised with the information obtained based on this Act, while fulfilling the tasks of the FIU, or in connection with them. Art. 18(12) of the AML/CFT Act provides that the authorities who receive the FIU disseminations shall be obliged to keep secret information and documentation provided under Art. 26(3) of the AML/CFT Act.

Regulation No. 159 set out rules governing the security and confidentiality of information processed through goAML system, which serves to record registry records, collect, process, analyse, store and exchange information obtained and arising in the process of fulfilling the tasks of the FIU in accordance with the AML/CFT Act. The Regulation also describes the provision of information protection, backup and data storage. Only registered users - FIU workers with their own login data - can access the goAML system. The procedure of handling information from UTR

reports (their receipt, registration, method of handling and analysing) is regulated by the FIU Methodological Order.[14] However, this procedure is tailored for the previous system (DMS) that was used by the FIU and it is not yet updated to reflect the introduction of goAML in 2025.

The communication with foreign FIUs is via encrypted communication channels Egmont Secure Web (ESW) and FIU-net. Terminals (computers) for both systems are in a separate room that only the staff of the International Co-operation Department can access. Acquired information from ESW and FIU-net encrypted mail is inserted in the goAML system by the designated staff of the International Co-operation Department.

The protection of disseminated information is a matter of some concern, as according to the AML/CFT Act, the dissemination of FIU products is quite wide ranging from *"authorities responsible for constitutional establishment protection, internal order and state security"* to the Police Force. The disseminations to the Police Force are carried out with regard to the substantive and territorial jurisdiction pursuant to Regulation of the Minister of the Interior of the Slovak Republic No. 56/2025 on activities in detecting crimes and on the procedure in criminal proceedings. However, the provision of Art. 26 (3) the AML/CFT Act on FIU's dissemination recipients is rather broad and leave some uncertainty on the scope of competent authorities. This is largely mitigated by the obligation of secrecy that shall apply to everyone who becomes familiarised with the information obtained under the AML/CFT Act, as well as the autonomy of the FIU on taking decisions to disseminate.

(b) The FIU police officers are obliged to maintain confidentiality about the facts they learn in the course of or in connection with the tasks of the Police Force (Art. 80 (1-3)) Act on Police Force. The confidentiality obligation does not apply to the notification of crime or other anti-social activity. The Minister or the President of the Police Force may discharge a person from the confidentiality obligation. There are no security clearance requirements for FIU staff, but this derives indirectly from an internal order issued by the FIU Head in August 2019 corroborated with the provisions of the Act No. 215/2014 Coll. on the protection of classified/confidential information. Pursuant to the Order of FIU 4/2019 on the list of functions for which authorised persons may access classified information, there are 36 management and execution level positions that can have access to "Confidential" information. The Act on protection of classified/confidential information foresees the obligation of each statutory body handling confidential information to request the National Security Bureau to carry out Levels II through IV security clearance of those nominated as persons authorised to be provided with access to classified information at the Confidential.

(c) There is limited and protected access to FIU facilities and information, including IT systems. Contactless cards are assigned to specific personal number of the FIU employees. Entrance areas are monitored, and the FIU servers are cut-off from external networks.

9. **Criterion 29.7** –

(a) The FIU is now under the direct supervision of the President of the Police Force. The FIU has increased its level of independence by having its own budget item in the overall Police Force budget and the FIU Director acquired the power to employ staff on its own decision. The Director of the FIU is appointed by decision of the President of the Police Force. The decision to analyse, request, and/or forward or disseminate specific information belongs to the FIU management. When the FIU disseminates information at the request of another competent authority, based on Art. 26(5) (defining the purposes for which information may be requested) and Art. 26(7) of the

14. The FIU has updated the Methodological Order to adjust it with the goAML system in July 2025. However, this was not reflected in the analysis since it was promulgated after cut-off date of June 13 2025.

AML/CFT Act, the FIU has the discretion to refuse to provide such information if doing so would conflict with the stated purpose of the request.

(b) The FIU is authorised to co-operate independently under Art. 26 (2 (b, j, k, l and m)), (3), (5) and (8) of the AML/CFT Act – with internal counterparts. These provisions include both information provided and requested by the Slovak FIU. The ability of the FIU to conduct international co-operation (including with foreign FIUs) on the basis of international treaties binding Slovak Republic and on non-contractual reciprocity principle is stipulated in Art. 28 of the AML/CFT Act. The FIU, as a department of PF, is entitled to co-operate with domestic actors in the virtue of Art. 3 of the Act on Police Forces. The FIU is also able to agree on co-operation with national competent authorities and foreign partners on a contractual basis. Although the FIU has demonstrated operational engagement by signing MOUs with its counterparts, there is no explicit legal authority for the FIU to conclude MOUs independently.

(c) The special position of FIU within the Police Force is derived from the provision of Art. 4(6) of the Act on the Police Force in conjunction with Art. 26 (1) and (2) of the AML/CFT Act and ensures distinct core-functions from those of another authority. The FIU does not fulfill any other tasks that are entrusted to other units of the Police Force.

(d) After the latest reorganisation (August 2019), the FIU has its own budget. On the basis of this change, the Economy Section of the Ministry of the Interior of the Slovak Republic designated the FIU as a cost center for the administration of state property and at the same time in the integrated accounting information.

10. **Criterion 29.8** – The Slovak FIU has been a member of the Egmont Group since June 1997.

Weighting and Conclusion

11. Slovak Republic meets almost all of the requirements under R.29 and only the following minor shortcomings remain: the authority of the Head of the FIU to independently conclude MOUs is not unequivocal (c.29.7(b)), there are deficiencies in the protection of disseminated information and the procedure for handling information is not adjusted to the newly introduced goAML system (c.29.6(a)). **The Slovak Republic is re-rated LC with R.29**.

Recommendation 32 – Cash Couriers

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (upgrade requested, maintained at PC)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	↑ LC (upgrade requested)

1. In its 5th round MER, Slovak Republic was rated PC with R.32 based on the following deficiencies: absence of the EU-internal border declaration system for cash or BNIs (c.32.1); transportation of cash/BNIs by legal persons and/or cross-border transportation of cash/BNIs via mail and cargo are not covered by the legislation (c.32.1); sanctions for non-declaration or false declarations are not dissuasive enough (c.32.5); the completed declaration forms are submitted to the FIU only on a monthly basis (c.32.6); absence of co-ordination among customs, immigration and other related authorities on issues relevant for R.32 (c.32.7); the legislation does not provide power to stop or restrain cash/BNIs for a reasonable period of time to check the existence of the evidence of ML/FT (c.32.8); limited scope of obligation to declare (c.32.1) and particularly the lack of Customs powers to stop or restrain currency (c.32.8) impact this criterion (c.32.11).

2. **Criterion 32.1** – Slovak Republic has a declaration system for incoming and outgoing transportation of cash and BNIs across the external borders of the EU by physical persons based on EU Regulation 2018/1672.

3. Art. 3 of EU Regulation 2018/1672 requires natural persons entering or leaving the EU to declare accompanied cash (defined, inter alia, to include any currency and bearer negotiable instruments (BNIs)), to the value of EUR 10 000 or more. This applies if the cash is on the traveller's person, in their luggage or in their means of transport. Art. 4 of the Regulation provides that where unaccompanied cash (including by post, courier, unaccompanied luggage or containerised cargo) of EUR 10 000 or more is entering or leaving the Union, the competent authorities (defined as customs and any other authorised authorities) may require the sender or recipient (or an authorised representative) to make a disclosure declaration within a deadline of 30 days.

4. In particular, the lack of legal provisions allowing the customs authorities to control cross-border transportation of cash/BNIs via mail and cargo identified by the AT has been addressed through Art. 4 of Regulation (EU) 2018/1672. Item 18 of Regulation (EU) 2018/1672 provides the notion of unaccompanied cash, which refers to postal packages, courier shipments, unaccompanied luggage or containerised cargo. A disclosure system for the intra-EU movements of cash and BNIs has been established (Customs Act and Act No. 35/2019 Coll. on the Financial Administration). According to Section 48a of Act No. 35/2019 Coll. on the Financial Administration, an armed officer of the Financial Administration is authorised to request any person entering or leaving the territory of the Slovak Republic from or to another EU Member State to declare cash exceeding EUR 10 000.

5. **Criterion 32.2** – (a - c) Art. 3 of EU Regulation 2018/1672 requires a written declaration for all travellers carrying cash to the value of EUR 10 000 or more, using a template declaration form as laid out in Commission Implementing Regulation (EU) 2021/776. Art. 3 also states that "The obligation to declare cash shall not be deemed to be fulfilled if the information provided is incorrect or incomplete or if the cash is not made available for control" i.e. an obligation that the declaration is truthful.

6. The declaration system mentioned under c.32.1 obliges any natural persons entering or leaving the territory of the EU carrying cash or BNIs in amounts equal to or greater than EUR 10 000. Passengers who meet this criterion are obliged to declare this fact in writing, by use of the reporting form prescribed by the Decree of the Ministry of Finance No. 161/2016 Coll. (Slovak Republican

authorities have resolved the issues noted in the 4th round MER and now they also use the CDF forms similarly to most of the other EU Member States.)

7. New declaration forms were introduced by Commission Implementing Regulation (EU) 2021/776 of 11 May 2021 (applicable from 3 June 2021) establishing templates for certain forms as well as technical rules for the effective exchange of information under the Regulation (EU) 2018/1672.

8. **Criterion 32.3** – For unaccompanied cash, Art. 4 of EU Regulation 2018/1672 provides that "The obligation to disclose unaccompanied cash shall not be deemed to be fulfilled where the declaration is not made before the deadline expires, the information provided is incorrect or incomplete, or the cash is not made available for control" i.e. to provide authorities with appropriate and truthful information upon request.

9. The domestic disclosure system at the EU internal borders applies to any natural person crossing the border between the Slovak Republic and another EU Member States while carrying cash or BNIs in amounts greater than EUR 10 000. In such cases, the competent authorities have the obligation to prepare an official report without delay containing the information provided by the carrier (para. 3 from Section 48a of Act No. 35/2019 Coll. on the Financial Administration).

10. **Criterion 32.4** – EU Regulation 2018/1672 allows competent authorities to temporarily detain the cash in such cases (see c.32.8) but does not provide any power to request or obtain additional information from a traveller (in the case of a false declaration) or a sender/recipient (in cases of a false disclosure declaration).

11. Customs authorities are required to request information on the origin of currency and BNI as part of the disclosure system (Section 48a(2) of Act No. 35/2019 Coll. on the Financial Administration).

12. **Criterion 32.5** – Art. 14 of EU Regulation 2018/1672 requires member states to introduce effective, proportionate and dissuasive penalties for cases where there has been a failure to comply with the declaration or disclosure requirements. Thus, each member state determines the amount and nature of any sanctions and should do so in line with Art. 14.

13. Infringements of the EU Regulation are penalised in an analogous manner as those applicable to infringements of the national customs law based on Art. 3 of Act 35/2019.

14. Failure to comply with the reporting obligation under Art. 4 of the Customs Act is an administrative offence under Art. 72(1)(n) of the same Act. It is punishable either as a customs tort/delict (if committed by a legal person or a natural person entrepreneur) or as a customs offence (if committed by a natural person). In the case of a customs offence referred to in Section 72(1)(n) the fine may be up to EUR 35 000 (Section 80(2) of the Customs Act,). The same sanctioning regime is foreseen for imports, exports or transportation of rough diamonds in violation of customs regulations or special regulations. For other delicts the threshold of administrative fine is up to EUR 10 000. In simplified (order-based) and on-the-spot fine proceedings (summary proceedings) the fine may be up to EUR 17 500 (Section 80(3) of the Customs Act,) and EUR 5 000 (Section 80(4) of the Customs Act) respectively, for the delict under Art. 72(1)(n).

15. A natural person who, upon request from an armed financial administration officer, fails to declare cash exceeding EUR 10 000 or provides false information about the amount is sanctioned percentage based. A fine of up to 10% of the cash transported may be imposed for this offence in standard administrative proceedings, in warrant proceedings up to 7% of the cash transported and in block proceedings up to 5% of the cash transported (§ 47(1)(n) and (2) of the Offences Act). Forfeiture of goods and articles is another possible sanction for both legal and natural persons (see also C.32.11).

Sanction for both customs delicts and offences are too low. Moreover, there are no supplementary measures. Hence, despite the presence of a range of sanctions, they are not considered as dissuasive.

16. **Criterion 32.6** – (a – b) Art. 9 of EU Regulation 2018/1672 requires that the competent authorities shall record the declaration and disclosure information and make it available to the FIU of the Member State where the information was obtained as soon as possible, and in any event within 15 days. Information is transmitted through the "Custom Information System – CIS", a database directly accessible by the FIU, in accordance with Art. 5 of Implementing Regulation 2021/776. The FIU is also required to share the information with relevant FIUs from other EU member states (Art. 53(1) of EU Directive 2015/849). All EU member state FIUs are connected to CIS.

17. The completed declaration forms as well as notifications on any infringements of the reporting obligation are submitted to the FIU as soon as possible, and in any event no later than 15 working days after the date on which the information was obtained (Regulation (EU) 2018/1672, Art. 9).

18. **Criterion 32.7** – The Slovak Republic reported examples of inter-agency co-operation on issues of co-ordinated exchange of information between different authorities. Financial administration co-operates with the national FIU and regularly provides the data about controls on cash in accordance with Art. 9 of the Regulation (EU) 2018/1672. Customs officers from the Financial Directorate of the Slovak Republic are also members of the Expert Co-ordination Body for the Fight against Crime MEKO, which performs the tasks of the national co-ordinating body for the fight against crime to ensure effective and co-ordinated action in the fight against crime in accordance with the principles of the Council of Europe and the European Union. The Financial Directorate of the Slovak Republic and the MoI of the Slovak Republic signed an Implementing Agreement on Co-operation, the subject of which is the regulation of mutual co-operation between the MoI and the Financial Directorate in the field of border controls and customs supervision. Financial administration co-operates and provides information in the area of cash controls to Office for the Fight against Organised Crime of the Police Force, Department West, National Bank of Slovakia and General Prosecutor´s Office of the Slovak Republic.

19. **Criterion 32.8** – (a–b) Art. 7 of EU Regulation 2018/1672, which has to be implemented under national law, allows competent authorities to temporarily detain cash when the obligation to declare or disclose cash has not been fulfilled or when there are indications that the cash (irrespective of the amount) is related to criminal activity. The initial detention period is limited to 30 days, but this can be extended by competent authorities to 90 days in appropriate cases, where this is necessary and proportionate.

20. The Slovak Republic has established the national procedures to enforce Art. 7 of Regulation. The existing legal framework authorises the Customs or other bodies to stop or restrain currency for a reasonable time in order to ascertain whether evidence of ML/FT may be found in cases mentioned under c.32.8.

21. **Criterion 32.9** – (a–c) Art. 10 of EU Regulation 2018/1672 requires exchange of declaration/disclosure information with competent authorities in other EU member states, and Art. 11 allows such exchange of such information through mutual administrative assistance with authorities in third countries (subject to conditions). Art. 9(2) also requires exchange of such information with relevant FIUs in other EU member states. Under Art. 13 all declaration/disclosure information (which includes information on the currency/BNI, and the identification data of the traveller/carrier) is to be retained for five years and may be further retained for an additional period of up to three years in specific circumstances.

22. The Slovak Republic also applies Council Regulation (EC) 515/97 on mutual administrative assistance in customs matters and Naples II Convention. International conventions (Nairobi

Convention) and agreements on mutual assistance provide basis for international customs co-operation with non-EU countries while in the course of criminal proceedings, MLA may be sought and provided (see R.37-R.38).

23. The retention period of all related documentation (covering all three categories under c.32.9) by the Customs authorities is ten years.

24. **Criterion 32.10** – (a–b) Art. 13 and recital 33 require that the use of personal data shall be carried out in accordance with EU law, and compatible with the purposes of Regulation 2018/1672. Any collection, disclosure, transmission, communication and other processing of personal data is also subject to the requirements of Regulations (EC) 45/2001 and (EU) 2016/679 of the European Parliament and of the Council. Art. 11 requires that any transmission of cash information to a third country is subject to the written authorisation of the competent authority which originally obtained the information and should also comply with national and EU law on the transfer of personal data to third countries.

25. All EU member states are part of an internal market, an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured (Art. 26/2 TFEU and Preamble of EU Regulation 2018/1672).Slovak Republic, as an EU Member State, applies the safeguards to the personal data privacy ensured by Art. 13 and recital 33 of Regulation 2018/1672 providing that the use of personal data shall be carried out in accordance with EU law, and compatible with the purposes of the Regulation. EU Regulation 45/2001 on the data protection is also directly applicable in this context to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

26. **Criterion 32.11** – In principle, natural persons transporting currency or BNI that is related to ML/FT or predicate offences would be subjects to the same criminal sanctions as referred under R.3 and R.5 above, in which case the general confiscation and provisional measures regime would be applicable to the respective currency or BNIs.

Weighting and Conclusion

27. Slovak Republic has implemented almost all criteria under R.32.The outstanding issue remains non-dissuasiveness of sanctions for breaching declaration/disclosure requirements for cash and BNI. **The Slovak Republic is re-rated LC with R.32.**

Recommendation 35 – Sanctions

	Year	Rating and subsequent re-rating
MER	2020	PC
FUR1	2022	PC (no upgrade requested)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (no upgrade requested)
FUR 4	2025	PC (update requested, maintained at PC)

1. In the 5th round MER, Slovak Republic was rated as PC with the R.35, as sanctions could not be imposed on senior management of obliged entities, and the available sanctions for violations of TFS were neither proportionate nor dissuasive.

2. **Criterion 35.1** –

Recommendations 8-23

3. The FIU may sanction all obliged entities for failing to comply with any of the duties laid down in the AML/CFT Act (Art. 33(1)). The FIU may also sanction a natural person who is a member of the statutory body, supervisory body, management body or procuration holder of an obliged entity with a fine of up to 10 times the monthly average of their total income for the preceding 12 months from the obliged entity for failure to comply with or breach of any obligations under the AML/CFT Act (Art. 33(4)). Other supervisory authorities (NBS & MoF) are required to inform the FIU once they uncover violations of AML/CFT requirements as part of their inspections (Art. 29(5)).

4. In determining the type/amount of the sanction (either a fine or other administrative sanctions), the FIU takes into account the seriousness, duration and consequences of the violation, as well as the level of co-operation provided by and size of the obliged entity, and whether the violation has been committed repeatedly (Art. 33 (5)).

5. Furthermore, if the obliged person violates the provisions of the AML/CFT Act consecutively for 12 months or repeatedly, the FIU has powers to request the relevant supervisory authority - either the NBS or MoF (GRA) - to withdraw the authorisation (license) (Art. 34). The supervisory authority in question is obliged to inform the FIU about the follow-up action taken within 30 days. The authorities stated that the NBS shall take into account the severity, duration and consequences of uncovered violations when considering the FIU's request to withdraw the authorisation (license) of banks and securities market intermediaries (Art. 50(1) of the Law on Banks). The Office for Gambling Regulation, as a sanction, may withdraw a license in case of violation of conditions of the Gambling Act or the conditions specified in the license in question (Gambling Act, Art. 91(1)), as well as for a breach of obligations under the AML/CFT Act (Art. 34). It shall take into consideration the nature, gravity, manner and degree of fault, duration and consequences of the unlawful conduct (Gambling Act, Art. 91(5)). The authorities did not explain the legal processes for withdrawing, restricting or suspending the authorisation (license) of other obliged entities for AML/CFT violations. The authorities did not explain the precise legal processes/mechanisms for withdrawing, restricting or suspending the authorisation (license) upon the FIU's request.

6. The FIU may impose fines of up to EUR 5 000 000 with regard to banks and other FIs and up to EUR 1 000 000 with regard to DNFBPs for violations concerning CDD and EDD measures (PEPs, correspondent banking), record-keeping, reporting and suspension of unusual transactions, submission of data to the FIU, and prohibition on dealing with shell banks (Art. 33(1)). The FIU may also impose fines of up to EUR 200 000 for any other violation of the AML/CFT Act (Art. 33(3)), issue cease and desist orders (Art. 33(7)), and require the publication of the FIU's decision to impose a sanction unless this would endanger the stability of the financial market (Art. 33a(1)). The time limit for imposing sanctions is seven years from the day when the violation occurred (Art. 33(6)).

7. The NBS may impose a fine of up to EUR 300 000 (or in case of repeated or severe violations, up to EUR 600 000) for the provision of unauthorised payment services or for breaches of information requirements concerning wire transfers under the Law on Payment Services (No. Art. 78(2) & Art. 86(2) (see also R.14).

8. The authorities did not explain what are the sanctions for breaches of information requirements concerning wire transfers that are not part of the AML/CFT Act.

Recommendation 6

9. The sanctions for the violation of requirements concerning terrorism & terrorist financing related TFS are provided by the Law on Implementation of International Sanctions (No. 289/2016). In particular, articles 21 and 22 stipulate that breaching a restriction, order or prohibition ensuing from an international sanction, or a failure to report the identified property subject to freezing measures shall incur a fine from EUR 5 000 to EUR 66 400, while breaching the tipping-off prohibition therein shall result in a fine from EUR 109 to EUR 6 600. Where these violations result in jeopardising foreign policy and security interests of Slovak Republic, the amount of fines may double, and where they also result in a benefit for the person concerned or a damage exceeding EUR 16 600, a fine from EUR 132 800 to EUR 1 659 700 can be imposed. While the authorities explained that the penalties are imposed in a decentralised manner by the state administrative authorities within the areas of their competence (MoF for the financial market and FIs; MoJ for property interests; MoI for means of transport and real estate), they did not explain what are the criteria for determining the amount of fines that is proportionate to the violation.

Financial sector

10. The measures applied to banks for not complying with the legal framework are provided by Art. 50 of the banks act:

"(1) Where NBS finds any shortcomings in the operations of a bank or a foreign bank branch consisting in a failure to comply with the terms and conditions stipulated in its banking authorisation or in a decision on prior approval, or with the requirements and obligations specified in other decisions of NBS imposed on a bank or a foreign bank branch, a failure to meet the conditions stipulated in Art. 7(2), (4) and (6), and Art. 8(2), (4) and (6), or a violation or circumvention of other provisions of this Act, legally binding acts of the European Union pertaining to banking activities, separate regulations,46 or other legislation of general application governing the conduct of banking operations, NBS may, depending on the seriousness, scope, duration, consequences, and nature of detected shortcomings" apply remedial measures, penalties or impose fines based on the impact determined by the fail of compliance.

11. The NBS has also enforcement and corrective measures regarding the other participants in the financial market as follows:

- Art. 144 of the Act no 566/2001 on securities and investment practices provides corrective measures and fines to be imposed for noncompliance with the provisions of the act and separate laws;
- Art. 139 of the Act no 39/2015 on insurance provides sanctions for noncompliance with the legal provisions of this Act and other separate laws;
- Art. 78 (2) of the Act no 492/2009 on payment services provides corrective measures for not complying with the provisions of the mentioned act and other separate law and regulations;
- Art. 24a of the Act no 202/1995 on foreign exchange provides corrective measures for failing to comply with the provisions of the abovementioned act.

12. The entire financial market legal framework, respectively all the regulations abovementioned use the same wording. Looking at the Art. 50 of the bank act written above, it seems that these provisions could also be used for not complying with any of the AML obligations but it is not specific for AML obligation. It is not enough to make references to other special regulations or other legally binding acts. AML breaches should be regulated in a special act and provide also specific sanctions for not complying with Recommendations 6, 8 to 23.

DNFBPS

13. The Office for Gambling Regulation under the Gambling Act (Art. 77) has powers to impose sanctions, including withdrawal of license, for the entities under their supervision if there are identified violations of the gambling act, special acts and other generally binding legal regulations applicable to gambling game operation, promotion of gambling games, conditions of operation of gambling games laid down in the Gambling Act or specified in an individual license or general license, the duties according to the approved game plan including the gambling game rules or fails to fulfil the duties imposed upon them by a valid decision of the supervisory body. The Office for Gambling Regulation imposes the sanctions on the nature, seriousness, way, rate of guilt, length of duration and consequences of the violation of duties.

14. The AML/CFT Act provides sanctions for AML breaches of the DNFBPs and SRB can withdraw certificates/license if any of the conditions on which it were issued are no longer available. The FIU can impose administrative sanctions for AML breaches on both natural and legal persons, including DNFBPs (Art. 33 (1), (3) and (4)).

15. **Criterion 35.2** – Sanctions can be applied to members of obliged entities' (both FIs and DNFBPs) statutory bodies or supervisory board, a member of the obliged entity's management body, or the obliged entity's procurator as well as natural persons – entrepreneurs (AML/CFT Act, Art. 33(1), (3) and (4)).

Sanctions for directors and senior management

16. According to Art. 33(1) and (3) of the AML/CFT Act, the administrative sanctions to natural persons – entrepreneurs can be applied for violation of the obligations under the AML/CFT Act.

17. If an obliged entity fails to comply with or breaches any of its obligations laid down in the AML/CFT Act, the FIU may impose on a member of the obliged entity's statutory body or supervisory board, a member of the obliged entity's management body, or the obliged entity's procurator a fine amounting up to ten times the monthly average of such person's total income for the previous twelve months from the obliged entity; if such person was receiving income from the obliged entity during a period shorter than the previous twelve months, the monthly average shall be calculated from the person's total income from the obliged entity for the months during which the person was receiving income from the obliged entity (AML/CFT Act, Art. 33(4)).

18. The financial sectors' supervisor has powers to impose a fine up to EUR 5 000 000 to a member of a bank's management, a chief executive officer, a senior employee (Art. 50 of the Act of banks). The insurance sector has in place measures to impose to members of the board of directors or supervisory board, to the head of a branch, or any other natural person controlling an insurance or a reinsurance undertaking a fine up to 50% of twelve times the monthly average of their income (Art. 139 (6) of the Act of insurance). The securities sector has in place measures to impose a fine up to twelve times the monthly average of the income of a director or a senior manager (Art. 202 (2) of the Act of securities). NBS can also impose sanction to a natural person who holds the position of a statutory body or member of the statutory body or supervisory body of a financial agent or a financial adviser, respectively a fine up to EUR 50 000 (Art. 39 (7) of the Act No. 186/2009 on financial intermediation and financial advisory services).

Weighting and Conclusion

19. The following moderate deficiency remains: the sanctions available for violations of TFS are not proportionate and dissuasive (c.35.1). In addition, minor deficiencies are as follows: no clear process for withdrawing, restricting or suspending the authorisation of other REs than banks, securities market intermediaries, and gambling entities, including upon the FIU's request; no clarity on the sanctions for breaches of information requirements concerning wire transfers that are not part of the AML/CFT Act; the legal provisions envisaging sanctions for financial institutions are of general nature and not specific for AML/CFT obligations embedded in Recommendations 6, and 8-23 (c.35.1). **The Slovak Republic remains rated as PC with R.35.**

Annex B: Summary of Technical Compliance – Deficiencies underlying the ratings

Recommendations	Rating	Factor(s) underlying the rating[15]
8. Non-profit organisations	PC (MER 2020) PC (FUR2 2023) PC (FUR3 2024) **PC (FUR4 2025)**	• The authorities have identified the features and types of NPOs likely to be at risk of TF abuse to a limited extent only. (c.8.1(a), as per FUR3 2024) • The Sectorial Risk Assessment lacks thorough analysis, along with detailed threat information, failing to identify specific nature of threats posed by terrorist entities to the NPOs at risk. (c.8.1(b), as per FUR3 2024) • As concerns remain under 8.1(a) criterion, it is not clear if adequacy of measures has been identified to the full extent. (c.8.1(c) as per FUR3 2024) • Absence of risk-based approach in supervision of NPOs. (c.8.3)
10. Customer due diligence	PC (MER 2020) PC (FUR1 2022) **LC (FUR4 2025)**	• There is no requirement to verify BOs based on reliable source data for low and medium risk customers. (c.10.5) • Possibility to rely on other credible sources for identification and verification purposes does not ensure that all required information is obtained and verified (c.10.9(a)) • Identifying the natural person authorised to act on behalf of the legal entity also does not amount to obtaining the names of all relevant persons holding the senior management position (e.g. senior managing directors). (c.10.9(b) - FUR1) • For beneficiaries that are designated by characteristics or class, the identification is limited to the circle of persons having a substantial benefit from the founding or operation of a trust (c.10.11(a) – FUR4) • There is no requirement for FIs to obtain sufficient information concerning the beneficiary of foreign trust (designated by characteristics or class) (c.10.11(a)- FUR4) • Regarding legal arrangements absence of specific obligation to identify persons having equivalent or similar positions to those in a trust (c.10.11(b) – FUR4) • There is no requirement to identify and verify the beneficiary that is a legal arrangement. (c.10.13 – FUR4) • Absence of legal provisions that would require FIs to apply CDD to existing customers depending on the materiality, and to take into account the timing of previous CDD measures and the adequacy of data obtained when determining the frequency of periodic reviews. (c.10.16)
12. Politically exposed persons	PC (MER 2020) PC (FUR1 2022) **LC (FUR4 2025)**	• The definition of family members does not include siblings of PEPs, which is part of the minimum standard provided by the FATF Guidance. (c.12.3)

15. Deficiencies listed are those identified in the MER unless marked as having been identified in a subsequent FUR.

		• Close associates of PEPs are limited. (c.12.3, FUR1) • There is no requirement for the FIs providing life insurance policies to take reasonable measures to determine whether the beneficiaries or the BO of legal arrangements are PEPs. (c.12.4 – FUR4) • There is no explicit requirement to consider making an UTR when beneficiary or BO are PEP. (c.12.4 – FUR4)
13. Correspondent banking	PC (MER 2020) PC (FUR1 2022) **C (FUR4 2025)**	
15. New technologies	LC (MER 2020) PC (FUR1 2022) PC (FUR3 2024) **LC (FUR4 2025)**	• The assessment of the VA/VASP Sector is constrained due to issues with lack of supervision, statistical data availability and complexity. (c.15.3(a), as per FUR3 2024) • Deficiencies in relation to c.1.11 apply in relation to VASPs. (c.15.3(c), as per FUR1 2022) • Deficiencies in the VASP risk assessment negatively impact the risk-based supervision. (c.15.6(a), as per FUR1 2022) • Deficiency identified under R.27, i.e., absence of the information regarding legal processes for withdrawing, restricting or suspending the license for AML/CFT violation, equally applies to VASPs (c.15.6(b)- FUR1) • Sanctions applicable to VASPs for violations of terrorism & TF related TFS are not proportionate and dissuasive. (c.15.8(a), as per FUR1 2022) • Identified deficiencies under R.10-21 equally apply to VASPs. (c.15.9(a), as per FUR1 2022) • The is no direct reference in the legislation to "monitor" the compliance of VASPs with R.7. (c.15.10, as per FUR3 2024) • International co-operation and exchange of information can occur with a view to covered VASPs in the extent allowed by the deficiencies identified under R.38 to R.40. (c.15.11, as per FUR3 2024)
18. Internal controls and foreign branches and subsidiaries	PC (MER 2020) PC (FUR1 2022) **PC (FUR4 2025)**	• The implementation of group-wide AML/CFT programs is required for foreign branches and majority-owned subsidiaries only (c.18.2 – FUR4) • The term intra-group sharing does not specifically cover provision of data between selected group-level functions (compliance, audit, and/or AML/CFT function) and it is not clear that the dissemination of those data to members of the group is required for risk management purposes. (c.18.2(a) and(b) – FUR4) • Limited requirement to include adequate safeguards prevention of tipping-off in the group-wide AML/CFT programs. (c.18.2(c) - FUR1) • The law does not explicitly require the application of home country AML/CFT measures where host country requirements are less strict, and host country requirements are only

		assessed against selected/limited AML/CFT requirements of Slovak Republic. (c.18.3 – FUR4)
19. Higher-risk countries	PC (MER 2020) PC (FUR2 2023) PC (FUR3 2024) **C (FUR4 2025)**	
23. DNFBPs: Other measures	PC (MER 2020) PC (FUR1 2022) **LC (FUR4 2025)**	• Shortcomings identified under Recs. 18, and 21 equally apply to DNFBPs. (c.23.2 and c.23.4) • TCSPs are not required to report suspicious transactions when performing the equivalent function of a trustee for other forms of legal arrangement (c.23.1(c))
28. Regulation and supervision of DNFBPs	PC (MER) PC (FUR1 2022) PC (FUR2 2023) **PC (FUR4 2025)**	• Absence of the measures in place to prevent associates of criminals from holding management functions in casinos (c.28.1 (b)) • There is no ongoing monitoring of fit and proper requirements for holders of managerial function (c.28.1(b)- FUR4) • Absence of the measures to prevent non-convicted associates of criminals to be professionally accredited or holding (or being a beneficial owner of) a significant or controlling interest or holding a management function in other DNFBPs (c.28.4 (b) – FUR4).
29. Financial intelligence units	PC (MER 2020) PC (FUR1 2022) **LC (FUR4 2025)**	• The procedure for handling information is not adjusted to the newly introduced goAML system (c.29.6(a)) • The Head of the FIU is not undoubtedly able to conclude MOUs independently (c.29.7(b))
32. Cash Couriers	PC (MER 2020) PC (FUR1 2022) **LC (FUR4 2025)**	• Despite the presence of a range of sanctions, they are not considered as dissuasive (c.32.5 - FUR4)
35. Sanctions	PC (MER 2020) **PC (FUR4 2025)**	• No clear process for withdrawing, restricting or suspending the authorisation of reporting entities other than banks, securities market intermediaries, and gambling entities, including upon the FIU's request (c.35.1) • No clarity on the sanctions for breaches of information requirements concerning wire transfers that are not part of the AML/CFT Act (c.35.1) • The legal provisions envisaging sanctions for financial institutions are of general nature and not specific for AML/CFT obligations embedded in R.6 and 8-23 (c.35.1) • Absence of proportionate and dissuasive sanctions or violations of TFS. (c.35.1)

GLOSSARY OF ACRONYMS

AML/CFT	Anti-Money Laundering/ Countering the Financing of Terrorism
BO	Beneficial ownership
C	Compliant
CASP	Crypto-Asset Service Provider
CDD	Customer due diligence
CTU-NAKA	Counter-Terrorism Unit NAKA
DLT	Distributed Ledger Technology
EDD	Enhanced due diligence
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial intelligence unit
FUR	Follow-up report
ISA	International Sanctions Act
JCO	Joint customs operations
JIT	Joint investigation team
LC	Largely compliant
LEA	Law enforcement agency
MER	Mutual evaluation report
MiCAR	Regulation (EU) 2023/1114 on Markets in Crypto-Assets
ML	Money laundering
MoI	Ministry of Interior
NBS	National Bank of Slovakia
NC	Non-compliant
NPO	Non-profit organisation
NRA	National risk assessment
NSAC	National Security Analytical Center
PC	Partially compliant
PEP	Politically exposed person
R.	Recommendation
SIS	Slovak Information Service
SRA	Sectorial risk assessment
SRB	Self-regulating body
TF	Terrorism financing
TFS	Targeted financial sanctions
UTR	Unusual transaction report
VA	Virtual assets
VASP	Virtual asset service provider

www.coe.int/MONEYVAL

December 2025

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Slovak Republic

4th Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Slovak Republic's progress in addressing the technical compliance deficiencies identified in the September 2020 assessment of their measures to combat money laundering and terrorist financing and in subsequent follow-up reports.