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(2026)4

Anti-money laundering and counter-terrorist financing measures

Bulgaria

3rd Enhanced Follow-up Report & Technical Compliance Re-Rating

June 2026

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 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating on Bulgaria was adopted by the MONEYVAL Committee through written procedure (12 May 2026).

Bulgaria: 3rd Enhanced Follow-up Report

I. INTRODUCTION

1. The 5th round mutual evaluation report[1] (MER) of Bulgaria was adopted in May 2022 (2022 MER). Given the results of the MER, Bulgaria was placed in enhanced follow-up[2] and its 1st Enhanced Follow-up Report was adopted in May 2024 (FUR 2024) and 2nd Enhanced Follow-up Report was adopted in May 2025 (FUR 2025). This report analyses the progress of Bulgaria in addressing the technical compliance (TC) deficiencies identified in its MER and subsequent FURs, 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.

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

- Liechtenstein
- Lithuania

3. Section III of this report summarises the progress made by Bulgaria in improving technical compliance. Section IV sets out the conclusion and a table showing which Recommendations (R./Recs) 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.

5. Current desk – based follow- up review is based on 2013 FATF Methodology.

6. In line with the FATF project on ensuring consistent and coherent assessments of European Union (EU) supranational measures, common text adopted in February 2025 has been used under R.7 and R.15.

II. BACKGROUND, RISK AND CONTEXT

7. 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.

8. Bulgaria has revised its confiscation regime addressing key deficiencies identified under **R.4** in 2022 MER. Changes to the CC (Art. 53) allow now confiscation of property and instrumentalities owned by non-*bona fide* third parties.

9. As regards to **R.5**, Bulgaria has amended the Criminal Code (CC) with material changes since the MER and prior follow-up reporting. It addresses the core technical deficiencies that previously prevented higher compliance under R.5, notably: (i) *per se* criminalisation of the treaty offences without an impermissible additional purposive element and completion of coverage of terrorist bombings (Art. 114c); (ii) comprehensive criminalisation of travel for terrorist purposes regardless of citizenship/residency constraints (Art. 114m); (iii) alignment of the TF offence with the FATF requirement to cover "*funds and other assets*" (Art. 114o(3)) and confirmation that lawful origin / actual use are not required; and (iv) restoration/strengthening of proportionate and dissuasive sanctions for natural persons and significantly reinforced administrative liability tools for legal

[1] Source available at: www.coe.int/en/web/moneyval/jurisdictions/bulgaria

[2] Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.

persons (Criminal Procedure Code (CPC) and Administrative Violations and Sanctions Act (AVSA) amendments).

10. Moreover, the changes to the Law on Measures Against the Financing of Terrorism and of Proliferation of Weapons for Mass Destruction (LMFTPWMD) have addressed all deficiencies identified in 2022 MER under **R.7**.

11. As regards to **R.8**, detailed non-profit organisations (NPOs) risk assessment has been carried out identifying NPOs under the threat of TF.

12. Deficiencies identified in 2022 MER under **R.13** are addressed through amendments to Law on the Measures Against Money Laundering (LMML) which require to apply additional measures to all cross-border correspondent relationships (regardless of risk level and whether the respondent institution is established in the European Union (EU) or European Economic Erea (EEA) Member State).

13. Regulations in relations to **R.15** (new technologies) have been enhanced covering gaps in relation to regulating virtual assets service providers (VASPs) and virtual assets (VA) as identified in 2022 MER.

14. In addition, the sanctions and mutual legal assistance regime has been enhanced addressing deficiencies under **R.35** and **R.38**.

III. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

15. This section summarises the progress made by Bulgaria to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER and applicable subsequent FURs for which the authorities have requested a re-rating (R.4, R.5, R.7, R.8, R.13, R.15, R.35 and R.38).

16. 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 Bulgaria submitted its country reporting template – at least six months before the follow-up report (FUR) is due to be considered by MONEYVAL[3].

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

17. Bulgaria has made progress to address the technical compliance deficiencies identified in the MER and applicable subsequent FURs. As a result of this progress, Bulgaria has been re-rated on Recommendations 4, 5, 7, 8, 13, 15, 35 and 38.

18. Annex A provides a description of the country's compliance with each Recommendation that is reassessed, set out by criterion, with all criteria covered[4]. Annex B provides the consolidated list of remaining deficiencies of the re-assessed Recommendations.

[3] 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.

[4] Amendments highlighted in grey shading are based on newly submitted information since the adoption of the MER or last follow-up report and amendments highlighted in yellow shading indicate changes introduced as a result of comments submitted by the Global Network and, correspondingly, require plenary's discussion and approval.

V. CONCLUSION

19. Overall, in light of the progress made by Bulgaria since its MER or 2nd FUR was adopted, its technical compliance with the Financial Action Task Force (FATF) Recommendations has been re-rated as follows:

Table 1. Technical compliance with re-ratings, April 2026

R.1	R.2	R.3	R.4	R.5
LC	LC (FUR1 2024) ~~PC~~	LC	**C (FUR3 2026)** ~~PC~~	**C (FUR3 2026)** ~~PC~~
R.6	R.7	R.8	R.9	R.10
C (FUR2 2025) ~~PC~~	**C (FUR3 2026)** ~~PC~~	**C (FUR3 2026)** ~~PC~~	LC	LC (FUR2 2025) ~~PC~~
R.11	R.12	R.13	R.14	R.15
LC	LC (FUR1 2024) ~~PC~~	**C (FUR3 2026)** ~~PC (FUR1 2024)~~ ~~PC~~	C (FUR1 2024) ~~PC~~	**LC (FUR3 2026)** ~~PC (FUR1 2024)~~ ~~PC~~
R.16	R.17	R.18	R.19	R.20
LC	C	LC (FUR1 2024) ~~PC~~	LC	LC
R.21	R.22	R.23	R.24	R.25
LC	LC (FUR1 2024) ~~PC~~	LC	C (FUR2 2025) ~~PC~~	LC (FUR1 2024) ~~PC~~
R.26	R.27	R.28	R.29	R.30
LC (FUR1 2024) ~~PC~~	LC (FUR1 2024) ~~PC~~	LC (FUR2 2025) ~~PC~~	LC	LC
R.31	R.32	R.33	R.34	R.35
C	C (FUR1 2024) ~~PC~~	C (FUR1 2024) ~~PC~~	C (FUR2 2025) ~~PC~~	**LC (FUR3 2026)** ~~PC~~
R.36	R.37	R.38	R.39	R.40
LC	LC	**LC (FUR3 2026)** ~~PC~~	LC	LC

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

20. Bulgaria has implemented all 40 Recommendations at the level of LC/C. In application of Rule 23(5) of the Rules of Procedure, no further reporting shall be required under MONEYVAL's 5th round of evaluations.

Annex A: Reassessed Recommendations

Recommendation 4 - Confiscation and provisional measures

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (no upgrade requested)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	C ↑ (upgrade requested, upgraded)

1. Bulgaria was rated PC on R.4 in 2022 MER. Following deficiencies were identified: (i) instrumentalities and intended instrumentalities of a criminal offence could only be confiscated from the perpetrator and not from third persons; (ii) there was no clear provision for all aspects of the confiscation of property "*intended or allocated for use*" in relation to TF; (iii) unless the respective object (property item) constituted material evidence in the criminal proceedings (and thus could be subject of seizure pursuant to the CPC) the provisional measures could not be applied before a formal accusation takes place and neither can they be applied to third parties (this also refers to the asset forfeiture proceedings by the CACIAF); (iv) for the purposes of applying provisional measures in the criminal procedure, there was no explicit definition of property subject to these measures; (v) there was no mechanism available for the active management of seized and confiscated assets beyond storage and safekeeping measures, and for managing and disposing of property that has been confiscated under the CC.

2. ***Criterion 4.1*** – Bulgaria has following conviction-based measures in place for the confiscation of assets either held by criminals or third parties:

(a) laundered property (CC, Articles 253 (6), 114o (4) and 53 (4) – (6));

(b) proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in ML, predicate offences (Art. 53 (1)(a), (2)(b), (3), (5) and (6);

(c) property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorist, terrorist acts of terrorist organisations (Articles 114o (4) and 53 (1)(a), (2)(b), (3), (5) and (6)); or

(d) property of corresponding value (CC, Art 53).

3. ***Criterion 4.2*** Bulgaria has measures in place to allow competent authorities to:

(a) identify, trace, and evaluate property that is subject to confiscation through the broad powers available to LEAs in the Criminal Procedure Code and available in all criminal investigations including seizure of documents and searches of databases (CPC, Articles 102, 112 and 159 (1); Credit Institution Act, Art.62(6));

(b) carry out provisional measures *ex parte* and without prior notice, including seizing property to prevent its transfer or disposal prior to confiscation, including property of equivalent value (CC, Articles 72 and 53);

(c) take steps that will prevent or void actions that prejudice the ability to seize or recover property subject to confiscation (Law on Obligations and Contracts, Art. 135; Law for Combating Corruption and Illegal Assets Forfeiture, Art. 143);

(d) take other investigative measures as set out in R.31.

4. ***Criterion 4.3*** - Bulgarian law protects the rights of *bona fide* third parties with legitimate interests in property at both the seizure and confiscation stages (CC, Articles 53(2)(b) and 253(6), including through general principle in the Law on ownership, which provides that good faith is always presumed until proven otherwise.

5. ***Criterion 4.4*** – Mechanisms are in place to manage confiscated assets (Law for Combating Corruption and Illegal Assets Forfeiture, Chapter 13 and CPC, Art.72a) and where necessary to dispose of seized and confiscated assets in relation to detained goods (Rules for the Administration of the Prosecutor's Office of the Republic of Bulgaria).

Weighting and Conclusion

6. All criteria are met. **R.4 is re-rated as C.**

Recommendation 5 - Terrorist financing offence

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (no upgrade requested)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	C ↑ (upgrade requested, upgraded)

1. Bulgaria was rated PC on R.5 in 2022 MER. The factors underlying this rating were: (i) The TF offence prescribed the purposive element for the TF offence, for all the offences, including the ones specified under the Conventions and Protocols listed in the Annex to the TF Convention; (ii) it was unclear whether and to what extent the TF offence extended to funds and other assets as required by the FATF standards; (iii) financing of travels to and from Bulgaria for the purpose of committing a terrorism-related act was not covered in its every aspect; (iv) the range of punishment for TF was lowered and the elimination of additional fines reduced the proportionality of the sanctions; and, (v) there was no corporate criminal liability and the administrative liability of legal persons for criminal offences is limited.

2. ***Criterion 5.1*** – Bulgaria criminalises TF in line with the TF Convention through Chapter One "a" (Terrorism) in the Criminal Code (CC), which establishes a dedicated set of core (main) terrorist crimes and related terrorist offences, including conduct corresponding to the offences in the Annex to the TF Convention.

3. ***Criterion 5.2*** – The TF offence is set out in Art. 114o(1) of the CC. It criminalises the direct or indirect collection or provision of financial means or other property, knowing or assuming that they will be used in whole or in part: (1) to commit a crime under Chapter One "a"; (2) by a terrorist group or organisation (CC, Art. 114p); or (3) by an individual terrorist, expressed as "*a person who has committed a crime under this chapter*". The legal motives clarify that the formula "*a person who has committed a crime*" is a material-law concept that does not require a conviction and encompasses completed offences as well as attempt and preparation; therefore, financing an "*individual terrorist*" is not dependent on a prior conviction and is not confined to a specific terrorist act.

4. ***Criterion 5.2bis*** – Bulgaria criminalises the collection or provision of funds or assets for the purposes of funding travel for an individual for terrorist purposes which includes travel for the purposes of preparing, planning of participating in a terrorist or receiving terrorist training (CC, Articles 114, 114m(2), 114m(3) and 114o(1)(1)).

5. ***Criterion 5.3*** – TF offense extends to any funds or assets whether from legitimate or illegitimate source (CC, Art 114o(3)). There is no legal requirement that the assets be of known or lawful origin and no requirement that the assets have been used for terrorism.

6. ***Criterion 5.4*** – The TF offences do not require funds or assets to be (a) actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s) if the funding is related to a terrorist organisation (CC, Art.114o)).

7. ***Criterion 5.5*** – Intent and knowledge can be inferred from objective factual circumstances (CPC, Art. 104).

8. ***Criterion 5.6*** – TF is punishable by imprisonment (3–12 years) and a fine (approximately from EUR 2500 to 15 300), together with deprivation of rights; aggravated forms carry 10–20 years' imprisonment with confiscation and deprivation of rights (CC, Art. 114o(1)). The offence also provides for forfeiture of the object of the crime (or its equivalent). In addition, Art. 114u of the CC provides for additional deprivation of rights and allows confiscation for crimes under the chapter. The penalties available are proportionate and dissuasive compared to similar offences in Bulgaria.

9. ***Criterion 5.7*** – Bulgaria does not recognise criminal liability of legal persons. This reflects a fundamental principle of domestic law (FPDL), as the relevant constitutional guarantees on criminal responsibility and due process are framed around the individual (natural person), notably Articles 5(3), 30(1) and 31(1), as further supported by Constitutional Court Ruling No. 12 of 5 November 2024. Nevertheless, Bulgaria provides for administrative-criminal liability of legal persons under Article 83a of the Administrative Violations and Sanctions Act (AVSA) for terrorism/TF-related offences. The July 2025 amendments strengthened the framework by enabling proceedings also where a legal entity was created or used for terrorism/ML/organised crime group purposes (addressing TF typologies where "benefit/enrichment" may be difficult to evidence). The pecuniary sanctions were recalibrated and now reach up to EUR 5 124 000 and are turnover-linked in defined circumstances (including a 5% annual turnover mechanism and a turnover floor where the benefit is non-material or cannot be determined). In addition, courts may impose non-pecuniary sanctions (1–3 years), including temporary bans from public procurement/concessions, bans on receiving EU funds/subsidies/grants, and public announcement of the decision. Furthermore, amendments to the CPC introduced the procedural status of an "*interested legal entity*", ensuring participation rights and representation safeguards (including appointment of a special representative where conflicts exist) and allowing, where appropriate, proceedings against natural and legal persons to proceed in parallel within the same case.

10. ***Criterion 5.8*** – Bulgaria has criminalised ancillary offences as follows through general rules in CC:

(a) attempt to commit the TF offence (CC, Art.18);

(b) participate as and compliance in TF offence or attempted offence (CC, Art.17);

(c) organise or direct others to commit a TF offence or attempted offence (CC, Art.20);

(d) Contribute to commission of one or more TF offence(s) or attempted offence(s), by group of persons acting with common purpose (CC, Art.20).

11. In addition, Chapter One "a" contains specific ancillary terrorist offences (e.g., incitement; recruitment/training; preparation and travel for terrorist purposes), further supporting comprehensive coverage of conduct required by this criterion.

12. ***Criterion 5.9*** – All criminal offences, including the TF offence in Art. 108a (2) of the CC, can constitute a predicate offence for ML (see c.3.2).

13. ***Criterion 5.10*** – TF offences apply, regardless of the location of the financier or the terrorist/terrorist organisation (CC, Articles 3 - 6 and 114o).

Weighting and Conclusion

14. All criteria are met. **R.5 is re-rated as C.**

Recommendation 7 – Targeted financial sanctions related to proliferation

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (no upgrade requested)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	C ↑ (upgrade requested, upgraded)

1. In 2022 MER, Bulgaria was rated PC on R.7. Main deficiencies identified were related to the absence of national procedures for the implementation of targeted financial sanctions (TFS) in relation to proliferation financing (PF).

2. Bulgaria implements PF TFS through EU decisions and regulations, complemented by domestic legislation[5]

3. **Criterion 7.1** –

(a) At the European Union (EU) level, implementation of TFS, pursuant to United Nations Security Council Resolution (UNSCR) 1718, does not occur "without delay." This is due to the time taken to consult between European Commission (EC) departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages.

(b) At national level, the Law on Measures Against the Financing of Terrorism and of Proliferation of Weapons for Mass Destruction (LMFTPWMD) ensures that restrictive measures introduced by the UNSC apply immediately to Bulgaria. Article 5a (1) LMFTPWMD obliges the Ministry of Foreign Affairs (MFA) to immediately publish on its website references to the adopted UNSCRs and successive designations on imposing sanctions in relation to proliferation of weapons for mass destruction or its financing. Upon publication, the obligation to freeze all funds or other assets immediately enters into force (Art. 4b LMFTPWMD). This creates a national framework to implement TFS in relation to PF without delay and addresses any potential delays at the EU level.

4. ***Criterion 7.2***

(a) At the EU level, all natural and legal persons within the EU are required to freeze the funds or other assets of designated persons or entities as soon as a designation is published, i.e. without prior notice (EU Regulation 2017/1509, art.1and 2). Though delays in implementation apply as described under c.7.1.

At national level, the measures are in place which include freezing funds or other assets (LMFTPWMD, Art. 3 (1)). These measures are applied to natural persons, legal persons, groups and organisations identified by the UNSC as associated with proliferation of weapons for mass destruction or for its financing (LMFTPWMD, Art. 4b) following the publication of the information under Art. 5a of the LMFTPWMD. The LMFTPWMD does not clearly specify who are obliged to implement these measures while it does not prescribe also that the LMFTPWMD is applicable only to a limited group. No provision of the LMFTPWMD requires that notice should be given to a party prior to a freezing.

(b) At the EU level, freezing actions for UNSCR 1718 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, and includes assets generated from such funds. (EU Regulation 2017/1509, art. 1 and 34). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35). While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds 'controlled' by the designated person (Para 55b. of the Guidelines on implementation and

[5] At the EU level, UNSCR 1718 (2006) on DPRK and its successor resolutions are implemented through Council Decision 2016/849/CFSP and EU Regulation 2017/1509.

evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy).

Article 6 (1) and (5) LMFTPWMD extend to also cover sanctions in relation to PF. Although the LMFTPWMD does not clearly cover assets held directly or indirectly by designated persons, indirectly held assets are covered by Article 6 (1) and (5) as it extends to assets held by any persons acting on their behalf or for their benefit or on their instruction.

(c) At the EU level, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU regulation 2017/1509, art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU.

At national level, Article 7 (1) LMFTPWMD prohibits providing directly or indirectly funds and other assets, as well as financial services, to any designated person, as well to any persons acting on their behalf and for their benefit or on their instruction, except by an authorisation issued under the terms and according to the procedure established by Article 6 LMFTPWMD.

(d) At the EU level, the same mechanism to communicate PF TFS is used as for TF TFS (see c.6.5(d)). Article 5a LMFTPWMD requires that the MFA shall publish immediately on its web site information on the adopted resolutions of the UNSC on imposing sanctions in relation to PF, as well as the amendments of the lists of persons under these resolutions.

At national level, The MFA has also developed a communication and information platform for public notification regarding the adoption, modification and lifting of targeted financial sanctions imposed by the UN Security Council as explained in the Guidance on the Implementation of Measures Against Financing of Terrorism and Financing of Proliferation.

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations. (EU Regulation 2017/1509, art. 50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations.

At the national level, Article 3 (2) LMFTPWMD stipulates that persons who have implemented TFS need to notify the Minister of Interior, the Minister of Finance, the Chairperson of the State Agency for National Security and the Commission for Illegal Assets Forfeiture, including in the cases of an attempt to carry out a transaction or operation with funds.

(f) At the EU level, protections are in place for third parties acting in good faith (EU Regulation 2017/1509, art.54).

5. **Criterion 7.3** – Under the EU Regulations 267/2012 (Art. 47) and 2017/1509 (Art. 55), EU Member States must take all necessary measures to implement EU regulations, which would include adopting measures to monitor compliance of the sanctions regime by FIs and DNFBPs. Article 14a LMFTPWMD outlines the authorities responsible for ensuring compliance with the obligations in the LMFTPWMD. The State Agency for National Security Chairperson is the primary entity overseeing compliance, following the procedures in Chapter Nine of the Measures against Money Laundering Act. Additionally, specific institutions are assigned oversight responsibilities. Article 14b LMFTPWMD states that for entities not covered under Article 4 of the Measures Against Money Laundering Act, compliance control is conducted by the Minister of Interior. Article 15 LMFTPWMD establishes penalties for violations of the LMFTPWMD.

6. **Criterion 7.4**

(a) – (d) At the EU level, listed persons are informed of their ability to petition the UN Focal Point or their own government for de-listing, through the EU Best Practices document for the effective implementation of restrictive measures (page 11, para. 23). At the EU level, procedures for unfreezing funds due to cases of mistaken identity are the same as those described under c.6.6(f). At the EU level, the regulation imposing TFS obligations under UNSCR 1718 contains measures for national competent authorities to authorise access to frozen funds or other assets under the conditions set out in UNSCR 1718. (EU Regulation 2017/1509, art. 35-36). At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c7.2(d) also contains information on the obligations to respect a de-listing action.

At a national level, natural persons, legal persons, groups and organizations listed under the sanction's regimes of for proliferation or its financing, may directly or through a representative submit a request to the Focal Point for Delisting established pursuant to United Nations Security Council Resolution 1730 (2006) for their de-listing. The contact details and the mandate of the Focal Point for Delisting established pursuant to UNSC 1730 (2006) are published on the website of the Ministry of Foreign Affairs (Art. 4(a1) LMFTPWMD). Regarding Criterion 7.4(b), the "Guidance On The Implementation Of Measures Against Financing Of Terrorism And Financing Of Proliferation" includes procedures to unfreeze funds in cases of false positives (chapter 4.3.6). Moreover, Article 6 (6-9) LMFTPWMD outlines the conditions under which frozen funds or assets may be used despite restrictions (Criterion 7.4(c)). In terms of Criterion 7.4(d), Bulgaria uses the same communication systems for notifying de-listings as it does for listings (see Criterion 7.2(d)). The "Guidance On The Implementation Of Measures Against Financing Of Terrorism And Financing Of Proliferation" includes delisting from the sanctions list of UN resolutions (chapter 4.4).

7. **Criterion 7.5**

(a) At the EU level, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EU Regulation 2017/1509, art. 34(9)).

At the national level, the Article 6 of the LMFTPWWD establishes the freezing of funds and assets belonging to certain individuals and entities to prevent their use. Newly acquired funds and assets after the public disclosure of restrictive measures are also frozen. Interest and civil benefits from frozen assets continue to accumulate but remain frozen. Designations under UNSC TFS, pre-existing contractual obligations (before the freezing measure) can still result in new receipts, but these too will be frozen (Art. 6 (4) LMFTPWWD).

(b) Payments due under a contract entered into prior to the date of listing are permitted provided that prior notification is made to the UN Sanctions Committee and that it is determined that the payment is not related to any of the prohibitions under the regulations (Art. 8 Reg. 329/2007; Art. 25 Reg. 267/2012).

Weighting and Conclusion

8. All criteria are met. **R.7 is re-rated as C**.

Recommendation 8 – Non-profit organisations

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (no upgrade requested)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	C ↑ (upgrade requested, upgraded)

1. In its 2022 MER, Bulgaria was rated PC on R.8. The summary of the factors underlying this rating were: (i) Bulgaria did not conduct comprehensive analysis of NPO sector recently (last complex analysis was conducted in 2012); (ii) Bulgaria had not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors could abuse those NPOs; (iii) No dedicated outreach was provided to the donor community; and (iv) the monitoring or supervisory measures were applied to all NPOs regardless of TF risk and were not risk based.

2. ***Criterion 8.1***

(a) In Bulgaria, NPO sector is regulated through the Law on Non-profit Legal Persons (LNPLP), according to which NPOs are associations and foundations carrying out activities for the public benefit. The National Risk Assessment (NRA), in the analysis of specific TF channels, highlights religious organizations operating internationally as being more vulnerable to TF abuse and reflect the overall Bulgarian NPO sector with medium risk, based on observations and Bulgarian context. In the period 2023-2025 Bulgaria conducted an extensive TF risk assessment of NPO sector (The 2023 NPO TF Risk Assessment Report) using relevant sources of information on features and types on NPOs and has identified organisations that fall within the FATF definition of NPO: 12 683 NPOs in Bulgaria fall under the FATF definition, with 364 classified as being at risk for TF abuse.

(b) Bulgaria has identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors could abuse those NPOs. Updates to NRA identified following 2 terrorism financing risk factors: TF risk via cash transfers and migrant risk. The 2023 NPO TF Risk Assessment Report identified following TF threats: false representation or sham NPOs; diversion legal funds intended for humanitarian programmes; abuse of programmes to promote philosophies designed to promote religious hatred and spread the ideas of a terrorist organisation; and, links to terrorist entities. Following characteristics have been identified at the risk of abuse for TF: carrying out activities in regions at risk of terrorism or receiving/sending funds from/to such regions; receiving/sending funds from/to regions in armed conflict or war or from/to third countries with identified strategic weaknesses in their national AML/CFT regimes; raising funds through the so-called crowdfunding or using virtual assets; and, carrying out activities that require contact with persons vulnerable to radicalisation or residing in regions with such activity.

(c) Several legislative changes were made to ensure the flexibility of legal obligations for NPOs as obliged entities (OEs), as well as introducing some elements of risk-based approach. In 2016 legislative changes were made in LNPLP to strengthen administrative sanctioning mechanism of NPOs that are subject to TFS or are reasonably believed to be carrying out activity in furtherance of terrorism. A review of the adequacy of measures, including laws and regulations was carried out in 2023 NPO TF Risk Assessment identifying that under the applicable Bulgarian legislation that a number of mechanisms ensure monitoring of the activities NPO sector.

(d) Provision to conduct and update the assessment of NPO sector in relation of terrorist financing risks is set in Article 96 of the LMML. The assessments shall be updated within the period of 3 years and be included in the NRA. (Article 95 Par. 1, Article 96 Par. 7 of LMML).

3. ***Criterion 8.2***

(a) Bulgaria has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs. The LNPLP sets the prerequisites for the foundation, the organization, financial management, and the dissolution of an association/foundation. Besides, NPOs operating in the country have annual reporting obligations. As envisaged in the Art. 6 (1) of LNPLP the legal capacity of NPOs originates from their registration in the register of non-profit legal persons (Art. 6, para 1 of the LNPLP). The register is kept by the Registry Agency to the Minister of Justice (Art. 17 of the LNPLP). According to the Art 38 (1) (2) of the Law on Accountancy the NPOs are obliged to publish their annual financial statements, consolidated financial statements and annual reports. Besides, NPOs operating for public benefit are also subject to statutory independent financial audit (Art. 37).

(b) NPOs that fall within the FATF definition are OEs under the Bulgarian legal framework. In 2020 the Bulgarian Centre for Non-Profit Law with the support of FID-SANS organized 4 workshops and consultations for NPOs with regard to AML/CFT matters, including measures that would protect NPOs from TF abuse. Following the 2023 NPO TF Risk Assessment, focus of outreach include potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks. Targeted workshop, live round table, online trainings were dedicated to NPOs and donor community. At the same time, the online availability of the NRA and the 2023 NPO TF Risk Assessment Report outcomes as well as other information regarding the NPOs (through the Commercial Register and Register for non-profit legal persons), leaflet on the risks of TF abuse for the NPO sector in Bulgaria with recommendations for preventing TF abuse provide access of the NPOs and donor community to relevant materials.

(c) FID-SANS together with the Bulgarian Centre for Non-Profit Law developed a Methodology and Criteria for Risk Assessment for NPOs, which is considered to be a useful tool helping NPOs to identify, understand and assess the risk of their activity being used for the purpose of ML/TF. FID-SANS and BCNL cooperated on the 2023 NPO TF Risk Assessment and on outreach and educational programmes relevant to NPO sector. The cooperation with BCNL included also other areas, such as capacity building within NPO sector, identification of BOs, which would per se in general also address TF risks and vulnerabilities.

(d) According to the Art. 3 of the Law on Limitation of Cash Payments, payments in the territory of Bulgaria shall be made only via bank transfers or deposits to payment accounts when the value of the payment is equal or in excess EUR 5000, as well as linked payments below the mentioned amount if total value is equal to or exceeds EUR 5000. Bulgaria encourages NPOs to conduct transactions via regulated financial channels in awareness-raising outreach seminars, as well as using publicly available leaflet on the risks of TF abuse for the NPO sector.

4. **Criterion 8.3** - NPOs that fall within the FATF definition are OEs according to the Art. 4(28) of LMML with limited obligations under the LMML. FID-SANS is the competent authority to supervise and monitor the level of implementation the relevant requirements by NPOs. Bulgaria has identified NPOs falling under the FATF definition and from those NPOs, the subset that are likely to at risk of TF abuse. Besides, NPOs are required to be registered, maintain accounting information, publish reports and etc. According to the Art. 78(1) of the Accounting Act, the National Revenue Agency monitors the compliance with the accountability requirements. FID-SANS and the National Revenue Agency carry out the supervision or monitoring of NPOs applying risk-based approach: Bulgaria has established a joint risk-based monitoring mechanism between FID-SANS and the National Revenue Agency, targeting only those NPOs identified as being at risk of terrorist financing abuse based on sectoral risk assessments. Oversight activities, including checks and inspections, are proportionately focused on higher-risk NPOs, while lower-risk entities are primarily subject to outreach and awareness-raising measures.

5. **Criterion 8.4**

(a) FID-SANS is the competent authority to supervise and monitor the level of compliance of NPOs with the relevant requirements, including the risk-based measures being applied to them by issuing mandatory instructions following inspections, monitoring their implementation, and conducting targeted outreach and training activities to address identified TF risks and vulnerabilities. In addition, the National Revenue Agency monitors the compliance with the accountability requirements, including the risk-based measures being applied to them through risk-based on-site and off-site checks of NPOs identified as being at risk of TF abuse, integrating TF risk indicators into its oversight activities and sharing results with SANS for further action where necessary.

(b) Only NPOs that fall within the FATF definition are OEs. Thus, the sanctions as envisaged by the LMML apply to them, as well as persons acting on their behalf (see R.35). In addition, under the Law on the Commercial Register and the Non-Profit Legal Entities Register breaches of registration requirements are liable to fines (approximately EUR 500- 2500). In addition, the National Revenue Agency applies sanctions for breaches of the Accounting Act, particularly in relation to submitting and publishing financial statements (approximately EUR1000-2500). Moreover, NPOs may also be dissolved in case they are listed under Art. 5 of LMFTPWMD. More severe measures, including administrative-penal sanctions and dissolution, are primarily linked to NPOs identified as being at risk of TF abuse. These are considered to be proportionate and dissuasive sanctions.

6. **Criterion 8.5**

(a) There are mechanisms in place for co-operation, co-ordination and information sharing with regard to combatting terrorism financing as envisaged in the LMFTPWMD. The SANS and FID-SANS play vital roles in these processes. The mentioned mechanisms would per se include also co-operation, co-ordination and information sharing in respect of NPOs. Besides, the information contained in the Register of non-profit legal entities is also public.

(b) The investigation of terrorism-related offences (including TF), including NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations is the responsibility of and ensured by the following authorities: the State Agency for National Security (pre-investigative stage) and the Ministry of Interior (investigative stage). The latter have the wide range investigative expertise and capability to examine also NPOs at stake.

(c) Full information on the administration and management of NPOs is accessible in a timely manner, given that relevant information is stored publicly and is easily accessible through the Register of Non-Profit Legal Persons. The access to financial and programmatic information not contained in the Register of Non-Profit Legal persons and is regulated under CCP (please refer to R. 9 and 31).

(d) Bulgaria has in place a legal framework to ensure that information is shared between competent authorities. According to Art. 9 of LMFTPWMD any person, including state bodies, who knows that given financial operations or transactions are intended to finance terrorism, shall be obliged to notify immediately the MoI and the Chairperson of the SANS. In addition, Art. 9a of LMFTPWMD envisages that supervisory authorities provide information on any findings related to terrorism financing to the MoI and SANS immediately, as well as FID-SANS and vice versa.

7. **Criterion 8.6** – Bulgaria uses the general procedures and mechanisms for international cooperation to handle requests relating to NPOs. International requests for information regarding particular NPOs that are suspected of TF or other forms of terrorist support are dealt with by MOJ in the case of MLAs or the FID-SANS in the case of requests received from other FIUs. Besides, all LEAS may also rapidly exchange information with their counterparties through International Operational Cooperation Directorate (IOCD) of the Ministry of Interior and vice versa.

Weighting and Conclusion

8. **R.8 is re-rated as C**.

Recommendation 13 – Correspondent banking

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	C ↑ (upgrade requested, upgraded)

1. In the 2022 MER, Bulgaria was rated PC on R.13 and the same rating remained in 2024 FUR since Bulgaria met some of the requirements for correspondent banking, however c.13.(a) requirements applied to respondent institutions from EU/EEA Member States only when a higher risk was identified. Bearing in mind the materiality of correspondent relationships with EU/EEA Member States, these were considered as moderate shortcomings.

2. **Criterion 13.1** – Art. 44(1) of the LMML (Amended, SG No. 49/2025) requires OEs (including FIs), to apply the following measures before establishing cross-border correspondent relationships (correspondent relationships with respondent institution from another country):

(a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of the supervision, including whether it has been subject to money laundering/terrorist financing (ML/TF) investigation or supervisory measures (regulatory actions) (Art. 44(1)(2) of the LMML).

(b) Assess the respondent institution's AML/CFT controls (Art. 44(1)(3) of the LMML).

(c) Obtain approval from senior management before establishing new correspondent relationships (Art. 44(1)(4) of the LMML); and

(d) Define and document the respective AML/CFT responsibilities of each institution (Art. 44(1)(5) of the LMML).

3. **Criterion 13.2** – Art. 44(2) of the LMML (Amended, SG No. 49/2025) states that, where third parties who are customers of the respondent institution also have access to the payable-through account:

(a) OEs must be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to the accounts of the OE; and

(b) OE must be satisfied that the respondent institution is able to provide relevant due diligence data immediately upon request.

4. **Criterion 13.3** – Art. 45(1) of the LMML prohibits OEs from establishing correspondent relationships with shell banks. In cases where a correspondent relationship with a shell bank has been established, the OE must immediately terminate such relationship. Art. 45(3) prohibits the OEs from establishing and maintaining correspondent relationship with an institution outside Bulgaria that allows its accounts to be used by shell banks.

5. Art. 45(2) of the LMML states that when establishing correspondent relationships with institutions from other countries, OEs shall collect sufficient information about the respondent institution to ensure that the respondent institution does not allow its accounts to be used by shell banks.

Weighting and Conclusion

6. All criteria are met. **R.13 is re-rated C.**

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	LC ↑ (upgrade requested, upgraded)

1. In the 2022 MER, Bulgaria was rated PC on R.15. The assessment identified some technical deficiencies related to assessment of the risk of new technologies; coverage of the virtual assets service providers (VASP) activities; application of fit and proper measures; application of preventative measures by VASPs; application of measures related to implementation of TF and PF-related TFS; and international cooperation.

2. During the follow-up period Bulgaria ensured that all the VASP activities and operations defined by the FATF Standards are regulated. However following deficiencies remained: (i) the lack of holistic risk assessment by the country when analysing new technologies-related risks, which also did not explicitly cover the use of developing technology (c.15.1);(ii) apart from the general requirement to mitigate the risks, there was no explicit reference to take appropriate measures to manage and mitigate the risks that specifically target new products and new business practices, new delivery mechanisms (c.15.2(b)); (iii) there were no legal provisions that would prevent criminals' associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP(c.15.4(b)); (iv) no proactive actions were taken by the authorities to identify natural or legal persons carrying on VASP activities without a prior registration (c.15.5); (v) there were no legal provisions enabling restriction or suspension of a VASP's registration (c.15.6(b)); (vi) no VASP specific AML/CFT guideline was issued (c.15.7); (vii) shortcomings identified under R. 7, (c.7.2I, 7.3, c.7.4(d)), 10, 13, 16, 20,34, 35, R.37 – R.40 applied to VASPs. Cumulatively these were considered moderate deficiencies in light of the growing materiality of the sector.

3. **Criterion 15.1** –

At a national level, Art. 96(1)(2) of the LMML (amended by SG No. 49/2025) provides a requirement for conducting and updating an assessment of the potential ML/TF risks arising from the introduction of new products, business practices and delivery mechanisms, as well as the use of new or developing technologies in new or pre-existing products, business practices and delivery mechanisms. Bulgaria has taken steps to analyse new technologies-related risks during its 2023 NRA exercise. The analysis is covered under specific topics, rather than as a holistic risk assessment on the topic, which is considered to be a minor shortcoming. For example, it is covered in: (i) Chapter 3 – subsections Frauds, Including Investment and Computer Frauds, drug trafficking, Assisting the Process of Money Laundering and "Professional Launderers" and National Money Laundering and Terrorist Financing Vulnerabilities; (ii) Chapter 5 – ML risk assessment by economic sectors, subsection on information technology (IT) and electronic money; (iii) Chapter 6 – ML risk assessment in financial sector and DFNBPs sector and subsection on e-money; (iv) Chapter 7- Cross-border risks; and (v) Chapter 8 – TF risks assessment.

Under Art. 48a(1) of the LMML (amended by SG No. 49/2025), OEs are required to take appropriate actions to identify and assess the potential risks of ML/TF arising from the introduction of new products, new business practices and new delivery mechanisms, as well as from the use of new or developing technologies for new or pre-existing products, business practices and delivery mechanisms.

4. **Criterion 15.2**

(a) Art. 48a (2) of the LMML (amended by SG No. 49/2025) requires OEs to assess the risks before the introduction of new products, new business practices and new delivery mechanisms, as well as before the use of new technologies for new or pre-existing products, business practices and delivery mechanisms.

(b) Art. 48b of the LMML (amended by SG No. 49/2025) requires Oes to take appropriate measures to manage and mitigate the identified risks of ML/TF arising from the introduction of new products, business practices and delivery mechanisms, as well as from the use of new or developing technologies in new or existing products, business practices and delivery mechanisms. OEs have to take enhanced measures where new technologies-related risks are assessed as high as part of the NRA or business risk assessment (BRA) process or based on the results of the OE's internal ML/TF risk assessment (Art. 35(5) of the LMML); and apply enhanced CDD consistent with the risk where a high risk of ML/TF is identified (Art. 30(7) of the RILMML).

5. **Criterion 15.3**

(a) At EU level, the European Commission identifies and assesses the risks emerging from virtual assets and the activities and operations from VASPs in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Art. 6) . The EU level risk assessment shall be updated by a report at least every two years.

At the national level, In February 2023 Bulgaria completed a Sectoral assessment of ML/TF risks related to VAs and VASPs which constitutes a comprehensive analysis of ML/TF threats, vulnerabilities, inherent risk factors associated with VA/VASPs based on the following components: (i) review of contextual factors affecting the VA ecosystem; (ii) measurement of the materiality of the VA and VASP sector in Bulgaria, including products and services involving VAs and VASPs in non-VASP regulated sectors (such as financial institutions and designated non-financial businesses and professions (DNFBPs)); (iii) analysis of the regulation and legal framework relevant to VAs/VASPs; (iv) review of the supervisory practice by FID-SANS; (v) analysis of the threats stemming from predicate offences, which serve as the main source for generating criminal proceeds for the VA ecosystem, as well as TF threat analysis; (vi) vulnerability analysis from legislative, operational and risk awareness perspective; (vii) analysis of customers and user profiles involved in VA and VASP-related crimes; (viii) analysis of other (non-VASP) economic sectors involved in the use of VAs; and (ix) analysis of VAs products and VASPs services.

The findings from each of these components were cross-analysed and integrated to produce a matrix or risk scenarios for Bulgaria in four risk assessment sections.

(b) Art. 96 and Art. 97 of LMML and Art. 59 of RILMML requires that at the national level the results of the NRA which also include assessment of risks related to VASPs and VAs be used to mitigate the identified risks.

Bulgaria adopted a strategy for countering ML and TF (2023-2027) which among others establishes priorities and defines key actions based on: (i) the 2023 NRA; (ii) Sectorial Assessment of ML/TF risks related to VAs and VASPs (February 2023). One of the main purposes of the Strategy is to properly allocate resources to areas where higher ML/TF risks are identified.

The Action Plan for the implementation of the Strategy was approved on 23 November 2023 by the Council for Coordination and Cooperation and subsequently adopted by the Council of Ministers (Council of Ministers Decision No. 66 of 31 January 2024).

(c) VASPs are required to identity, assess, manage and mitigate risks in line with the requirements analysed under c.1.10 and c.1.11.

6. **Criterion 15.4** –

(a) While this part of the criterion was met in the FUR 2024, the legal framework in Bulgaria has since been updated in line with the EU Regulation 2023/1114 (MiCAR). A person providing crypto[6] asset services within the EU is subject to prior authorisation (Art. 59 of the MiCAR) by the authority of the Member State where it has its registered office. The Financial Supervision Commission (FSC) is the national competent authority in Bulgaria responsible for the licensing (authorisation) of crypto-asset service providers under MiCAR (Art. 3(1), 14 of the Law on Markets in Crypto-Assets (LMCA)), except in cases falling within the exclusive competence of the Bulgarian National Bank (BNB) (namely, when credit institution provides crypto-asset services, issues electronic money tokens and/or asset referenced tokens (Art. 2(2) of the Law on Credit Institutions (LCI)), or electronic money institution issues electronic money tokens (Art. 182a(1) of the Law on Payment Services and Payment Systems (LPSPS)). A crypto-asset service provider under the MiCAR 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) of the MiCAR). 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). The previously applied legal provisions on registration of VASPs (legal and natural persons) (Art. 9a of the LMML) have been repealed by SG No. 54/2025 and no longer allow for new registrations as of 8 July 2025 (Art. 4 and 5 of the Transitional and Final Provisions of the LMCA).
However, the VASPs previously registered in the VASP registry maintained by the National Revenue Agency may continue to carry out the activity they have been registered for without authorisation until 1 July 2026 or until the grant or refusal of authorisation pursuant to Article 63 of the MiCAR, whichever comes first (Art. 3 of the Transitional and Final Provisions of the LMCA), and remain OEs until 1 July 2026 (Art. 4(38), 4(39) of the LMML, amended by SG No. 54/2025).

(b) Authorisation requirements applied to crypto-asset service providers include 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 of the MiCAR). These provisions empower authorities to prevent individuals convicted of offences relating to ML/TF or of any other offences that affect their good repute from

[6] In the terminology of the EU Regulation 1114/2023 (MiCAR) '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.

assuming relevant functions. Regarding members of the management body, as well as shareholders and members, whether direct or indirect, that have qualifying holdings, proof of the absence of a criminal record and sufficiently good repute is required (Art. 62(2)(h) and 62(3) of the MiCAR). The LMCA further clarifies that reliability and suitability of members of the management body, shareholders or persons who have a direct or indirect qualifying holding in the crypto-asset service provider is assessed based on the information collected about them and their associates, as well as the links between them (Art. 17(2)(9) of the LMCA).

7. **Criterion 15.5** –The LMCA prescribes appropriate sanctions for CASPs that provide services without the requisite license (authorization): immediate cessation of the activity (Art. 32), blocking websites (Art. 35a), blocking apps, deleting domain names, disabling accounts (Art. 36). The fines are applicable to both natural and legal persons, whereby the fines amount (Art. 37).

8. For natural persons: fine from BGN 1400 (approximately EUR 700) to BGN 700 000 (approximately EUR 350 000), and, for a repeated violation – from BGN 2800 (approximately EUR 1400) to BGN 1 400 000 (approximately EUR 700 000).

9. For legal persons: fine from BGN 25 000 (approximately EUR 13 000) to the higher amount between BGN 5 000 000 (approximately EUR 25 000 000)and 2.5 per cent of the annual turnover of the legal person, and, for a repeated violation – from BGN 50 000 (approximately EUR 25 000)to the higher amount between BGN 10 000 000 (approximately EUR 5 000 000)and 5 per cent of the annual turnover of the legal person.

10. Regulation at EU level prohibits the provision of services without authorisation (Art. 59 (1) MiCAR). EU Directive 2015/849 and MiCAR 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. MiCAR, 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 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 authorization requirement (Article 110 MiCAR). Violations of licencing requirements shall be communicated through the preparation of a dedicated report to the Deputy Chairperson of the FSC in charge of the Investment Activity Supervision division.

11. The range of fines that is available can be applied proportionately to greater or lesser breaches of requirements.

12. In line with Strategy for monitoring Fintech sector 2025 – 2027, Bulgaria has taken actions with targeted aim to identify natural or legal persons that carry out CASP activities without the requisite license: information campaigns to consumers, reviews of information from national and foreign authorities, searches of adverse media. These measures are already being implemented, while interagency activities, such as databases cross-checks, have been planned to be carried out on a regular basis, taking into account the applicable legal timelines for the availability of tax data.

13. **Criterion 15.6** –

(a) VASPs and CASPs are subject to AML/CFT requirements and are supervised by FID-SANS (Art.108 of the LMML and Art. 14a of the LMFTPWMD), FSC (with respect to CASPs). The provisions of Art. 114 of the LMML (SG No. 49/2025) provide a legal basis for a risk-based supervision of VASPs and CASPs. Relevant risk factors, characteristics of the OE or group and information collected by supervisory authorities to assess and understand the ML/TF risk the OE is exposed to are used for planning supervisory activities, including making decisions on the scope, depth, duration and frequency of the on-site inspections proportionate to those risks. In addition, Art. 115(3) of LMML prescribes that the results of the NRA shall be taken into consideration when applying the risk-based approach to supervision. Ongoing monitoring and periodic reviews of risk assessments, including upon the occurrence of essential circumstances or changes in the OE management and activities (to ensure that the risk assessment and resource allocation are current, applicable and relevant) are required by Art. 114, paragraph 1, item 4 of LMML. When assessed for market entry, crypto asset service providers are required to have mechanisms and controls in place that ensure compliance with AML/CFT requirements (MiCAR, Art. 63 (2) to (10)).

FID-SANS has internal manuals in place for carrying out on-site and off-site inspections, whereby inspections are carried by taking into account (inter alia): (i) NRA; (ii) sectoral risk assessment related to VAs and VASPs; and (iii) FID-SANS data on the number of received STRs and their quality by sectors. The risk of individual OE is evaluated by FID-SANS during the off-site monitoring process, based on the collected information.

FID-SANS conducts two types of inspections. Off-site inspections (or so-called remote checks) include reviews of internal documents, rules, policies, own risk assessment and matrix of the inspected OE. On-site inspections are conducted based on the scope outlined in the inspection plan. Follow-up actions are also carried out, whereby the inspected OE is requested to develop and provide to FID-SANS an action plan for addressing the identified deficiencies, if there are any.

(b) EU Directive 2015/849 and MiCAR task competent authorities in member states to ensure compliance by crypto asset service providers with requirements to combat money laundering and terrorist financing. MiCAR, 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 crypto asset service providers is regulated at EU level in Art. 64 of MiCAR and, alongside other administrative penalties and administrative measures, shall also be implemented at national level (MiCAR, Art. 111). FID-SANS is authorised to carry out on-site and off-site inspections of VASPs and CASPs, FSC – of CASPs (see c.15.6(a)) regarding the application of AML/CFT requirements. Compulsion of information is required by Art. 109 of the LMML and Art. 14a of the LMFTPWMD.

FID-SANS, FSC have powers to: (i) apply remediation measures such as ordering a VASP, a CASP to cease a violation, to take specific measures necessary for remedying the violation and set a time limit for taking such measures (Art. 126 of LMML and Art. 14a of LMFTPWMD; (ii) impose sanctions on VASPs and CASPs, their managers and representatives for AML/CFT breaches (Art. 123(1) of LMML and Art. 16(1) of LMFTPWMD); (iii) in case of serious or systematic violations, forbid a natural person from holding a senior management position (Art. 124 of LMML and Art. 15(7) of LMFTPWMD); and (iv) in cases of repeat violations (under the terms established at Art. 116(2)) or serious or systematic violations at Art. 116(3) of the LMML, to withdraw authorisations for licence or registration. Both FID-SANS and FSC have power to withdraw, restrict or suspend the VASP's license or registration, where applicable (Article 125 of LMML, Article 18 of LMFTPWMD).

14. **Criterion 15.7** –In 2023 FID-SANS issued guidance (Guidance on Measures against TF, Guidelines related to customer risk assessments, and Guidelines related to PEPs) which are relevant to all OEs, including VASPs and CASPs. 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). EBA Guidelines on ML/TF risk factors are applicable to all OEs, including VASPs and CASPs. In 2024 FID-SANS issued guidelines on implementing anti-money laundering and countering the financing of terrorism (AML/CFT) obligations for VASPS and CASPS containing sector specific ML/TF risk indicators, reporting a suspicion.

15. **Criterion 15.8** –

(a) EU Directive 2015/849 and MiCAR 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 MiCAR stipulates sanctions for a number of infringements including minimum fines. Range of proportionate and dissuasive criminal and administrative sanctions are applicable to VASPs and CASPs in cases of violation of AML/CFT requirements (c.35.1).

(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 MiCAR, Art. 111, shall also apply to members of the management body of a crypto-asset service provider. Sanctions are applicable to directors and senior management (c.35.2).

16. **Criterion 15.9** – Shortcomings under Recommendations 16 and 20 apply here. When weighting the shortcomings, the risk and materiality of the VASP sector is taken into consideration. A progress was demonstrated with: (i) c.10.9-10 and c.10.16, which rectified the issues by the adoption of amendments to LMML, namely repealing the exemption for customer verification (repealed Art. 54(11) of the LMML), clarifying the requirements regarding identification of persons who exercise control via other means (Art. 59(5) of the LMML) and CDD applied to existing customers (Art. 16(2) of the LMML); (ii) R.13 (see c.13.1 for details).

(a) According to Art. 11(5) of LMML, for the occasional transactions with crypto assets the designated threshold where CDD is applicable for VASPs amounts to or exceeds EUR 1 000 or the equivalent in another currency.

(b) The EU Regulation 2023/1113 (TFR) repeals and replaces the 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 (crypto assets) and is directly applicable in Bulgaria. VASPs and other FIs are subject to the TFR when conducting virtual asset (crypto asset) transfers as set out in Article 2 of the TFR:

(i) The TFR requires an originating institution to obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, and submit such information in advice of, simultaneously or concurrently with, the transfer of crypto-assets in a secure manner. Art. 14(1) of the TFR requires the originating crypto-asset service provider to obtain originator and beneficiary information (Art. 14(1), (2) and (3) of the TFR) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Art. 14(4) of the TFR). Before transferring crypto assets, the service provider shall verify the accuracy of the originator information (Art. 14(6) of the TFR). Crypto-asset service provider of the originator must retain records of the originator and beneficiary information for a period of five years (Art. 26(1) of the TFR) and the information has to be provided to competent authorities responsible for AML/CFT upon request (Art. 24 of the TFR).

(ii) Art. 16 of TFR requires the crypto-asset service provider of the beneficiary to implement effective procedures, including, where appropriate, monitoring after or during the transfers, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (Art. 16(1) and (3) of the TFR). Crypto-asset service provider of the beneficiary must retain records of the originator and beneficiary information for a period of five years (Art. 26(1) of the TFR) and the information has to be provided to competent authorities responsible for AML/CFT upon request (Art. 24 of the TFR).

(iii) The TFR covers the requirements of Recommendation 16 and applies them to virtual asset (crypto asset) transfers, including on monitoring of the availability of information

(Art. 14(8) and Art. 16 (1) of the TFR) as well as freezing action and prohibiting transactions with designated persons and entities (Art. 23 of the TFR).

(iv) FIs are covered by the scope of relevant provisions of the TFR through the broad definition of crypto-asset service provider in Art. 3(1)(15) of the TFR, with reference to Art. 3(1)(15) of the MiCAR, including FIs that provide crypto-asset services in accordance with Art. 59, 60 of the MiCAR.

17. Additionally, Art. 3(3) of the Transitional and Final provisions of the LMCA explicitly requires VASPs which remain operating in Bulgaria without authorisation under MiCAR (see c.15.4.a for details) to apply the requirements of the TFR when transferring crypto-assets.

18. **Criterion 15.10** – With respect to targeted financial sanctions (TFS), the relevant elements described under Recommendations 6 and 7 apply to VASPs, including those related to communication, reporting and the provision of guidance to obliged entities. At EU level, the communication and publication of listings and de-listings relating to both terrorist financing and proliferation financing are ensured through directly applicable Council Regulations and publication in the Official Journal of the European Union. At national level, the LMFTPWMD (amended by SG No. 49/2025) requires competent authorities to issue guidance on the implementation of measures against the financing of terrorism and proliferation, as well as the conditions for suspension. "Guidance on implementation of the measures against financing of terrorism and financing of proliferation" (2023) has been updated in accordance with the amendments and supplements to the LMFTPWMD (amended by SG No. 49/2025).

19. **Criterion 15.11** – MiCAR, Art. 107, expressly provides that competent authorities should, where necessary, conclude cooperation 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. MLAs, extradition, international co-operation in relation to money laundering, associated predicate offences and terrorist financing is applicable relating to virtual assets, FID-SANS and FSC have a legal basis for exchanging information with their foreign counterparts. Remaining minor deficiencies under R.38 to R.40 apply to this criterion.

Weighting and Conclusion

20. Bulgaria requires the risk assessment of new technology and services when launching the products, business practices and delivery mechanisms, as well as the use of new or developing technologies in new or pre-existing products, business practices and delivery mechanisms. The VASP sector is regulated and subject to AML/CFT obligations, registration and licensing requirements, range of sanctions are applicable to VASPs and CASPs in cases of violation of AML/CFT requirements. Remaining minor deficiencies under R.16, R 20, R.38-40 continue to be of relevance under this recommendation. **R.15 is re-rated as LC**.

Recommendation 35 – Sanctions

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	LC ↑ (upgrade requested, upgraded)

1. In 2022 MER, Bulgaria was rated PC on R.35. Moderate shortcomings were identified: (i) Criminal Code did not provide for more dissuasive penalties for *more serious* crimes; (ii) Criminal Code applied only to the LMML violations and not to the LMFT violations; (iii) the FSC is not able to restrict (as opposed to revoke) a licence; (iv) the FSC was only able to revoke licence regarding the LMML

violations and not for the LMFT violations, however, there were no powers to revoke a license of an AIM; (v) the FSC had no legal basis for issuing written warnings or orders to address violations; (vi) the NaRA (regarding gambling) had no legal basis to sanction other than imposition of administrative financial penalties; (vii) monetary penalties applicable to directors and senior management were not fully dissuasive; (viii) sanctions for non-compliance with the TFS related to TF requirements did not appear fully dissuasive, especially with respect to maximum amount of fine applicable to OEs; (ix) no sanctions were available for non-compliance with TFS related to PF.

2. **Criterion 35.1 -** A range of criminal and administrative sanctions is available to deal with natural or legal persons that fail to comply with AML/CFT requirements.

For breaches of TFS obligations (R.6)

Art. 15 of the LMFTPWMD provides proportionate and dissuasive administrative sanctions for TFS related both to TF and PF violations up to EUR 1 500 000 for natural persons and up to same amount or up to twice the benefit gained for legal persons; and for OEs up to EUR 7 500 000 or 10% of annual turnover.

For breaches related to NPOs (R.8)

For breaches related to NPOs (R.8), there is a range of proportionate and dissuasive sanctions available as described under c.8.4(b).

For breaches of preventive measures and reporting obligations (R.9-23)

For breaches of preventive measures and reporting obligations (R.9-23) under the LMML and the LMFTPWMD, a range of proportionate and dissuasive sanctions is available which may be imposed by the relevant supervisors. Available sanctions range from warnings, the right to restrict, suspend or revoke the license, respectively to suspend, terminate or delete the registration, or to revoke the issued authorization or certificate for carrying out individual transactions or actions of the person in cases of repeat violations (LMML, Articles 116(2), (3) and 124; LPSPS, Art. 169(1); LMFTPWMD, Art 18; MFIA, Art. 276(2); Insurance Code Art. 40(2)1; CISOUC Art. 264 (1) 4, 8 (9); Gambling Act, Articles 85 (1) and (2) and 86; PSA, Art. 57 and CRC, Art. 58) to administrative penalties and criminal sanctions (LMML, Chapter 10, particularly Articles 116 and 118). Administrative penalties range from up to EUR 1 500 000 for natural persons and up to the same amount or up to twice the benefit gained for legal persons; and for OEs up to EUR 7 500 000 or 10% of annual turnover. Criminal sanctions include (Art. 253b of the Criminal Code) in cases of significant impact, imprisonment for up to three years and a fine from EUR 500 to EUR 1500, unless the deed does not constitute a more serious crime in case of which more severe sanctions apply depending on the act committed (e.g. the punishment shall be imprisonment for one to eight years and a fine up to EUR 10 000).

3. **Criterion 35.2** – Administrative sanctions applicable to directors and senior management are listed under Art. 116a (5), Art. 117(1), Art. 119(1) and Art. 120(3) of the LMML and Art. 15(4) of the LMFTPWMD. The provisions apply to any person who manages and represents an FI/DNFBP covered under the LMML and the LMFTPWMD, as well as to persons responsible for, or exercising, the internal controls over AML/CFT compliance. Across all levels of infringement severity, the legislation provides for higher maximum administrative fines applicable to directors and senior management under Arts 117, 119 of the LMML and Art. 15 (4),(5) of the LMFTPWMD, compared to those applicable to non-management natural persons (Arts 116, 118 of the LMML; Art. 15 (1)-(3) of the LMFTPWMD).

4. Arts. 117 and 119 of the LMML establish direct personal administrative liability of directors, senior management and persons responsible for internal control for AML breaches, while Art. 15 (4)-(5) of the LMFTPWMD provides for direct personal liability for TF/PF breaches, with fines escalating for repeated and serious/systematic violations and reaching levels up to EUR 7,5 million, depending on the category of obliged entity, and, in most instances, are 33-50 % higher than those applicable to non-management natural persons.

5. Article 116a of the LMML (new, SG No 84/2023, SG No 54/2025) introduces administrative sanctions for the performance of TCSPs and safekeeping activities without required registration as well as for failures to declare changes to registration. The same fines are applicable to directors, senior management and persons responsible for internal control (Art. 116a (5)), and a differentiated sanctioning approach for them is not established. Having regard to the country's identified risks relating to laundering funds through the extensive use of cash, shell companies, the absence of the differentiated sanctioning levels for ordinary and senior managerial/control personnel is considered a deficiency.

6. In addition, persons who have been issued an administrative sanction for serious and repeated violations are prohibited from occupying a senior management role for a period of 3 months or 1 year (Art. 124(1) and 124(2) the LMML and Art. 15(7) the LMFTPWMD.

Weighting and Conclusion

7. Minor deficiency remains in respect of breaches which concern the performance of specific TCSP and safekeeping activities without the relevant registration, as a differentiated sanctioning approach for directors and senior management is not established (c.35.2). **R.35 is re-rated as LC.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)
FUR2	2025	PC (no upgrade requested)
FUR3	2026	LC ↑ (upgrade requested, upgraded)

1. In 2022 MER, Bulgaria was rated PC on R.38. Shortcomings identified were following: (i) deficiencies identified in c.4.1(b), c.4.1(c) and c.4.4 of R.4 were applicable in context of international cooperation; (ii) provisional measures pursuant to Art. 72 CPC could not be applied if the perpetrator was unknown or has dead; and, (iii) Bulgaria had no specific measures in place to regulate the possibility of arrangements for coordinating seizure and confiscation actions with other countries.

2. ***Criterion 38.1*** – Bulgaria has the authority to take expeditious action in response to foreign requests for assistance to identify, freeze, seize and confiscate criminal assets:

(a) Laundered property from - through the measures provided for in the Bulgarian laws and described under R. 4 which equally are available upon request of a foreign country as for local proceedings; for EU countries through *EU Regulation 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders*; and, for non-EU countries through the general rules on mutual legal assistance (MLA) in CPC, Chapter 36 as well as relevant Ministry of Justice order No. LS-04-115/03.04.2023 and).

At EU level, EU Regulation 2018/1805provides for the mutual recognition, between EU member states, of freezing and confiscation orders resulting from proceedings in relation to a criminal offence includes freezing and confiscation orders that apply to property that is held in the name of or owned by non-bona fide third parties. EU Regulation 2018/1805 does not provide for the recognition of requests for investigative measures or non-criminal seizure of assets. Whether "freezing" also extends to cover situations in which competent authorities take physical control of an asset is an issue to be determined by the law of the member state. For orders that concern criminal offences with a maximum penalty of at least 3 years imprisonment, and which are also listed in Article 3 of the Regulation (which mirrors the offences set out in the FATF definition of "designated categories of offences"), the order should be executed without verifying dual criminality. Otherwise, the member state can verify that dual criminality exists. Recognition and execution of freezing and confiscation orders should occur without delay.

For non-EU countries, the general rules of MLA in Chapter 36 of the CPC apply. As for the receipt and execution of foreign seizure and freezing orders, Chapter 36 contains no specific procedural rules beyond the general provisions governing MLA in Art. 471 which is in stark contrast with the detailed procedures in the aforementioned EU (based) legal instruments. There is an order of the Ministry of Justice in place, governing the organisation of the work and the document management, but in this order, there are no specific rules in the field of detection, seizure and confiscation. Dual criminality is not required by the CPC but, indirectly, by other international instruments in this field such as the 1959 European Convention on MLA (by means of a reservation made by Bulgaria).

Execution of foreign (non-EU) confiscation orders is provided by Art. 469 of the CPC which renders such orders executable pursuant to the general rules of recognition and enforcement of sentences issued by a foreign court, a formal court procedure with its respective deadlines (Art. 465). For the execution of a foreign confiscation order, dual criminality is required (Art. 463).

In accordance with Articles 53 and 253(6) of the CC, laundered property, proceeds, instrumentalities used in, and instrumentalities intended for use in a crime (or equivalent) can be confiscated. In cases of ML the object of crime or the property into which it has been transformed shall be forfeited to the benefit of the state, and where absent or alienated, its equivalent shall be awarded. In accordance with Art. 72 of the CPC, the Bulgarian court imposes security for the fine, confiscation and confiscation of property in favour of the state. This procedure is applied both in the pre-trial proceedings and for the laundered items, the benefits, the used funds and the funds used for ML/TF, as well as for securing the assets in order to return them to the legal owner.

(b) Proceeds from, (c) instrumentalities used in, or (d) instrumentalities intended for use in, ML, predicate offences or TF, or (e) property of corresponding value; can be identified, seized and restrained using the same mechanisms as set out in criterion 38.1(a).

3. ***Criterion 38.2*** – The confiscation measures under Art. 53 CC apply irrespective of criminal liability and can thus be imposed also in lack of conviction (e.g., in case of the death of the perpetrator/ perpetrator was unknown). The measures to secure forfeiture of objects to the benefit of the state set forth in the Code of Civil Procedure also apply in criminal procedures (CPC, Art. 72).

4. ***Criterion 38.3*** – Bulgaria has:

(a) Arrangements for co-ordinating seizure and confiscation actions with other countries through general provisions of the CPC which however do not contain specific measures, and through the EU Regulation 2018/1805, according to which it is mandatory to recognise and enforce the freezing and confiscation order of another EU member state, unless the executing authority invokes one of the grounds for non-recognition and non-execution. This means that there is de facto reliance on the findings of fact in the foreign order;

(b) Mechanisms for managing, and when necessary, disposing of, property frozen, seized or confiscated with minor gaps as noted under c.4.4.

5. ***Criterion 38.4*** – Confiscated assets can be shared with other EU countries (Recognition of Orders Act Art. 28; and EU Regulation 2018/1805, Art.30) and with non-EU countries under bilateral MLA treaties.

Weighting and Conclusion

6. Remaining shortcomings are: (i) there are no specific measures in place to regulate the possibility of arrangements for coordinating seizure and confiscation actions with non-EU countries (c.38.1); (ii) there are no specific rules for sharing the confiscated or forfeited property with non-EU countries (c.38.3(a)). These shortcomings are considered minor. Consequently, **R.38 is re-rated LC.**

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

Recommendations	Rating	Factor(s) underlying the rating[7]
4. Confiscation and provisional measures	~~PC (MER)~~ C (FUR 2026)	
5. Terrorist financing offence	~~PC (MER)~~ C (FUR 2026)	
7. Targeted financial sanctions	~~PC (MER)~~ C (FUR 2026)	
8. Non-profit organisations	~~PC (MER)~~ C (FUR 2026)	
13. Correspondent banking	~~PC (MER)~~ C (FUR 2026)	
15. New technologies	~~PC (MER)~~ LC (FUR 2026)	• Remaining minor deficiencies under R.16, R 20, R.38-40 continue to be of relevance under this recommendation
35. Sanctions	~~PC (MER)~~ LC (FUR 2026)	• In respect of breaches which concern the performance of specific TCSP and safekeeping activities without relevant registration, a differentiated sanctioning approach for directors and senior management is not established (c.35.2)
38. Mutual legal assistance: freezing and confiscation	~~PC (MER)~~ LC (FUR 2026)	• There are no specific measures in place to regulate the possibility of arrangements for coordinating seizure and confiscation actions with non-EU countries (c.38.1). • There are no specific rules for sharing the confiscated or forfeited property with non-EU countries and deficiencies under c.4.4 apply (c.38.3).

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

Glossary of Acronyms[8]

AML	Anti-money laundering
AML/CFT	Anti-Money Laundering/Countering Financing of Terrorism
Art.	Article
BO	Beneficial Owner
C	Compliant
CC	Criminal Code
DNFBP	Designated Non-Financial Businesses and Professions
EEA	European Economic Area
EU	European Union
EUR	Euro
FI	Financial Institution
FID-SANS	Financial Intelligence Directorate of State Agency for National Security
FIU	Financial Intelligence Unit
LMFTPWMD	Law on Measures Against the Financing of Terrorism and of Proliferation of Weapons for Mass Destruction
LMML	Law on the Measures Against Money Laundering
MER	Mutual Evaluation Report
MFA	Ministry of Foreign and Political affairs
ML	Money Laundering
NRA	National Risk Assessment
NaRA	National Revenue Agency
OE	Obliged entity
OEA	Office for Economic Activities
TCSP	Trust and Company Service Provider
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolution
VAs	Virtual assets
VASP	Virtual Assets Services Provider

8 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

www.coe.int/MONEYVAL

May 2026

Anti-money laundering and counter-terrorist financing measures -

Bulgaria

3rd Enhanced Follow-up Report &
Technical Compliance Re-Rating

This report analyses Bulgaria's progress in addressing the technical compliance deficiencies identified in the May 2022 assessment of their measures to combat money laundering and terrorist financing and in subsequent follow-up reports.

Follow-up report