ČNB ČESKÁ NÁRODNÍ BANKA

DATE: 13 OCTOBER 2022

Supervisory benchmark No 4/2022

On prudent approach of credit institutions to publicly available information with AML/CFT implications

I. Relevant legislation

Key regulations and standards

- Act No 253/2008 Coll., on certain measures against the legalization of proceeds of crime and the financing of terrorism, as amended (hereinafter the "**AML Act**")
- Decree No 67/2018 Coll., on certain requirements for the system of internal principles, procedures and control measures against legitimisation of proceeds of crime and financing of terrorism, as amended (**hereinafter the "AML Decree"**)
- Decree No 163/2014 Coll., on the performance of the activities of banks, credit unions and investment firms, as amended (hereinafter "**Decree No 163/2014 Coll.**")
- The Guidelines pursuant to Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions, repealing and replacing Joint Guidelines JC/2017/37 (hereinafter the "**Guidelines**")

II. Purpose

1. Media cases in which investigative journalists have published documents on the possible transfers of significant proceeds from (potentially) illegal activities, and in which some Czech natural and legal persons were involved, have confirmed that there are no borders in today's financial world. These cases also served as a reminder that key financial crime threats are constantly evolving, including the form of the typologies used. **For example, the abuse of transit accounts, shell companies, nominees and other non-transparent structures can be highlighted here, including in some cases in connection with the legalisation of the proceeds of corruption.**
2. The basic measures for the prevention of the legalisation of the proceeds of crime and terrorist financing (hereinafter "AML/CFT") - client identification and due diligence, and in particular the determination of the meaning and purpose of the business relationship, the origin of the funds and regular review of this information and its comparison with the actual conduct of the client - are crucial for the fight against financial crime and must be applied thoroughly, continuously and in a timely manner.
3. The purpose of this benchmark, however, is primarily to set the expectations of the Czech National Bank ("CNB") regarding credit institutions (hereinafter "institutions"), not only

as a reaction to such cases but also more generally for the monitoring of publicly available information with implications for the management of money laundering and terrorist financing risks (hereinafter "ML/TF risks"). In this context, the benchmark also addresses the appropriate response to acquired information.

III. Summary of CNB conclusions and expectations

4. In the framework of a risk-based approach in the fight against ML/TF, the effective application of AML/CFT preventive measures requires that institutions have at their disposal and take into account the widest possible range of available information on which they can reasonably rely, i.e. in particular information whose truthfulness and credibility are not subject to reasonable doubt. The results of the evaluation and assessment of this information must be further incorporated into an institution's internal regulations and reflected in its procedures.

5. **The CNB therefore expects that an institution:**

Step 1. Actively monitors publicly available information directly related to its ML/TF risk management
The institution will regularly and continuously review available public information on which reasonable reliance can be placed. This procedure will be enshrined in its internal regulations.
Step 2. Assesses which information is relevant to its activities and risk management
The institution will carry out assessments primarily in relation to specific transactions and business relationships, where it will primarily assess whether the information relates to specific clients, related parties, the institution's business relationships or other entities relevant to its activities. Specifically, the institution will examine the relationship of the information in question to, inter alia: • clients and connected persons, • business relationships, • trading counterparties, • institutions in a correspondence relationship.
The institutions will further assess the relevance of the information available at the level of its overall activity. Here, the institution will first of all generalise the cases and related typologies appearing in public information and assess whether adjustments are required to some of its assessments, processes and settings. Specifically, this will mainly involve the typologies involved in the case in question that may be relevant for the institution in general with regard to its activities, i.e. where the given risk may materialise. Examples include: • the type of product being abused, • the type of client, • the subject of the client's business, • the related geographical area, • the method of implementation of the criminal activities.
Step 3. Takes into account information relevant to its activities in its procedures and measures applied to risk management
In the context of specific transactions and business relationships, if the institution identifies that the persons concerned are among its clients or are otherwise related to the institution's activities (e.g. the product provided or the distribution channel used), it will then assess the business relationship in the context of such new information. The purpose of this consideration will be to assess, in particular, whether the level of risk and the type of measures applied are adequate

in the light of such new information. In the case of negative information from the media, this can lead to:

- an increase in the risk category,
- the application of enhanced client screening (in particular, the identification of additional information, thorough assessment of the business relationship, increased monitoring),
- a suspicious transaction report,
- the limitation or termination of the business relationship.

At a strategic level, the institution will use the information available for the purpose of understanding the generalised risks. These conclusions should be reflected in the institution's risk assessment and other internal regulations (and subsequently regarding similar clients, if relevant). Thus, if a particular product or type of client is abused in a given case, or if the case is linked to a particular geographic area or other risk factor, the institution will assess its exposure to that risk in light of its business and client structure. In this context, it will evaluate the procedures and measures it applies to manage this risk to determine whether they are sufficient to prevent it. This consideration should be made in the context of the case pursuant to review, i.e. whether the measures applied by the institution would have prevented its abuse under a similar threat. If the institution's current practices are re-evaluated, this change may be reflected with other existing clients. Examples of generalised risk factors from past cases include:

- transit accounts,
- shell companies with no real activity,
- nominee structures,
- international trade transactions with no real economic substance,
- politically exposed persons,
- legal persons from countries with low levels of transparency in corporate structures,
- business relations without any real connection to country in question.

6. The CNB expects that the above procedures will be established and applied in the context of the principle of proportionality and in relation to identified risks. The CNB is aware of the presumption of innocence and other legal principles. Of course, it is possible that some claims, even from public sources that can reasonably be relied upon, will subsequently be refuted. The approach described in this benchmark is not intended to penalise entities that are or will be the subject of public information, but only to ensure that institutions adequately identify, assess and manage potential risks. All related procedures must be enshrined in the institution's internal regulations.
7. Detailed information on each of these steps is provided in Chapters IV to VII below.
8. **In view of the above, the CNB also expects the institutions to actively communicate with the CNB's supervision departments. In particular, it expects the active provision of information to the relevant CNB supervision departments in the event of significant findings, including communication of the conclusions of assessments carried out[1] in connection with significant cases.**

IV. Summary of relevant legal obligations

9. AML/CFT legislation in the Czech Republic and related and recognised standards are based on a risk-based approach to ML/TF prevention. The basis of this approach is the identification of all relevant risks to which the institution is exposed and the identification

[1] This is also relevant in the context of the mandatory information obligation pursuant to Article 116 of Decree No 163/2014 Coll.

and application of appropriate measures to manage, in a targeted manner, those risks relevant to the institution and its business and business relationships. Effective implementation of this approach therefore requires the identification and analysis of all available relevant information and the identification of appropriate practices within the institution's activities. All information and procedures used must be up-to-date and relevant to the real situation.

10. The specific provisions that are key in this context with regard to the practical implementation of preventive measures are based primarily on the client identification and due diligence obligation (Article 7 et seq. of the AML Act and Article 6 et seq. of the AML Decree), and also the provisions governing the procedure in the event of the impossibility of client identification and due diligence and in the event of the identification of ML/TF suspicion (Article 15, 18 et seq. of the AML Act). The details of the fulfilment of these obligations must be regulated in detail in the internal regulations of the institution (Article 21 of the AML Act and Article 4 of the AML Decree) and must be based on a comprehensive risk assessment of the institution (Article 21a of the AML Act and Article 5 of the AML Decree). The Guidelines, which institutions are obliged to take into account in their internal regulations (Article 4(2) of the AML Decree), also provide more detailed guidance on the individual steps.

11. The AML Act also establishes the CNB's supervision powers over the control of the implementation of AML/CFT measures (Article 35 of the AML Act), and the CNB's specific supervision powers are further regulated primarily in sectoral regulations governing the functioning of the financial market.

12. It is also key to stress that the risk-based approach also assumes that the implementation of AML/CFT measures is appropriate to the size and scope of the institution's activities[2]. The procedures applied must therefore be appropriate to the specific risks and will not always be the same in scope. The risk-based approach justifies differences in practices not only between institutions but also within an individual institution. The specific measures and procedures may therefore vary in intensity and for different categories of clients. However, the procedures applied must always be risk-appropriate and must be as prudent as possible for higher-risk clients (e.g. for private banking in the context discussed here).

V. Collection of information

13. In order to effectively apply AML/CFT measures, and risk management in general, an institution must have a sufficient range and quantity of information available to enable it to identify and assess the risks to which it is exposed. The institution must also ensure that the information it has available is up-to-date and valid.

14. **The CNB therefore expects institutions to actively monitor publicly available information related to AML/CFT and with impacts on the implementation of preventive measures against ML/TF. An institution will further assess which of this information is relevant to its activities and the management of the risks to which it is exposed. An institution must take into account all available information both in the context of its specific transactions, business relationships and activities, and by type with respect to its activities in general.**

i. Information on individual transactions and business relationships

15. The obligation to acquire and assess relevant information relates primarily to the individual business relationships, in particular with regard to the client identification and due diligence

[2] This is without prejudice to certain legal obligations that are mandatory in nature and do not allow the application of a risk-weighted approach.

obligation and thus information on the nature of the business relationship, the client's conduct during the business relationship, the sources of funds and assets in the business relationship or, in the case of politically exposed persons, all assets (Article 8 et seq. of the AML Act). Institutions must collect this information to the extent necessary to assess the potential ML/TF risk (Article 9(3) of the AML Act).

16. In the case of a business relationship or transaction with increased risk, the institution will conduct enhanced client due diligence that includes at least the identification of additional information about the client, other relevant persons, the business relationship, and the relevant assets (Article 9a of the AML Act and Article 9 of the AML Decree).

17. For the duration of the business relationship or in the course of further transactions, the obliged person will check the validity and completeness of the information obtained in the context of client identification and due diligence (Article 8(9) of the AML Act and Article 7(3) of the AML Decree).

ii. Information on the activities of the institution

18. The institution is obliged, at institution level, to map the risks to which it is exposed in general (risk assessment pursuant to Article 21a of the AML Act). This risk assessment will comprehensively analyse the risks to which the institution is exposed in its entirety and in its individual activities. In that regard, the institution will "take into account at least such scope and types of sources of information that ensure that the risk assessment genuinely reflects the real risks connected with the activities of the institution" (Article 5(2) of the AML Decree).

19. Similarly, the Guidelines take a similar approach to risk assessment, expecting institutions to assess the risk to which they are exposed in the context of the whole enterprise and individual business relationships/transactions (point 1.2), and that to identify relevant risks and apply appropriate measures, institutions must, as part of their ML/TF risk management systems and controls *"ensure that they have systems and controls in place to identify emerging ML/TF risks and to assess and, where appropriate, incorporate these risks into their individual and enterprise-wide risk assessments in a timely manner"* (point 1.8) and assess available information on an ongoing basis to "*identify trends and emerging problems, both in relation to individual business relationships and to the business activities of the enterprise*" (1.9.a). Institutions must have enshrined in their internal regulations *"processes to ensure that the enterprise regularly reviews relevant information sources, including those listed in Guidelines 1.28 to 1.30 and, in particular ... media reports that are relevant to the sector or jurisdictions in which the enterprise operates"* (paragraph 1.9.b).

20. The guidelines also address the range of relevant sources of information that institutions should use to identify ML/TF risk (paragraphs 1.29 et seq.). Here, it specifically states that *"businesses should use information from a variety of sources that can be accessed independently or through commercially available tools or databases that bring together information from multiple sources".* Institutions should always take into account information from public authorities (e.g. national risk assessments, the European Commission's list of countries at risk, information from the FAO, other state authorities, etc.) and information available from their own activities, in particular from client identification and due diligence. However, other sources of information also include *'information from credible and reliable freely available sources, such as reports in trusted newspapers'* and *'information from credible and reliable commercial organisations, such as risk reports and intelligence reports'.*

VI. Analysis and use of publicly available information

21. The CNB expects institutions to consistently take into account all information known to them. In the case of negative information from the media that can reasonably be relied upon, institutions will examine whether and how such information is relevant to their activities. Specifically, the institution should[3]:

a. verify whether the persons mentioned in the public information are its clients or persons related to them or are otherwise relevant to the institution's business activities; where appropriate, take the information into account in the measures it applies to the clients concerned; in order to comprehensively manage the risks to which the institution is exposed, including reputational risk, the CNB expects the institution to carry out this assessment in a similar and appropriate manner with regard to other entities relevant to its activities;

b. analyse public information in order to generalise the risks involved and assess the potential impact on the institution's activities; where appropriate, reflect the identified risks in its internal rules.

i. Assessment of specific entities

22. As regards the consideration of available information with regard to specific business relationships, an institution should first of all check whether the information contained in public sources is relevant to its business activities. In particular, this will be the case where the subject of the transaction is a person who is a client of the institution or is otherwise connected to its clients (e.g. the beneficial owner of the client). Publicly available information on which reasonable reliance can be placed is an important source of information in assessing a client's reputation in the context of its risk assessment (points 2.3 and 2.5 of the Guidelines). Although publicly available information may also contain information that reduces the risk of a business relationship, we focus below on how to deal with negative information.

23. If the institution determines that the information obtained is relevant to its particular business relationship(s), it must, in particular, consider the new information in the context of existing information about the client and the business relationship. Pursuant to Article 7(3) of the AML Decree, the institution is obliged to establish and apply procedures for updating the risk profile of the client. Thus, even in the case of publicly available information, the institution should have procedures in place to determine whether there are facts that require such an update without delay. Subsequently, it will also assess whether the new information justifies a change in the approach to the client (in particular, a change in the risk profile of the client and the related intensity of the measures applied; Article 9 et seq. of the AML Act and Article 6 et seq. of the AML Decree).

24. In the case of an increased risk (or directly a higher risk profile), the institution performs enhanced identification and due diligence of the client to the extent and in a manner that ensures effective management of the identified risk (Article 9a of the AML Act and Article 9 of the AML Decree). In the case of higher risk clients, it will often be appropriate for institutions

[3] In a number of cases, it must do so even according to the applicable regulations – among others, Article 9(4)(a) and (d) of the AML Decree.

to identify and assess publicly available information more intensively[4]. At the same time, in the event of an increase in risk due to negative information, this should generally lead to the application of more intensive measures by the institution towards the client.

25. In other related situations and follow-up procedures, institutions must also follow the relevant AML/CFT regulations. Therefore, if an institution detects a suspicious transaction in the context of the above procedure, it will notify the FAO without undue delay (Article 18 of the AML Act). Alternatively, if there is a risk that the seizure of the proceeds of crime or the funds intended for TF may be frustrated or substantially impeded, the institution will suspend the client's order (Article 20 of the AML Act). In the event of inability to perform client identification or due diligence or in case of doubts about the veracity of the information provided by the client or the authenticity of the documents submitted, the institution will refuse to execute the transaction or terminate the business relationship (Article 15 of the AML Act, point 4.66 of the Guidelines, Opinion of the European Banking Authority (EBA) on de-risking)[5].

26. In the context of risk management in general[6] , an institution should also take an appropriate approach to other entities relevant to its activities, particularly with regard to correspondent and respondent relationships or significant counterparties.

ii. Strategic analysis of associated risks

27. Along with analysing the impact of publicly available information on the client portfolio, the CNB expects institutions to assess publicly available information by carrying out a generalised analysis of it from a strategic perspective in order to identify the risks to which the institution is or might be exposed in general. Similarly, just as institutions take into account information and typologies from national risk assessments, FAO annual reports, or law enforcement agencies generalized to their specific activities, so should potential risks associated with specific cases be assessed and generalized. Among other things, this includes an assessment of the institution's level of exposure to the risk of its clients' possible involvement in illegal activities and an assessment of the adequacy of the procedures set up to prevent the identified risk.[7].

28. Following the above-mentioned analysis, the institution will assess whether its conclusions have an impact on the institution's risk assessment and, if necessary, revise it (Article 21a of the AML Act and Article 4(5) of the AML Decree). Furthermore, the institution will consider whether the risk assessment (in particular any changes thereto) justifies a general revision of its internal AML/CFT regulations (Article 4(5) of the AML Decree, point 1.18 of the Guidelines

---

[4] Some mandatory situations of increased risk are listed in Article 9a of the AML Act and Article 9(3) and (4) of the AML Decree. Closely related to the topic of this benchmark are also the changes made by the 2021 amendment, where among the increased risk factors added was *"the fact that information available to the institution indicates that the client has acted unlawfully in the last 5 years, if this unlawful conduct may have been related to ML/TF".*

[5] In this context, the Guidelines stress that institutions should take into account that *"the application of a risk-based approach does not require them to refuse to enter into or to terminate business relationships with entire groups of clients that they associate with a higher risk of money laundering and terrorist financing, as the risk associated with individual business relationships varies even within a single category"* (point 4.68 of the Guidelines). The EBA's opinion on de-risking (EBA/Op/2022/01) emphasises the possibility of managing risk by, for example, narrowing the range of products provided or limiting their features.

[6] In the context of, *inter alia*, Article 31 of Decree No 163/2014 Coll.

[7] As an example, if the negative publicly available information that can reasonably be relied upon will typically involve specific jurisdictions (e.g. offshore) or forms/arrangements of clients (e.g. nominee structures), it is appropriate to assess the frequency and significance of these factors in the institution's activities as well.

on ML/TF risk factors). In any case, it is essential that an institution's internal procedures always correspond to the risks identified and manage them effectively.[8].

VII. Internal procedures and regulations

29. The above-mentioned procedures for handling publicly available information must be enshrined in the institution's internal procedures as risk assessment and risk management measures (Article 21(5)(d) of the AML Act). Specifically, at least when the above assessments are carried out, their scope and method, the person responsible, and the method of evaluating their results must therefore be regulated. These procedures should always be proportionate to the scope of the activities and the importance of the institution.
30. Where warranted, the internal rules must also retrospectively take into account the results of individual assessments - see the above on risk assessment and setting up follow-up procedures to manage identified risks.
31. The assessments carried out must meet the requirement for retrospective reconstructability (Article 18 of the AML Decree, Article 11(2) of Decree No 163/2014 Coll.) so that it is clear what considerations, evaluations, results and follow-up have been achieved. Retrospective reconstructability will also ensure that the institution is able to demonstrate compliance with the legal obligations described above (Article 35 of the AML Act and Article 9(3) of the AML Act).
32. The collection, assessment and evaluation of publicly available information should also be included in the institution's evaluation report (Article 19 of the AML Decree), *inter alia* to ensure that the institution's managers are informed (point 1.17. Guidelines on ML/TF risk factors). In the case of non-applicability, this information should also be provided (e.g. that no public information relevant to the institution's activities was available).

VIII. Interaction and cooperation with the CNB

33. The CNB is the competent authority to supervise the fulfilment of the obligations set out in the AML/CFT regulations (Article 35 of the AML Act). As part of its AML/CFT supervision activities, the CNB will also examine compliance with the supervision expectations described in this benchmark.
34. The CNB has a range of supervision powers and tools at its disposal, in particular with regard to access to information relevant to the exercise of supervision. In addition to direct supervision activities, the CNB considers active cooperation with institutions to ensure mutual information to be key. Article 116 of Decree No 163/2014 Coll., which requires an institution to inform the CNB without undue delay if it detects the risk of a significant threat to its reputation (*inter alia*, in connection with a significant trend in AML/CFT), is also relevant here.
35. **In this respect, the CNB expects institutions to share their results proactively with the CNB in the event of relevant analyses being carried out, particularly in the context of publicly available information with a clear link to a specific institution or a significant impact on the Czech financial market.**

[8] For example, for the facts above (risk jurisdictions or client forms), these factors can generally be assigned a higher risk and more intensive ML/TF risk management measures applied to the business relationships where they occur.