The obligation to update customer data

Regulation

- Act No. 253/2008 Coll., on Certain Measures Against Legitimisation of Proceeds of Crime and Financing of Terrorism, as amended (**AML Act**)
- Decree No. 67/2018 Coll., on Selected Requirements for the System of Internal Rules, Procedures and Control Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism (**AML Decree**)

Provisions

- **Articles 8(7) and 15 of the AML Act**
- **Articles 7, 8 and 10 of the AML Decree**

Question

How should the obliged entity regularly update the information it holds regarding a customer?

Answer

Pursuant to the AML Decree, the obliged entity must establish procedures for updating customer data. The frequency and scope of the updates shall be based on the risk identified.

The obligation to regularly update customer information is based on Article 8(7) of the AML Act.[1]

Articles 8(1) and 8(2)(b) of the AML Decree further require the obliged entity to put in place procedures based on which it will, pursuant to the customer's risk profile, apply to the customer measures to ensure effective mitigation of the risks associated with the customer, including procedures regarding the frequency and scope of customer due diligence processes. More specifically as regards updating data, Article 7(3) of the AML Decree requires the obliged entity, in the case of a business relationship, to regularly check the validity and completeness of the information about the customer and, where appropriate, to update this information and the customer's risk profile. The provision further requires the obliged entity to set out the procedures for this updating in its system of internal rules and to determine the facts on the basis of which the update will always be performed. At the same time, however, maximum intervals for performing updates must be set. These procedures should be based on the identified risk associated with the business relationship.

Pursuant to the AML Decree, the obliged entity's system of internal rules must include procedures based on which the obliged entity will update the information it holds on the customer and the suitability of the risk profile established:

1. regularly, and
2. on an *ad hoc* basis in justified instances.

The information must be updated in a way that is based on and is in accordance with the institution's risk assessment. It can, therefore, be assumed that the set procedures will differ across risk categories. For example, the frequency of updating can be set in a different manner for different risk categories, but it can also be appropriate to adjust the scope of the information to be obtained to the risk identified. It is to be emphasised that the set procedures must ensure effective mitigation of identified or potential risks of abuse of the business activities of the obliged entity for money laundering or financing terrorism, and it is, therefore, necessary to establish these procedures taking this aspect into consideration.

To mitigate the risk of abuse of the obliged entity's business activities for money laundering and terrorist financing, it is crucial that the institution has all the valid, up-to-date and relevant information it needs to apply appropriate risk mitigating

[1] Article 8(7) provides that "*For the duration of the business relationship or in other transactions, the obliged entity shall check the validity and completeness of the customer's identification data and information gathered in the course of the customer due diligence process (Article 9), and the justification for performing simplified customer due diligence (Article 13) or exempting the customer from the due diligence process (Article 13a), and shall record changes thereof.*"

measures (including customer risk categorisation) and to identify and assess potential suspicions (without prejudice to the obligation to always identify and update the information required by law).[2]

Pursuant to Article 15 of the AML Act, the obliged entity must not perform a transaction or must terminate the business relationship if it is unable to conduct customer identification or customer due diligence. This should, therefore, be the final step as a last resort, even if the obliged entity is not able to update the information held on the customer (as this is part of the customer due diligence process). However, it can be assumed that this step will be preceded by other actions, such as limiting the type and scope of services provided in order to reduce risk (while prompting the customer to provide the required information).

In addition, under Article 10(1) of the AML Decree, the obliged entity must also always verify the information it holds on the customer without undue delay if it has doubts as to the correctness or veracity of information obtained previously. Under paragraph 2 of the same provision, the obliged entity must also add missing information in the event of a change in legislation (i.e. if new legislation extends the scope of information required, obliged entities must ensure that they hold the same types of information about customers with which a business relationship was established before the new regulations took effect).

When in doubt about the correctness or veracity of the information held, the obliged entity must verify this information without undue delay, whereas in the case of completing information after a change of legislation, the AML Decree requires the revision to be made within deadlines defined with respect to the risk profile of the customer (i.e. the obliged entity can graduate the delays for performing this update across risk categories).

Nature of the Opinion	This answer expresses the opinion of Czech National Bank staff members. The court and, as the case may be, the Bank Board of the Czech National Bank may be of a different opinion.
Contact person:	Kateřina Pscherová, katerina.pscherova@cnb.cz
Date:	20 May 2019

[2] An example of scope for discretion by the obliged entity is the identity card number, which the obliged entity must update if it deems it appropriate and useful to do so. However, it is not a legal obligation, since the law only requires it to update identification data, not information associated with identification.