5th AML Directive already active in Lithuania | How it affects your business?

On January 10, 2020 the Law amending Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing (**the Law**) came into effect implementing the 5th AML Directive and bringing some key changes.

As these changes are already mandatory, it is important to assess whether and how this affects the business and decide on necessary actions to be taken.

We summarize the key changes that affect financial market participants below in this briefing.

Expansion of the regulated sector

As a general rule, the Law was and remains to be applicable to financial institutions and other obliged entities. The novelty that was introduced is related to the expansion of the list of obliged entities which now covers also the following businesses:

- Operators of crypto exchanges;
- Operators of custodian wallets;
- Persons trading or acting as intermediaries in the trade of works of art where the value of the transaction or a series of linked transactions amounts to EUR 10.000 or more;
- Free zones where the value of the transaction or a series of linked transactions amounts to EUR 10.000 or more;
- Persons providing material assistance, support or advice on tax matters;
- Real estate rent intermediaries concluding rent agreements where the monthly rent is equal or exceeds EUR 10.000.

From now on the persons engaging in these areas will be subject to full scope AML regime and will be required to conduct customer due diligence, perform monitoring, undertake suspicious activity reporting duties, etc.

If you do not fall under the above list of obliged entities but you are a financial institution targeting the above persons as your customers, from now on you will have to assess whether such customers are compliant with their AML duties. This might also require reviewing and updating your AML procedures and customer risk assessments.

New duties for crypto businesses and ICOs

Besides the general obligations, the Law establishes specific duties for the operators of crypto exchanges and custodian wallets. For instance, operators of crypto exchanges are required to report to the Financial Crime Investigation Service (the "**FCIS**") about each transaction equal or exceeding EUR 15.000 value (in comparison, financial institutions have the same reporting duty only for cash transactions). Operators of crypto exchanges and custodian wallets will have to notify the Register of Legal Entities within 5 business days about the start or end of their activity as operators. Additional requirements for the operators are established in the Regulations for the Operators

of Crypto Exchanges and Custodian Wallets Aimed at Preventing Money Laundering and Terrorist Financing approved by Order No V-5 of FCIS's Director and valid as of January 10, 2020.

ICOs, even though were left outside the scope of "other obliged entities", also became subject to specific AML regime. Namely, persons offering ICOs are now obliged to identify a person acquiring virtual currency and its beneficial owner(s) and to assess the sources of assets and funds used for execution of a transaction in virtual currency equal or exceeding EUR 3.000 or equivalent in crypto currency fixed at the transaction conclusion moment. ICOs will also have to submit information on their activity requested by FCIS as well as to store customers' data for 8 years as of the transaction execution moment.

Facilitated customer identification

Financial institutions and other obliged entities are now allowed to collect all data required for the identification of a customer and UBO(s) from official state databases and registers without requesting the same documents from a customer. This right may be implemented in the following cases:

- Where the customer confirms the data collected by the financial institution or other obliged entity with his signature (including the advanced e-signature or qualified e-signature);
- If the data newly collected by the financial institution or other obliged entity does not differ from the data that was previously confirmed by the customer;
- If the data collected is about the executive officer of the customer;
- If the data is collected from the Lithuanian Population Register.

The above exemption is applicable both for remote and physical identification of a customer.

UBOs identification

The Law introduced limited but rather significant two changes in the field of UBO(s) identification.

First, the requirement to collect information about the *"ownership and control structure"* of each customer who is a legal entity replaced the previous requirement which was limited only to identification of the *"management structure"*. In practice this means that financial institutions and other obliged entities are now required to collect official documents allowing to identify the whole shareholding structure until the UBO(s) and other controlling persons, if any, of the customer being legal entity. It is worth mentioning that the same requirement was already applied before, however, now it has even a stronger and clearer legal basis.

Second, even before January 10, 2020 the Law introduced a possibility to consider the senior executive officer as UBO of a legal entity provided that individual persons holding not less than 25% of a legal entity or having another control towards the entity cannot be identified. Still, in such a case the problem was to decide which senior executive officer shall be treated as UBO if there were few entities in the customer's shareholders chain. For instance, if a customer legal entity X is 100% owned by a legal entity Y which shares are divided among individual persons each holding less than 25% and having no other control rights towards the entity Y, it was not clear whether senior executive officer of entity X or entity Y should be treated as UBO. The Law finally gave clarity towards such situation. Now it clearly states that it should be a person who holds senior officer's position within a person being identified, thus, it would be an officer of entity X.

In addition to the above, the Law established a duty to fully identify the senior executive officer if he is treated as customer's UBO. The latter change, however, would not be a burden in case the legal entity is represented by its senior executive officer who in any case would be required to be identified.

Enhanced due diligence (EDD)

The below changes were introduced with respect to EDD processes:

- More clarity was given for EDD performance when transaction or business relationship are concluded with persons residing or established in countries that are qualified as high-risk third countries by European Commission. Namely, a list of additional information to be requested from a customer is now established as well as a new requirement to ensure that the first payment of such customer comes from his account with EU credit institution or credit institution of a third country applying the same AML standards and being supervised by local supervisory authority is now applied;
- A ground to perform EDD in *"cases indicated by the European supervisory authorities and the European Commission"* was eliminated from the Law;
- FCIS was authorized to establish additional duties for the financial institutions and other obliged entities in case of servicing customers from high-risk counties. Implementation of such right of FCIS is directly linked with the results of the national risk assessment.

Simplified due diligence (SDD)

Relevant changes were introduced with respect to SDD processes:

- E-money institutions were given a right to perform SDD for a customer if within a calendar year the value of the issued e-money does not exceed EUR 1.000 (previously this condition was linked with the amount of transacted operations which included both issued and redeemed e-money). Other conditions remain unchanged;
- Simplified due diligence is now available for payment initiation and account information service providers;
- A ground to perform SDD in *"cases indicated by the European supervisory authorities and the European Commission"* was eliminated from the Law.

Other key changes introduced by the Law

- The list of public prominent functions (relevant to identify PEPs) was slightly changed and will be subject to on-going revision at least once every 4 years.
- Banks are now forbidden to rent anonymous safe-deposit boxes. FCIS acquired a right to check the content of safe-deposit boxes rented by banks.
- Foreign e-money and payment institutions who engage in Lithuania through their agents were released from a mandatory duty to appoint local contact point for communication with FCIS. From now, the mentioned institutions will be required to appoint local contact point only if they meet at least one criterion established under Article 3(1) of Regulation (EU) No 2018/1108.
- The following activity of a customer was qualified as exposing to a higher risk: activity related to oil, guns, precious metals, tobacco products, cultural artefacts and other assets that are valuable from the archaeological, historical, cultural or religious point of view, items of rare scientific value, deals with ivory and protected species.
- Depending on the results of the national risk assessment, additional prohibitions to establish activity in high-risk countries, distinguished by the European Commission, may be imposed in the future. Among such prohibitions it may be prohibited to establish subsidiaries, branches, agency relations or correspondent relations with persons from such countries.

Additional changes expected in the nearest future

Apart from the wide palette of changes that were already introduced by the Law, further changes are yet to come.

The Bank of Lithuania already prepared a draft to amend its Resolution No 03-17 which establishes requirements to the financial market participants aiming at preventing money laundering and terrorist financing. The draft provides a more detailed description on the scope of financial market participants' AML duties. Among the new requirements, financial market participants will have to perform regular (at least once per year) overall company's risk assessment which shall assist the company to understand the changes in its risk appetite, risks to which the company is exposed, the level of risk mitigation, the need to invent new monitoring tools, etc. The draft legal act is likely to be adopted in Q1 of 2020.

There is one more draft amending the Law registered at the Parliament. The aim of this draft is to introduce a possibility for the financial institutions and other obliged entities to use driver's license for customer identification purposes. So far, there is no clarity as to when this draft will be approved.

***

The above is only a briefing of the new requirements of the Law. The Law contains a number of other changes which have not been covered by this overview, but which may be important for your business. If you are subject to the provisions of the Law, it is advisable to review your internal processes and procedures to make sure your operations are in all respects compliant with the applicable legal requirements.

Contact information:

Simona Kišūnaitė

simona.kisunaite@walless.com

+370 656 62027