Anne Saaber, Estonia

Notaries tasks in preventing money laundering and financing of terrorism have been provided for in the Estonian legislation since 2004. The current Money Laundering and Terrorist Financing Prevention Act entered into force on 27 November 2017 (some sections will enter into force on 1 September 2018 and 1 January 2019). Obliged entities, including notaries, must bring their activity into compliance with the requirements of this Act and update their rules of procedure within one year as of the entry into force, i.e. by 27 November 2018.

The Ministry of Justice has delegated supervision over the compliance of notaries' activities with the Money Laundering and Terrorist Financing Prevention Act to the Chamber of Notaries. The Chamber of Notaries has decided to solve the issue by establishing, in particular, common rules of procedure. The rules of procedure will be minimum standards the notaries should comply with in their professional activity. The notaries may apply the rules of procedure established by the Chamber of Notaries directly or draft an additional set of rules for their notary's office. The rules of procedure applicable today were approved by the general meeting of the Chamber of Notaries on 26 March 2010. New rules of procedure have been drafted and circulated to the notaries for making amendments.

The common rules of procedure are an attempt to systematise requirements and highlight notary-specific activities, such as risk assessment and management as well as to provide instructions for a risk analysis.

Notaries apply the Money Laundering and Terrorist Financing Prevention Act primarily when authenticating transactions related to sales of immovable, sales of shares or stocks, transfers of a company and foundation of a legal entity as well as depositing money or securities.

In particular, the notaries are obliged

- To apply due diligence measures;
- To inform the Financial Intelligence Unit of suspicion of money laundering or terrorism or cash transactions;
- To follow international financial sanctions.

In 2017, Estonian notaries submitted 168 reports to the Financial Intelligence Unit (cf. in 2016 – 137), including 138 of cash transactions exceeding the limits provided for cash transactions in the Act, 24 of money laundering suspicions and 3 of suspicions of terrorist financing. Reports are submitted to the Financial Intelligence Unit electronically via a designated web site.

In 2017, a total of 5,418 reports were submitted to the Financial Intelligence Unit (2016 – 5,525). It is worthwhile to single out that while others inform the FIU of mostly suspicions of money laundering or terrorist financing, notaries informed primarily of cash transactions.

According to the FIU statistics, only a fraction of reports lead to criminal proceedings. In 2016, 68 money laundering criminal offences were registered in Estonia, including four based on the FIU data. The same year, the Financial Intelligence Unit forwarded information from 484 reports, including 4 reports by the notaries. Thus, 6–8% of the reports are of major interest and a minor part leads to criminal proceedings.

The international financial sanctions are followed via the E-notary system, the notaries' electronic working environment. The E-notary system is interfaced with designated lists and for each transaction an enquiry is made into the relevant register.
Some of the due diligence measures arising from the Money Laundering and Terrorist Financing Prevention Act overlap with provisions from other acts regulating the notary's professional activity. Identification of customers, establishment of the customers' intent, verification of the right of representation, registration and retention of their customers' data is undisputable for the notaries.

Specific requirements arising from the Money Laundering and Terrorist Financing Prevention Act, such as the obligation to identify the beneficial owner of the transaction, to identify the foreign politically exposed person, to ascertain, if necessary, sources financing the transaction, etc., are more complicated and need additional instructions.

In case of companies registered in Estonia the identification of the beneficial owner is usually not difficult. The database of the Estonian Commercial Register has data both on partners and majority shareholders. Shareholders' data can be established in the Estonian Register of Securities. The notaries can access the registers by making enquiries via the E-notary system.

Pursuant to the Money Laundering and Terrorist Financing Prevention Act, as of 1 September 2018, the commercial register shall have to disclose the data of the beneficial owner. The management board of the company shall be obliged to submit the data of the beneficial owner to the register. The data of the beneficial owners shall be accessible via the commercial register as of 1 November 2018.

The situation will be complicated if there are no data in the commercial register, in particular, if the beneficial owner of the foreign legal entity, not entered in the Estonian commercial register, has to be established. In this case, the notary will have to interview the party. According to the rules of procedure, the party to the transaction shall have to fill in the Beneficial Owner's Questionnaire. In addition, each notary as an obliged entity can assess the customer and the transaction to be performed; in case of doubt, require additional documents to identify the beneficial owner.

The identified beneficial owner is also subject to due diligence measures and to verification whether the person is subject to financial sanctions or whether other higher risk factors apply.

In order to determine whether the party to the transaction is a foreign politically exposed person, a questionnaire is filled in. Besides, the notary can use other available tools to acquire publicly available information (such as, conduct a name search using public search engines, etc.).

The Chamber's rules of procedure will also establish requirements how to determine the degree of risk of the customer and of the transaction. The degree of risk is either lower than usual, average or higher than usual. In compliance with the risk degree established, the notary will have to apply the due diligence measures either as usually or enhance them. The customer's risk profile is assessed at least upon the first contact with the customer, whereas the risk profile of the transaction upon the performance of each transaction. If it is a higher-risk customer or transaction, additional information will have to be gathered, e.g., about the origin of funding sources and the property. In certain cases, the transaction can be performed only with the

written consent of the Financial Intelligence Unit or the obliged entity may be obliged to refuse from making the transaction.

The customer's degree of risk will be determined based on residency, political exposure, lists of international sanctions and the third party related to the customer (the beneficial owner). The risk profile of the transaction will be determined, in particular, based on the purpose of the transaction and the mode of financing of the transaction. If characteristics of money laundering or terrorist financing appear in the transaction (such as, large cash payments, explicitly incorrect price in the transaction, payments to third parties unrelated to the transaction, the money used in the transaction accrued in offshore territories or from a person residing in the so-called risk state), if necessary the FIU will be informed or in certain cases the notary will refuse to make the transaction.

The Chamber of Notaries' rules of procedure establish several questionnaires to collect data:

- To identify the beneficial owner
- To identify the foreign politically exposed person
- To establish sources used to fund the transaction and the origin of the customer's property
- To identify the customer's profession or field of activity

All questionnaires compiled and materials received while applying the Money Laundering and Terrorist Financing Prevention Act will be retained together with the transaction. They will be submitted to the FIU where necessary.