ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

To : **Regulated Entities**
i. CIFs
ii. ASPs
iii. UCITS Management Companies
iv. Internally managed UCITS
v. AIFMs
vi. Internally managed AIFs
vii. Internally managed AIFLNPs
viii. Companies with sole purpose the management of AIFLNPs

From : **Cyprus Securities and Exchange Commission**

Date : **May 10, 2019**

Circular No. : **C318**

Subject : **National Risk Assessment on Money Laundering and Terrorist Financing – Automated screening systems to enhance customer due diligence measures**

Further to Circular C292 'National Risk Assessment on Money Laundering and Terrorist Financing', in which the Cyprus Securities and Exchange Commission (the 'CySEC') informed regulated entities of the findings of the National Risk Assessment on money laundering and terrorist financing (ML/TF) (together, the "NRA"), CySEC wishes to inform the regulated entities on the implementation of automated screening systems for the enhancement of regulated entities' customer due diligence (CDD) measures.

The NRA identified the requirements to strengthen anti-money laundering and counter-financing of terrorism (AML/CFT) practices of the regulated entities. As announced in Circular C292, an Action Plan was formed on the basis of the NRA results to remedy the vulnerabilities identified and recorded in the NRA Report. In particular, the Action Plan refers to the encouragement of controls such as electronic screening from commercial databases for the enhancement of CDD measures.

As announced in CySEC's Circular C260, and Circular C314 it was identified that regulated entities were not fully equipped to conduct accurate identification, recording and ongoing evaluation of the risk posed by customers. This was due to weak processes of obtaining and assessing information about customers' or beneficial owners' backgrounds. In addition, in some cases, weaknesses in screening customers on sanctions/restrictive measures adopted by the United Nations (UN)/European Union (EU) were identified.

In addition to performing normal CDD measures, regulated entities must have in place appropriate risk management systems, including risk-based procedures, to determine whether customers or beneficial owners of the customer is a Politically Exposed Person (PEP), as defined in section 64(1)(c) of the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2018. In particular, point 5(g)(i) of the 4th Appendix of the Directive DI144-2007-08 on the Prevention of Money Laundering and Terrorist Financing refers specifically to the means through which PEPs may be detected. These include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs. These databases can be based on information from the customer themselves and from publicly available information. Further analysis on the use of commercial databases for the detection of PEPs can also be found in the FATF Guidance on Politically Exposed Persons (Recommendation 12 & 22).

The European Supervisory Authorities' 'Risk Factors Guidelines' also state that regulated entities should identify which ML/TF risks they are, or would be, exposed to as a result of entering into a business relationship or carrying out an occasional transaction. The Risk Factors Guidelines refer to the various sources from which information should derive regarding the relevant ML/TF risk factors, '*including who their customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer requires and the channels the firm uses to deliver these products, services and transactions*'. Specifically, points 14-16 of the Risk Factors Guidelines read as follows:

*'**Sources of information***

*14. Where possible, information about these ML/TF risk factors should come from a variety of sources, whether these are accessed individually or **through commercially available tools or databases that pool information from several sources. Firms should determine the type and numbers of sources on a risk-sensitive basis [CySEC highlights].***

15. Firms should always consider the following sources of information:

- *the European Commission's supranational risk assessment;*
- *information from government, such as the government's national risk assessments, policy statements and alerts, and explanatory memorandums to relevant legislation;*
- *information from regulators, such as guidance and the reasoning set out in regulatory fines;*
- *information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and*
- *information obtained as part of the initial CDD process.*

16. Other sources of information firms may consider in this context may include, among others:

- *the firm's own knowledge and professional expertise;*
- *information from industry bodies, such as typologies and emerging risks;*
- *information from civil society, such as corruption indices and country reports;*
- *information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;*

- *information from credible and reliable open sources, such as reports in reputable newspapers;*
- *information from credible and reliable commercial organisations, such as risk and intelligence reports; and*
- *information from statistical organisations and academia.'*

It is important that regulated entities capture the above-mentioned sources when identifying their ML/TF risks and developing their processes for AML/CTF risk assessment, determining for example whether the client is subject to EU/UN and international sanctions, politically exposed person (PEP), convicted or suspected criminal. The primary requirement for regulated entities is to ensure the correct ML/TF risk classification on the basis of CDD measures before establishing a business relationship with a client, and on an ongoing basis.

There is a variety of commercially available automated screening systems which can assist in the detection and assessment of whether a person falls into any of the above categories. Use of these automated screening systems is not a mandatory requirement of the Law. However, such systems are considered important support tools to complement required CDD measures. The core purpose of using such screening systems is to improve, not replace, the effectiveness of the regulated entities' AML/CFT compliance by helping regulated entities obtain a more complete view of their ML/TF risks, and hence adjust the extent of the CDD measures on a risk-sensitive basis.

Overall, CySEC expects that regulated entities:

- Have an effective customer screening system appropriate to the nature, size and ML/TF risks of the regulated entity. This should include well-documented policies and procedures.
- Screening should be performed before: (i) the establishment of a business relationship; (ii) the provision of any services; and (iii) undertaking any transactions for a customer. Thereafter, monitoring should be undertaken on an ongoing basis for customers and customers' related entities, directors and beneficial owners.
- Ensure that customer data used for ongoing screening is up to date and correct.
- Ensure that there is a full understanding of the capabilities and limits of the automated screening system.
- Tailor the automated screening system in line with regulated entities' risk appetite, and perform regular reviews of the calibration and rules to ensure its effective operation.
- Implement controls that require referral to relevant compliance staff prior to dealing with flagged persons.
- Have in place procedures for the treatment of potential 'target matches'. For example:
  - investigating whether a potential match is an actual target match or a false positive,
  - notifying senior management,
  - freezing accounts where appropriate and where an actual target match is identified,
  - keep a clear, documented audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.

All regulated entities must account for automated screening systems when applying CDD measures, demonstrating and evidencing, based on the information gathered, that the CDD measures applied are commensurate to the ML/TF risks they are exposed to.

Sincerely,

Demetra Kalogerou
Chairwoman of the Cyprus Securities and Exchange Commission