5TH EU MONEY LAUNDERING DIRECTIVE

ADAPTING TO CHANGES IN **AML COMPLIANCE**

LexisNexis®
RISK SOLUTIONS

The **5TH MONEY LAUNDERING DIRECTIVE** (5MLD)
came into being in January 2020 and is now known as :
The Money Laundering and Terrorist Financing (Amendment) Regulations 2019

The purpose of this guide is to summarise the key changes as a result of 5MLD and to support compliance teams in understanding the impact of these changes on their compliance requirements.

Why have the regulations changed?

As the financial landscape evolves, new channels and new financial products open up new opportunities for business and consumers, but also for financial criminals. As such, the Financial Action Task Force (FATF) has provided further guidance in a number of areas to tighten regulation around money laundering and terrorist financing.

Reflecting this, the EU launched the 5MLD, adopted by the European Parliament in April 2018, hot on the heels of the 4th Money Laundering Directive. Member states are expected to integrate 5MLD into individual country AML and CFT regulations from January 2020.

The additional requirements have been, in part, driven by recent events:

A significant change in terrorist attacks in Europe over the last five years.

The Panama Papers leaks which identified the extent to which offshore accounts are used to disguise beneficial ownership.

The adoption of cryptocurrencies and other digital channels for money laundering, which are currently unregulated sectors.

The EU's intent to ensure FATF anti-money laundering recommendations are implemented.

What were the main changes reflected in 4MLD?

4MLD was adopted by the UK in the 2017 Money Laundering Regulations and reflected in the amended Joint Money Laundering Steering Group guidance.

Key changes included:

Risk-based Approach

Requiring obliged entities to provide evidence that they have undertaken appropriate levels of customer due diligence (CDD) to fully understand the possible risks associated with a customer, both at the onboarding stage and then throughout the entire customer relationship.

Beneficial Owners

Mandating that organisations take steps to know the beneficial owners of corporate entities, trusts and individuals (where the transaction may be being conducted for a significant 3rd party who is not present). In addition, each country was required to establish a central registry of beneficial owner information which in the UK is the Persons of Significant Control Register established in 2016.

Politically Exposed Persons (PEPs)

Widening the definition to include persons who hold prominent positions in their home country. After careful consideration, the directive stated that PEPs must be monitored for a minimum period of 12 months after leaving office.

4MLD also mandated other changes, particularly in relation to record keeping and reducing limits on transaction values to trigger CDD.

The requirements of 4MLD have been retained in the 2017 Money Laundering regulations with the newly-updated regulatory amendments being added in accordance with 5MLD to form The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

Main additional requirements of 5MLD

1

Extension of sectors that are now 'obliged entities' and in scope of the updated regulations

Includes:

Cryptoasset exchange providers – entities that either exchange virtual assets to money or to other virtual assets. Or vice versa.

Custodian Wallet Providers – entities that provide services to safeguard, hold, store and administer virtual assets on behalf of its customers.

Letting Agents – firms that provide services for people either looking to let or rent land/property which has a monthly rent of 10,000 Euros or more.

Art Dealers – firms engaged in the business of trading in works of art which have a transactional value in one or a series of linked transactions greater than 10,000 Euros. The fuller definition of a work of art is referenced to the fuller definitions provided in the 1994 VAT Act.

Compliance Considerations

All newly obliged entities will require a full suite of policies, controls and procedures designed to meet their new regulatory obligations and designed for their specific business. Appointment and full training of competent persons – e.g. MLRO and Skilled Person – is also required.

With these sectors now formally classified as higher risk, existing obliged entities will need to carry out a risk assessment to understand whether they are transacting in these areas and ensure they are able to conduct appropriate Customer Due Diligence checks (in the case of virtual assets this will require screening of both the sender and the beneficiary). The European Supervisory Authorities (ESA) have issued new guidelines around risk assessment, identifying risk factors for certain business sectors that obliged entities should be familiar with.

Training will be required for staff, and the firm's Senior Management will need to engage with all existing AML policies.

Thoughts from LexisNexis® Risk Solutions

As obliged entities extend the scope of their controls to include these new sectors, it's a good opportunity to carry out a thorough review of the effectiveness of onboarding and screening processes. For example, if organisations are already experiencing high levels of false positives and costly alert remediation, broadening the sector base will only exacerbate the issue. Benchmarking of data, recalibrating risk settings and looking at new solutions that can significantly reduce the level of false positives can dramatically improve operational effectiveness and improve customer experience.

Main additional requirements of 5MLD

2

Politically Exposed Persons

Member states are required to keep an up-to-date list of the exact functions that qualify as prominent public functions. In addition, prominent functions of any international organisations hosted by the member state must be included. The European Commission aims to compile a single list of all prominent public functions, which will be made public.

Compliance Considerations

Key issues for consideration will be the accuracy and completeness of such lists, including how up to date they are. Note also that this only covers the EU region and that, outside of the EU, such lists may not exist for other countries.

PEP lists need to be accurate and conform to FATF guidelines, for global consistency. Organisations need to understand the criteria their PEP list provider is using to compile the list; how it is kept up to date; and the extent to which secondary identifiers are available to help reduce false positives. Commercial PEP list providers should also include any country specific lists such as those from EU countries, so-called micro PEP lists.

Enhanced due diligence measures are still required if a PEP is identified.

Thoughts from LexisNexis® Risk Solutions

Obliged entities need to be confident that they are using correct PEP definitions and that the PEP data they rely upon is accurate and up to date. It is not unusual for obliged entities to experience high levels of false positives when carrying out PEP screening. As such, PEP lists (commercial or independently generated), need to be reviewed constantly to make sure the data is up to date and contains secondary identifiers such as date of birth, sex, nationality, photo and where possible, date appointed to office. Ideally, PEP data list providers should also be able to offer obliged entities:

- the opportunity to communicate directly with their research teams, to check and verify available information;
- the ability to construct network charts, showing PEP associates and linked entities.

Main additional requirements of 5MLD

3

Beneficial Owners

Under 4MLD, member states were required to establish or maintain a central register of beneficial owner information on registered corporate or other legal entities that identify persons of significant control. This information must be publicly accessible. The UK created the Persons of Significant Control Register in 2016 mandating beneficial owner information to be reported from that date.

The amended regulations now require discrepancies relating to beneficial owner information found in the course of conducting due diligence to be reported. Companies House has provided detailed guidance as to what constitutes a reportable discrepancy and how to report it.

Compliance Considerations

Firms need to ensure that the details of the amended regulations are fully understood, and implement appropriate controls. In particular they should note situations of exemption such as legal privilege or those covered under the Companies Act 2006, such as the case for Limited Liability Partnerships.

Firms will recognise this is as a new additional obligation and should review their policies and procedures accordingly, to ensure that relevant persons are trained and capable of meeting this obligation.

There may also be data privacy considerations that need to be taken into account, balancing the privacy rights of the individual with public interests in the prevention of money laundering and terrorist financing.

Thoughts from LexisNexis® Risk Solutions

Obtaining beneficial owner information is a huge challenge for organisations as the Panama Papers scandle highlighted. There is no ‘silver bullet’ solution. Many registries around the world simply do not publish beneficial owner information, or else the information is partial and incomplete. Whilst an obligation for all newly formed entities to self-publish this information on national registers will help in time, currently there is no process to independently check and verify this information, making it difficult to rely upon for compliance purposes.

Often organisation structures are complex and include offshore entities. As a result, unpacking ownership structures and correctly identifying beneficial owners is a specialist skill requiring experienced and highly trained staff, particularly as these are the types of organisation that are most likely to be used by financial criminals. It is advisable for obliged entities to work with an experienced provider in order to assist with this process.

Main additional requirements of 5MLD

4

Customer Due Diligence in onboarding

The amended regulations add to the previous guidance, recognising the growing use of electronic identity verification (EIV) and adding a further option to conduct EIV with a trust service. However it states that such an outsourced solution must be from a trusted service that is secure from fraud and misuse. The only eIDAS* approved scheme currently available in the UK is GOV.UK Verify.

** EU 910/2014, the Regulation on electronic identification and trust services for electronic transactions – eIDAS*

Compliance Considerations

Firms will need to closely monitor the further development of trust services and can expect this sector to develop rapidly in the light of the amended regulations. For in-house processes, this is an area driven by new technology and obliged entities will need to ensure they have the technological infrastructure to support digital identification in onboarding. Migration from traditional physical identification and verification methods to digital identity should not be underestimated.

Thoughts from LexisNexis® Risk Solutions

While the 5MLD stipulates that electronic identification should be used wherever possible, it is widely believed that by 2020, electronic verification will become widespread. It is therefore prudent for all regulated firms to look at electronic solutions now, in preparation for the inevitable and begin this process as soon as possible.

Main additional requirements of 5MLD

5

Enhanced Due Diligence

Further requirements for enhanced due diligence measures are provided in the amended regulations. EDD is now required when transactions are complex, unusually large or there are unusual patterns of transactions, as well as where a transaction makes no sense from an economic or legal point of view.

Furthermore, a detailed list of the type of information that must be gathered in EDD checks is given in some detail and identifies specific situations requiring additional checks such as beneficiaries of life insurance policies or applications for citizenship rights from overseas persons when transfer of capital, bonds or property are involved.

Compliance Considerations

Obliged entities are advised to review their policies, controls and procedures to ensure that when the risk based approach indicates a higher level of risk, that appropriate checks are defined, implemented and in line with 5MLD. Firms should also note the newly-defined areas of 'higher risk'. Procedures will need updating to ensure that information is gathered as prescribed by the amended regulations and that controls are in place to ensure they are followed. Such checks will need to be in depth and explore the wider risks that can be encountered through associated entities or individuals, such as with PEPs.

Thoughts from LexisNexis® Risk Solutions

Many firms rely on their own resources to conduct enhanced due diligence checks, yet without the correct tools and support this can be time consuming and leave them exposed to unseen risk.

When enhanced due diligence searches rely mainly on the use of popular search engines, there is a danger of missing vital information. For example, checks on breaches of regulation, litigation cases, bankruptcy or insolvency notices require access to information that is often hidden behind firewalls or accessible only via subscription.

Knowledge of regional information sources and the ability to conduct checks in languages other than English is essential when dealing with overseas entities. Having access to local experts who know the local market and its culture will often uncover insightful information that might otherwise not be immediately obvious or readily available.

Main additional requirements of 5MLD

6

Other Areas

Payment Cards

In recognition of the fact that pre-paid cards are now widely used for financial crime and terror attacks, the new directive requires customer due diligence to be conducted to identify holders of pre-paid cards at a reduced threshold of €150 or more and any remote payment transactions over €50.

Compliance considerations in this area will require operational assessment and recalibration of payment systems to ensure the new thresholds trigger customer due diligence measures appropriately. In particular, the risk-based approach will need to reassess transactions when the source is in a high risk country, or with known poor AML controls, and when transactions are anonymous.

FIUs and Information Sharing

5MLD recognises that information sharing between Financial Intelligence Units (FIUs) plays a vital role in fighting money laundering and the financing of terrorism. Creation of central bank account and payment transaction registers and electronic data retrieval systems, to facilitate easier and quicker access of information by permitted authorities, will improve detection rates. Under 5MLD, FIUs will have the authority to obtain this information even if a Suspicious Activity Report has not been filed.

The challenge for compliance teams will be to ensure that they have the right controls and processes in place to collect, store and make customer account data available, on a timely basis and on demand.

We are likely to see further directives in the next two years in three key areas:

Further measures to improve information sharing between all stakeholders.

A requirement for obliged entities to develop an in-depth understanding of the predicate offences for money laundering and the criminal methodologies which give rise to these.

Tougher penalties for money laundering offences and further alignment of legislation with anti-bribery laws, creating a corporate offence for money laundering and the financing of terrorism.

How can LexisNexis® Risk Solutions help?

LexisNexis® Risk Solutions provides a comprehensive range of products and services that can assist firms in every area of the typical KYC/AML workflow, including initial customer onboarding, customer screening for sanctions, PEPs and adverse media, alert remediation, enhanced due diligence and ongoing monitoring.

Our products and services cover:

- **Identity Management**
- **Customer Data Management**
- **Financial Crime Compliance**

For more information, call **029 2067 8555**
or email **ukenquiry@lexisnexis.com**

risk.lexisnexis.co.uk

For more information, please call 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk