

Criminal Justice
(Money
Laundering and
Terrorist
Financing) Act
2010

DILLON  EUSTACE

DUBLIN CORK BOSTON NEW YORK TOKYO

CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010

Introduction


On 5 May 2010, the Third-Anti Money Laundering Directive (2005/60/EC) (the “Third AML Directive”) was finally transposed in Ireland by the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (“the Act”). The aim of the Third AML Directive is to widen the scope of previous anti-money laundering and terrorist financing legislation based on the revised recommendations of the Financial Action Task Force (“FATF”).

The Department of Justice and Law Reform has confirmed that the commencement date for the Act will be 15 July 2010, except for Chapter 9 of Part 4 (Authorisation of Trust and Company Service Providers). This leaves a very short time frame for all designated persons to comply with the new requirements.

Key Changes

The responsibilities of designated persons in relation to the prevention and detection of money laundering and terrorist financing has widened significantly with the implementation of the Act. The purpose of this memorandum is to consider the implications of the increased responsibilities on designated persons, which include credit institutions, financial institutions, life assurance companies and intermediaries providing life assurance and other investment related services, auditors, external accountants, tax advisors, independent legal professionals, trust or company service providers, property service providers, casinos, private members’ clubs in relation to gambling activities and any person who is trading in goods in cash for a total of at least €15,000 (whether this is a one off transaction or a series of transactions which appear to be linked to each other).

The Act introduces the following important changes for designated persons:

-  the definition of money laundering has widened to include the proceeds of any criminal conduct, however minor;

- ▣ the terminology of “know your customer” has been replaced by “customer due diligence” (CDD);
- ▣ the level of CDD required will be determined using a risk based approach. This can range from “simplified” where there is a low risk of money laundering or terrorist financing to “enhanced” where there is high risk of money laundering or terrorist financing;
- ▣ there are enhanced obligations to identify the “beneficial owner” whereby the designated person must ensure that they take reasonable measures to understand the ownership and control structure of the client;
- ▣ there is a new requirement to identify non domestic politically exposed persons (“PEPs”) as defined in the Act - i.e. those persons in a prominent public position and their families or close associates;
- ▣ those persons who meet the definition of “trust and company services provider” will need to be authorised;
- ▣ a guard at superintendant level or higher and/or a District Court judge has the power to direct a designated person not to carry out a specified service for a specific timeframe where a customer is subject to investigation;
- ▣ the number of offences that can arise under the Act are significantly greater than under the previous legislation;
- ▣ the Minister for Justice and Law Reform, in conjunction with the Minister for Finance, can approve the Guidance Notes to be used by designated persons. A Court can have regard to the Guidance Notes when determining if a designated person took all the appropriate measures.

We will now examine some of the more significant changes.

A Risk Based approach to Customer Due Diligence

Going forward, to be in a position to determine what is the appropriate level of customer due diligence, designated persons will be required to assess the risk of money laundering or

terrorist financing by conducting an internal risk assessment which considers factors such as the:

- ▣ nature of the customer base;
- ▣ nature of the products or services to be provided;
- ▣ methods of distribution; and
- ▣ geographic areas of operation.

The risk assessment will need to take into consideration the matters outlined in the Act as being deemed low risk and high risk.

If on completion of the risk assessment the designated person determines that the risk of money laundering or terrorist financing is “low” then “simplified due diligence” can be applied to the customer. At the other end of the scale where the designated person determines that the risk of money laundering or terrorist financing is “high” then “enhanced due diligence” is required. All other customers will have normal customer due diligence applied to them.

Customer Due Diligence

The significant change for designated persons is the timing whereby customer due diligence is required to take place. The Act specifies that the CDD must take place prior to the occurrence of any of the following circumstances:

- ▣ establishing a business relationship with a customer;
- ▣ carrying out a transaction or series of transactions for a customer greater than €15,000 (previously €13,000);
- ▣ carrying out a service for a customer if there is a suspicion of money laundering or terrorist financing;
- ▣ carrying out a service for a customer where there is doubt about the veracity or adequacy of previously obtained identification documentation.

There are a number of exceptions where a designated person is not required to operate CDD on a prior to basis as outlined above. In relation to life assurance business the

verification of the beneficiary of a life assurance policy can be deferred at the time a policy is taken out, however such verification must be carried out:

- ▣ prior to the policy being paid out, or
- ▣ prior to the beneficiary exercising any other right vested under the policy.

Other exceptions to the prior to rule are as follows:

- ▣ where a designated person has reasonable grounds to believe that prior identification would interrupt the normal conduct of business and there is no real risk that the service or customer is involved in money laundering/terrorist financing;
- ▣ a credit institution may allow a bank account to be opened before verifying identity, however no transactions can be carried out through the account until verification is completed.

In order to complete CDD, a designated person must complete the following:

- ▣ verify the customer's identity;
- ▣ identify any beneficial owner connected with the customer or service concerned;
- ▣ obtain information in relation to the purpose and nature of the business relationship; and
- ▣ carry out ongoing monitoring.

It should be noted that it is permitted to verify a customer's identity electronically, however due to the higher risk of exposure to impersonation when using electronic verification, one or more additional checks should be used. Typically, if electronic verification is relied upon then the first payment should be through an Irish/EU/Equivalent jurisdiction bank account in the customer's name.

Simplified Customer Due Diligence

The full CDD procedure outlined earlier is not required where a designated person is deemed to be dealing with a “specified customer” or a “specified product” so long as a number of conditions are satisfied. In such cases simplified CDD can be applied as the risk of money laundering or terrorist financing is deemed to be low.

Under simplified CDD a designated person is not required to:

- ▣ verify the customer's identity;
- ▣ establish the beneficial ownership;
- ▣ establish the purpose of the business relationship.

However, ongoing monitoring of the business relationship is required.

A specified customer is defined as:

- ▣ a credit institution or a financial institution that carries on business in Ireland or is situated in another EU member state that has adopted the Third AML Directive or is in a prescribed third country which has requirements equivalent to the Third AML Directive;
- ▣ any listed company admitted to trading on a regulated market;
- ▣ a public body;
- ▣ certain other EU public bodies.

A specified product is defined as:

- ▣ a life assurance policy where the annual premium is no more than €1,000 or the single premium is no more than €2,500;
- ▣ an insurance policy in respect of a pension scheme, which does not have a surrender clause and cannot be used as collateral;

- ▣ a retirement pension scheme for employees where the contributions are made by way of deduction from payroll and the rules of the scheme do not permit a member's interest to be assigned;
- ▣ electronic money up to certain limits.

It should be noted that there are certain circumstances where a designated person may be dealing with a "specified customer" or a "specified product", however they cannot avail of simplified CDD because:

- ▣ the customer is an individual and has not being physically present for identification purposes;
- ▣ the customer is from a country not deemed to have adequate procedures for the detection of money laundering or terrorist financing;
- ▣ there are reasonable grounds to believe there is a real risk that the customer is involved in money laundering or terrorist financing; or
- ▣ there is doubts about the adequacy of documentation previously received.

Enhanced Customer Due Diligence

The Act provides that enhanced CDD will apply:

- ▣ in any situation where there is a high risk of money laundering or terrorist financing;
- ▣ where the customer (who is an individual) has not been physically present for identification purposes;
- ▣ in the case of a non-domestic politically exposed person (PEP); and
- ▣ in the case of a correspondent banking relationship with a non EU credit institution.

Enhanced CDD involves seeking additional identification documentation and/or requiring the first payment to be made through an Irish/EU/Equivalent jurisdiction bank account in the customer's name.

Politically Exposed Persons (PEPs)

A PEP is defined in the Act as an individual who is, or has been entrusted with a prominent public function, or an immediate family member, or a known close associate of that person. It is important to note in this context that an individual ceases to be a PEP one year after he or she has left office.

Prominent public functions include among others - heads of state, heads of government, members of parliament, ambassadors and members of the courts of auditors or of the boards of central banks.

In relation to PEPs a designated person is required to:

- ▣ have appropriate risk-based procedures to determine whether the customer is a PEP;
- ▣ have senior management approval for establishing business relationships with such customers;
- ▣ take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
- ▣ conduct enhanced ongoing monitoring of the business relationship.

While a designated person with a predominantly domestic client base will have very low exposure to PEPs, those designated persons that are established to provide services to parties outside of Ireland have a higher exposure to PEPs and will need to implement measures to check PEP status such as a PEP database developed either in-house or sourced from an external provider.

Trust or Company Service Providers

Under Chapter 9 of Part 4 of the Act any person carrying out the business of a trust or company service provider ("TCSP") will be required to be authorised by the Minister and will be classed as designated person under the Act.

A TCSP is any person whose business involves:

- ▣ forming companies or other legal persons;
- ▣ acting as a director or secretary of a company under an arrangement with a person other than the company (e.g. personal service company);
- ▣ arranging for another person to act as a director or secretary of a company;
- ▣ acting as, or arranging for another person to act as a partner of a partnership;
- ▣ acting as or arranging for another person to act as (i) a trustee of an express trust, (ii) a nominee shareholder for another person (other than a company listed on a regulated market which is subject to disclosure requirements), or (iii) providing a registered office, business address, correspondence or administrative address or other related services for a company or a partnership.

Once a TCSP is authorised by the Financial Regulator, the authorisation will be valid for a period of three years.

It should be noted that a TCSP does not include the following (i) a member of a designated accountancy body, (ii) a barrister or a solicitor, or (iii) a credit institution or a financial institution.

The Department of Justice and Law Reform has not yet confirmed the commencement date for Chapter 9 of Part 4 (Authorisation of Trust and Company Service Providers) of the Act.

Reliance on Third Parties

Where a customer is introduced to a designated person by a “relevant third party” as defined in the Act, then the designated person can rely on the due diligence measures already taken by that third party so long as the designated person obtains a written confirmation from the third party setting out that:

- ▣ the third party is regulated/licensed by a competent authority;
- ▣ it has policies and procedures in place which meets with the requirements of the Third AML Directive or legislation equivalent to the Third AML Directive;
- ▣ it will retain the CDD documentation used to identify and verify its customers for a period of at least 5 years after the relationship with its customer had ended; and

- ▣ it will, on request by the designated person, make available copies of all relevant CDD documentation to the designated person.

However, it is important to remember that ultimate responsibility for customer due diligence still remains with the designated person.

In terms of the ongoing monitoring requirements applicable to a business relationship and transactions with the customer, this activity cannot be outsourced by a designated person to a third party. The designated person is responsible for this activity.

Reporting Suspicious Transactions

In terms of reporting suspicious transactions, designated persons and their directors and employees remain responsible for reporting any known or suspected suspicious transaction relating to money laundering or terrorist financing. Where a designated person has appointed a Money Laundering Reporting Officer (MLRO) employees should be instructed to file the suspicious transaction report (STR) with the MLRO who will investigate the matter and report it to the appropriate authorities.

Record Keeping

Under the Act, a designated person is obliged to keep the following documents and information for use in any investigation by the Gardai Siochana or the Revenue Commissioners or other competent authorities into any suspected cases money laundering or terrorist financing:

- ▣ in the case of customer due diligence, the designated person must keep records of the procedures applied and the information obtained about the customer. An original or copy of all documents used to verify the identity of the customer/beneficial owner must be retained for a period of at least five years after the relationship ceases with the customer or the date of the last transaction, whichever is the later;
- ▣ in the case of the ongoing monitoring, the designated person must keep records evidencing the history of services and transactions carried out in relation to that customer for a period of at least 5 years from the date on which the transaction was completed.

- ▣ copies of STRs made to the Gardai Siochana and the Revenue Authorities should be retained for at least five years;
- ▣ records relating to staff training include material used and attendance records should also be retained for a period of at least five years.

The records referred to above may be retained electronically so long as they are capable of being reproduced in electronic form.

Staff Training

To ensure compliance with the relevant provisions of the Act, designated persons will need to review and update their internal procedures to reflect the new requirements. Staff training in relation to customer due diligence and how transactions are classified as low and high risk will be required. To meet the ongoing monitoring obligation designated persons will need to have a thorough understanding of the nature and type of business activities that their customers are engaged in to determine what might constitute suspicious activity related to money laundering or terrorist financing. To this end, employees will be required to participate in ongoing education and training programmes to assist them in recognising practices that may be related to money laundering or the financing of terrorism and the appropriate action to take in such circumstances.

Conclusion

The challenges posed by the Act rest with the practical implementation of the risk based approach to CDD, the ongoing monitoring of business relationships and transactions and the identification of PEPs by designated persons. The risk based approach to CDD gives rise to extended obligations for designated persons and its effective implementation will require a multi-faceted and flexible approach in identifying relevant situations, assessing the risks and devising the most appropriate measures to tackle them.

Core Guidance Notes, which are currently under public consultation, are available on the Financial Regulator's website, while sector specific Guidance Notes for the Banking, Investment Funds, Stockbroking, Insurance and Credit Union sectors are at an advanced drafting stage. With only a matter of weeks left to the commencement date of 15 July 2010, designated persons need to ensure that their policies and procedures are updated to meet

and comply with the new requirements. The consequence of non-compliance with these requirements may result in a prison sentence of up to 5 years and /or an unlimited fine.

Date: June 2010
Author: Breeda Cunningham

CONTACT US

Our Offices

Dublin

33 Sir John Rogerson's Quay,
Dublin 2,
Ireland.
Tel: +353 1 667 0022
Fax.: +353 1 667 0042

Cork

8 Webworks Cork,
Eglinton Street,
Cork, Ireland.
Tel: +353 21 425 0630
Fax: +353 21 425 0632

Boston

26th Floor,
225 Franklin Street,
Boston, MA 02110,
United States of America.
Tel: +1 617 217 2866
Fax: +1 617 217 2566

New York

245 Park Avenue
39th Floor
New York, NY 10167
United States
Tel: +1 212 792 4166
Fax: +1 212 792 4167

Tokyo

12th Floor,
Yurakucho Itocia Building
2-7-1 Yurakucho, Chiyoda-ku
Tokyo 100-0006, Japan
Tel: +813 6860 4885
Fax: +813 6860 4501

e-mail: enquiries@dilloneustace.ie
website: www.dilloneustace.ie

Contact Points

For more details on how we can help you, to request copies of most recent newsletters, briefings or articles, or simply to be included on our mailing list going forward, please contact any of the team members below.

Partner – Paula Kelleher

e-mail: paula.kelleher@dilloneustace.ie
Tel : +353 1 673 1759
Fax: +353 1 667 0042

Director – Breeda Cunningham

e-mail: breeda.cunningham@dilloneustace.ie
Tel : +353 1 673 1846
Fax: +353 1667 0042

DISCLAIMER:

This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace.

Copyright Notice:

© 2010 Dillon Eustace. All rights reserved.

DILLON  EUSTACE

DUBLIN CORK BOSTON NEW YORK TOKYO

33 Sir John Rogerson's Quay, Dublin 2, Ireland.
www.dilloneustace.ie

In alliance with Arendt & Medernach