The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018

The primary purpose of the Act is to amend the 2010 Act, and to transpose the 4th Money Laundering Directive and to give effect to the recommendations of the Financial Action Task Force. It imposes obligations relating to assessing the risks of money laundering and terrorist financing; putting policies in place to mitigate that risk; and carrying out customer due diligence measures.

Please note this is a summary of the Act and is not definitive in respect of all new requirements. See Brokers Ireland Guidance Document on the Compliance Section of our website.

Designated persons
Any persons trading in goods that involve cash transactions of at least **€10,000** is now included as a 'designated person', lowering the previous threshold from €15,000.

Beneficial Owner
The Act removes the hard threshold of 25% meaning that an individual with less than a 25% shareholding or ownership interest could be considered a beneficial owner of a body corporate.

Business Risk Assessment
The Act introduces a requirement for designated persons to conduct a '**business risk assessment'** to identify and assess the risks. Designated persons must assess the level of risk of money laundering/terrorist financing involved in carrying out their own business activities.

Various specified risk factors must be taken into account: the type of customer, products and services, countries or geographical areas, type of transactions, delivery channels.

The business risk assessment must be documented and must be available to the relevant competent authority upon request. The business risk assessment must be **reviewed** and **managed** by a designated person at regular, predefined intervals and it must be **approved by senior management**.

It is an offence to fail to comply with these requirements.

How the risk assessment affects customer due diligence
In deciding the level of Customer Due Diligence (CDD) to be applied, the designated person when undertaking a transaction/entering a business relationship must consider a number of factors, including: the relevant business risk assessment, the purpose of an account/relationship, the level of assets deposited/the size of the transaction and the regularity of transactions/duration of the business relationship.

Due Diligence
In addition to the requirement under the 2010 Act that customer due diligence be carried out at particular times, the 2018 Act adds that CDD must be executed **at any time**, including situations where the relevant circumstances of a customer have changed, where the risk of money laundering/terrorist financing warrants its application.

Where a person purports to act on behalf of a customer, a designated person will be obliged to verify (a) the identity of that person, and (b) that they are authorised to so act.

Simplified Customer Due Diligence (SDD)

Designated persons will be allowed to carry out SDD where the customer or business area is considered to be low risk. SDD can only be applied where a designated person has **identified in its business risk assessment, an area of lower risk** into which the relationship or transaction falls, and the relationship or transaction concerned can reasonably be considered to be low risk. Please see schedule three and four of the 2018 Act for a list of factors suggesting potentially lower and higher risk.

Where this section is applied, the reasons for its application and the evidence on which it was based must be recorded and the business relationship and transactions must be monitored to enable the designated person to detect unusual or suspicious transactions.

Enhanced Customer Due Diligence

1) *High risk third countries*
   A designated person is required to apply enhanced customer due diligence measures when dealing with a customer **established or residing in a high-risk third country**. There is an exemption that applies when the customer is a branch or majority-owned subsidiary of a designated person established in the European Union which complies with the group's group-wide policies and procedures. These cases must be dealt with using a risk-based approach.

   It is an offence to fail to comply with these requirements.

2) *Relationship/transaction presents a higher risk*
   A designated person is required to apply enhanced customer due diligence measures where a **business relationship or transaction** presents **a higher degree of risk**. This is to applied where the relationship or transaction concerned can reasonably be considered, having regard to certain matters, to be high risk.

   It is an offence to fail to comply with these requirements.

Monitoring

A designated person is required to investigate "**complex or unusually large**" transactions, or "**unusual patterns of transactions**" in greater detail and increase monitoring if they appear suspicious.

It is an offence to fail to comply with these requirements.

Politically Exposed Persons (PEPs)

Due diligence measures that previously applied only to PEPs resident outside of Ireland now also apply to PEPs resident in Ireland.

Life Assurance Policies/PEPs

Additional requirements are imposed regarding the identification of the beneficiaries of life assurance policies and other investment-related assurance policies. Specific steps must be taken where the **PEP is a beneficiary of a life assurance policy**. If a designated person knows or has reasonable grounds to believe that a beneficiary of a life assurance or other investment-related assurance policy or a beneficial owner of the beneficiary concerned, is a politically exposed person, or an immediate family member or a close associate of a politically exposed person, it shall:

(a) inform senior management before pay-out of policy proceeds and
(b) conduct enhanced scrutiny of the business relationship with the policyholder

Internal policies, controls and procedures
A designated person shall adopt internal policies, controls and procedures in relation to the designated person's business to prevent and detect the commission of money laundering and terrorist financing. These requirements also apply to persons to whom AML obligations have been outsourced.

The internal policies, controls and procedures shall include:

(a) identification, assessment, mitigation and management of risk factors relating to money laundering/terror financing
(b) customer due diligence measures
(c) monitoring transactions and business relationships
(d) the identification and scrutiny of complex/large transactions, unusual patterns of transactions and any other activity that the designated person has reasonable grounds to regard as particularly likely to be related to money laundering/terrorist financing
(e) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,
(f) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments,
(g) reporting (including the reporting of suspicious transactions),
(h) record keeping,
(i) measures to be taken to keep documents and information relating to the customers of that designated person up to date,
(j) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,
(k) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and
(l) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures.

Documents and other records relating to clients shall be kept for a period of not less than five years.

A designated person shall ensure that the policies, controls and procedures are **approved by senior management** and shall keep these policies, controls and procedures **under review** in particular when there are changes to the business profile or risk profile of the designated person. These policies, controls and procedures shall have regard to any guidelines issued by the competent authority.

A designated person must ensure that persons involved in the conduct of the business (includes directors, other officers and employees) receive instruction and training in respect of the law and on how to identify transactions or other activity that may relate to money laundering or terrorist financing (suspicious transactions) and how to proceed once identified.

It is an offence to fail to comply with these requirements.

Requests from An Garda Síochána for client information/records
For the purposes of providing information to the Garda Síochána this must be requested in writing be a member of the force not below the rank of Sergeant (who may give a direction, which must also be in writing, to retain the documents/other related records for a period up to a maximum of five years.

Non exhaustive List of factors considered potentially lower risk

Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
(b) public administrations or enterprises;
(c) customers that are resident in geographical areas of lower risk as set out in subparagraph (3).

Product, service, transaction or delivery channel risk factors:

(a) life assurance policies for which the premium is low;
(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

Geographical risk factors:

(a) Member States;
(b) third countries having effective anti-money laundering (AML) or combating financing of terrorism (CFT) systems;
(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised Financial Action Task Force (FATF) recommendations and effectively implement these requirements.".

Non-exhaustive list of factors suggesting potentially higher risk

Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;
(b) customers that are resident in geographical areas of higher risk as set out in subparagraph (3);
(c) non-resident customers;
(d) legal persons or arrangements that are personal asset-holding vehicles;
(e) companies that have nominee shareholders or shares in bearer form;
(f) businesses that are cash intensive;
(g) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

Product, service, transaction or delivery channel risk factors:

(a) private banking;
(b) products or transactions that might favour anonymity;
(c) non-face-to-face business relationships or transactions;
(d) payment received from unknown or unassociated third parties;
(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Geographical risk factors:

(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
(c) countries subject to sanctions, embargos or similar measures issued by organisations such as, for example, the European Union or the United Nations;
(d) countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.".