

Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2018

The long awaited Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2018 (the [Bill](#)) has now been published.

The Bill gives effect to the Fourth Money Laundering Directive (Directive (EU) 2015/849 (4AMLD)) and proposes a range of amendments to existing anti-money laundering (AML) legislation set out in the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 and 2013. The Bill does not repeal the current legislation. Going forward, all businesses falling within the scope of this legislation will need to be mindful of three separate Acts and any further associated guidance to be issued.

Risk Assessment (s. 10)

- In line with the focus of 4 AMLD on applying more rigour through a risk based approach, it is now a statutory requirement to conduct an AML risk assessment (this was previously referred to in regulatory guidance, including the Department of Justice Guidelines on the 2010 Act).
- Designated persons will now be required to conduct a specific assessment of the ML/TF risks involved in carrying out their business (referred to in the Bill as a “**business risk assessment**”). In addition to the typical risk factors relating to customer, product type, geographical considerations etc., designated persons must have regard to a range of other matters, including the National Risk Assessment, any guidance on risk issued by a relevant competent authority and, in the case of credit institutions and financial institutions, any guidelines issued by the European Banking Authority, the European Securities and Markets Authority or the European Insurance and Occupational Pensions Authority.
- A business risk assessment must be documented unless a competent authority confirms that this is not required and notifies the designated person accordingly. Records of the risk assessment must be available on request to the relevant competent authority.
- Senior management engagement with the risk assessment process is also provided for by the Bill. Risk assessments must be approved by senior management and businesses must keep their risk assessment up to date. “Senior management” is defined for this purpose as “an officer or employee with sufficient knowledge of the institution’s money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors”. This definition is wide enough to apply potentially to a range of business roles outside of those senior executives who are accountable to the board for the day to day running of the business, including the MLRO and Head of Compliance.
- This sharper focus on risk assessment is supported by penalties and sanctions for failure to comply with the relevant requirements.

Customer Due Diligence (CDD) and Risk Assessment (s.10)

- While the 2010 Act envisaged different levels of CDD for certain categorisation of customer relationships, the Bill makes it clear that the ML/TF risk of a particular customer relationship should fully inform the approach

to CDD and the level of rigour applied to that customer.

- Designated persons are required to assess ML/TF risk in relation to a range of factors, including taking into account the relevant business risk assessment, and any risk variables, including the purpose of an account or relationship, the level of assets to be deposited by a customer or the size of the transactions undertaken as well as the risk factors set out in the Schedules to the Bill.
- A competent authority may direct a designated person to document its risk determination relating to a particular customer relationship. The discretion of the competent authority to make such a direction will be informed by the size and nature of the designated person's business. Failure to comply with such a direction will be an offence. Similarly, a State competent authority may direct a class of designated persons to document their risk determinations.

Changes to CDD Rules (s. 11, 12)

- A new provision states that CDD must be applied at any time where the risk of ML/TF warrants their application, including a situation where the relevant circumstances of a customer have changed. This reinforces the need to assess the adequacy of steps originally taken for CDD purposes should a designated person identify, through its ongoing monitoring of customer activity, that the ML/TF risk of a particular customer relationship has changed.
- In addition to verifying the identity of a person acting on behalf of a customer, the Bill requires verification of their authority to so act. This brings an additional layer of compliance to the process.
- The flexibility currently provided to credit institutions to allow an account to be opened before CDD measures are completed, provided no transaction is conducted, is extended to all 'financial institutions'. This corrects a long standing anomaly in Irish AML legislation. There is also clarity that this flexibility applies to accounts that permit transactions in transferable securities.
- New detailed provisions setting out the CDD measures relating to beneficiaries of trusts and life assurance policies are included.
- The Bill includes an exemption from some

CDD measures in respect of electronic money where certain conditions are satisfied including that the monetary value that can be stored on the instrument must not exceed prescribed financial thresholds. This exemption will not apply where the customer is established or resident in a high risk third country or if the customer or beneficial owner is a politically exposed person (PEP). The EU Commission issues a list of high-risk third countries for the purposes of 4AMLD.

Simplified Customer Due Diligence (SCDD) (s. 13)

- The Bill moves away from the 'rules based' approach to SCDD as currently reflected in Section 34 of the 2010 Act. This allowed SCDD to be applied to specified categories of customers and business lines perceived as presenting low ML/TF risk. The Bill reflects the risk based approach endorsed by the 4 AMLD. It now provides that SCDD can only be applied where a designated person is satisfied that the relevant business presents a low ML/TF risk and where it has considered a range of matters in reaching this conclusion, including the 'low risk factors' set out in Schedule 3 to the Bill.
- Designated persons must retain records supporting the reasons for their determination in this regard and the evidence on which it was based must be maintained. Designated persons must also conduct sufficient monitoring of customers' transactions and business relationships to enable the designated person to detect unusual or suspicious transactions.
- The upshot of this is that the application of SCDD based on a customer's status (for example, as a credit institution) is no longer permitted. In practice, there may be little impact here insofar as customers who were eligible for SCDD profiling under the 2010 Act may, following an appropriate risk assessment, still be classified as low risk customers. However, further diligence and risk assessment of individual customers is now required before this assessment can be concluded for any particular customer relationship.

Enhanced CDD (s. 18, 19)

- The Bill requires designated persons to make a risk based assessment and judgment as to whether a customer or business line present a

higher degree of ML/TF risk. This risk must be assessed having regard to a range of factors noted above, including the factors set out in Schedule 4 to the Bill (which sets out specific indicators of high risk). The Bill sets out specific and harmonised enhanced customer due diligence (ECDD) steps which must be applied in these situations.

- The Bill also requires that these harmonised ECDD steps be applied when dealing with a customer established or residing in a high risk third country. These steps may not need to be applied when the customer is a branch or majority owned subsidiary of an EU based entity which complies with the group's 4 AMLD compliant group-wide policies and procedures.

Politically Exposed Persons (PEPs) (s. 16)

- The Bill extends the definition of a PEP to include domestic PEPs (persons residing in the State). The Bill extends the requirement to determine if a customer, or a beneficial owner connected with the customer or service concerned, or a beneficiary of a life assurance policy or other investment related assurance policy, or a beneficial owner of the beneficiary, is a PEP (or an immediate family member or close associate of a PEP). In addition, the section sets out the measures to be taken when a beneficiary of a life assurance policy is a PEP.

Correspondent Relationships with Third Country Respondent Institutions (s. 17)

- The prohibition in the 2010 Act on credit institutions entering into correspondent banking relationships with credit institutions outside the EU, unless certain conditions are fulfilled, is extended to all financial institutions.

Correspondent Relationships with Shell Banks (s. 31)

- The current prohibition on credit institutions from entering into a correspondent relationship with shell banks is extended to financial institutions

Third Party Reliance Arrangements (s. 20)

- The Bill amends Section 40 of the 2010 Act which concerns the circumstances under which a designated person may rely on a third

party to carry out CDD. The Bill prohibits reliance on third parties established in high risk third countries, except in the case of branches or majority owned subsidiaries of a designated person established in the EU where these branches or subsidiaries are compliant with group-wide 4AMLD compliant procedures. Current provisions require that the third party is supervised or monitored for compliance with AML legislation and that the Firm is satisfied that the third party will forward the relevant documents to the Firm. Under the Bill certain of these conditions are eased.

Record Keeping Requirements (s. 27)

- The Bill provides for the deletion of personal data collected as part of CDD after prescribed retention periods unless otherwise directed by the Garda Síochána or required for the investigation or prosecution of money laundering.

Monitoring (s. 4)

- The Bill introduces a new definition of 'monitoring' in relation to a business relationship between a designated person and a customer. Monitoring of a business relationship is envisaged by Section 35 of the 2010 Act. This sets out the steps that are envisaged for such monitoring. The Bill aligns the monitoring exercise required with the risk assessment by stipulating that the designated person must also ensure that the customer's transactions are consistent with the customer's risk profile.

Examination of Background and Purpose of Certain Transactions (s. 15)

- Designated persons shall, in accordance with policies and procedures, examine the background and purpose of all complex and unusual transactions and increase the degree and nature of monitoring in order to determine whether the transaction appears suspicious. Again, the Bill is aligning the broader CDD requirements with the policies and procedures of the designated person.

Beneficial Owners (s. 6, 7, 8)

- The 4AMLD places increased focus on understanding the beneficial ownership of customers. It sets out the meaning of

'beneficial owner' in the context of corporates, partnerships and trusts. These definitions are carried over by the Bill.

- **Beneficial owner – body corporate.** The definition of “beneficial owner” in the Bill also mirrors the definition contained in the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations, 2016, that is the meaning given to it by Article 3 (6)(a) of the 4 AMLD. This defines the term, in the case of corporate entities, as the natural person(s) who ultimately owns or controls the entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights in that entity or through control by other means as referred to in the relevant article. A percentage of 25% plus one share held by a natural person is stated to be evidence of direct ownership and a shareholding of over 25% held by a corporate entity under the control of a natural person(s) or by multiple corporate entities which are under the control of the same natural person(s) is stated to be an indication of indirect ownership.
- **Beneficial owner – partnership.** Previously, where an individual was not entitled to or did not control (either directly or indirectly) more than a 25% share of the capital or profits of a partnership, or more than 25% of the voting rights in the partnership, they would only fall within the definition of 'beneficial owner' where they controlled the management of the relevant partnership. The Bill extends this definition of beneficial owner to any person who “controls” a partnership.
- **Beneficial owner – trust.** The definition of beneficial owner in the context of trusts in the 2010 Act is amended so that the definition no longer only applies to trusts that administer and distribute funds. The threshold of 25% ownership no longer applies and settlors, trustees and protectors are now to be considered beneficial owners.

Functions and Powers of the Financial Intelligence Unit (s. 21, 22)

- The Bill sets out the role, functions and powers of the Financial Intelligence Unit (FIU), which is part of the Garda Síochána.
- The FIU is responsible for receiving and analysing suspicious transaction reports and other information relating to MT/TF. The FIU's analysis function will involve conducting

an operational analysis which focuses on individual cases and specific targets or on appropriate selected information depending on the type and volume of the disclosures received and the expected use of the information after dissemination. It will also conduct a strategic analysis addressing ML/TF trends and patterns.

- The FIU may access the beneficial ownership registers which are to be established under Articles 30 and 31 of the 4 AMLD
- The FIU may request information from designated persons, competent authorities, the Revenue Commissioners and the Minister for Employment Affairs and Social Protection (the Minister) so as to carry out its functions
- The FIU must respond to requests from competent authorities, the Revenue Commissioners and the Minister where there are grounds to suspect ML/TF. The FIU will also have a power to share certain information with FIUs in other EU Member States.
- Consequential amendments are made to other provisions of the legislation, including reporting obligations, so that STRs are received by the FIU Ireland.

Reporting (s. 25)

- The requirement in current law for designated persons to report all transactions with countries specified in an order made under Section 31 of the 2010 Act is replaced with a requirement to make a report in respect of all transactions with certain high risk third countries.

Amendment to the Tipping-off Defence (s. 24)

- Section 51 of the CJA 2010 establishes defences to the offence of tipping-off. They include making a disclosure that an investigation into ML/TF is being contemplated or carried out. The defence currently applies where disclosures are made between credit and financial institutions within the same group. The Bill extends this defence to disclosures made to majority owned subsidiaries and branches within the same group. It also imposes a requirement for the defence to be available, that the institutions concerned were in compliance with the group's policies and procedures.

Policies and procedures (s. 26)

- There are a number of changes to the rules relating to the policies and procedures which must be maintained by a designated person.
- The Bill introduces more detailed requirements as to what matters policies and procedures should cover. Essentially, it is envisaged that that they should address all aspects of AML/CTF compliance.
- Policies and procedures must be approved by senior management and kept under review.
- A designated person must ensure that persons involved in the conduct of the business are instructed on money laundering law and provided with training.

Competent Authorities May Impose Additional Obligations (s. 26)

- A competent authority may also direct a designated person to appoint an individual at management level to be called a compliance officer to monitor and manage compliance with, and the internal communication of, internal policies, controls and procedures adopted by the designated person.
- A competent authority may also direct a designated person to appoint a member of senior management with primary responsibility for the implementation and management of AML measures.
- Similarly, a competent authority may direct a designated person to undertake an independent external audit to test the effectiveness of the internal policies controls and procedures. The decision to make such directions will be informed by the scale and complexity of the designated person.

Requests from the Garda Síochána for Records (s. 27)

- There is an amendment to the section which requires credit and financial institutions to have systems in place to enable it to respond to enquiries from the Garda Síochána as to whether it has had a business relationship with a specified person within the previous 6 years. This requirement is now extended to all designated persons and the relevant period is reduced from 6 years to 5 years.

Group-wide Policies (s. 29, 30)

- The Bill requires the implementation of

group-wide policies and procedures to be implemented by any designated person that is part of a group. A designated person incorporated in the State that operates a branch, majority owned subsidiary or establishment must ensure that it adopts and applies group wide policies and procedures. Designated persons with branches and subsidiaries in other Member States may apply the law of those Member States which transposes the 4AMLD. Designated persons with branches and subsidiaries in third countries which have less strict money laundering laws than those of the State must apply the requirements of the State. Where the law of the place that is not a Member State does not allow the application of those policies and procedures, the designated person must ensure that additional measures are applied and inform the relevant competent authority. The Bill sets out actions which the competent authority may take in these circumstances.

- STRs may be shared within a group, subject to the tipping off offence.

Supervision (s. 34)

- Certain financial institutions who are not otherwise authorised by or registered with the Central Bank are now obliged to register with the CBI to enable it to identify the persons whom it is responsible for supervising for AML purposes. Failure to register is an offence.

Sanctions (s. 35)

- The Bill provides additional detail on the monetary penalties which are to apply where the CBI applies the administrative sanctions regime in respect of AML contraventions. In addition to the monetary limit of €10m and 10% of annual turnover for corporate entities, and €1m for individuals, financial penalties can now be increased to twice the amount of any benefit derived from the relevant contravention which may be higher than the previous limits.

Central Registers of Beneficial Ownership

- While the Bill transposes the bulk of the 4AMLD, some aspects will be transposed by the Department of Finance. (i.e., the establishment of registers of beneficial ownership of companies and trusts).

Key contacts



Dario Dagostino
Partner
+353 1 649 2308
ddagostino@algoodbody.com



Kevin Allen
Partner
+353 1 649 2338
kallen@algoodbody.com



James Grennan
Partner
+353 1 649 2318
jgrennan@algoodbody.com



Paula Reid
Partner
+353 1 649 2348
preid@algoodbody.com



Kenan Furlong
Partner
+353 1 649 2260
kfurlong@algoodbody.com



Nollaig Greene
Knowledge Lawyer
+353 1 649 2359
ngreene@algoodbody.com

Disclaimer: A&L Goodbody 2018. The contents of this document are limited to general information and not detailed analysis of law or legal advice and are not intended to address specific legal queries arising in any particular set of circumstances.