TRANSPOSITION OF THE 5TH EU MONEY LAUNDERING DIRECTIVE

March 2020

This newsletter is not a substitute for seeking professional advice and has no legal standing.

This newsletter only covers substantive amendments as a result of the transposition of 5MLD, and readers are advised to seek their own professional advice on the application of Regulations and compliance with the same.

This newsletter covers amendments made to legislation in order to transpose the EU's 5th Money Laundering Directive (2018/843) "5MLD" through the Proceeds of Crime Act 2015 (Amendment) Regulations 2020 (5MLDRegs) published on the 13th March 2020 (LN110 of 2020).

The 5MLDRegs amend the following pieces of legislation;

1. Proceeds of Crime Act 2015
2. Register of Ultimate Beneficial Owners Regulations 2017
3. National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016
4. Supervisory Bodies (Powers etc.) Regulations 2017
5. Terrorism Act 2018

AMENDMENTS TO THE PROCEEDS OF CRIME ACT 2015 (POCA)

Information Request

Through the introduction of a new section of POCA, 1DAA, the GFIU is now empowered to seek information from a relevant financial business (RFB) in pursuit of its functions (see S1C) that is no longer restricted to information pursuant to a suspicious transaction report (STR).

The same criteria that used to previously apply to information requests for STRs (See S1DB) continues to apply to these wider requests.

The information must be supplied within such time as GFIU considers reasonable.

International Co-operation

GFIUs powers to co-operate with other FIUs on all criminal matters, not just those concerning tax offences, is clarified in the amendments to S1IB and S1IC, which highlights the requirement on all FIUs subject to 5MLD co-operate regardless of the type of associated predicate offences or differences in legal definitions and interpretations of criminal conduct.

Tipping Off Liability

An amendment to S5(5) clarifies that liability for tipping off shall not be extended in respect of disclosures made between different branches of credit institutions or financial institutions which are members of the same group.

Protection of individuals making disclosures

Individuals working at relevant financial business who make disclosures (whether internally, to the relevant supervisory authority or to the GFIU) are now afforded greater protections through the amendments to S6A(2)(b) which requires ensuring that individuals are not exposed to threats, retaliatory action by other

employees, management or customers as well as protections from discriminatory employment actions and also providing that these individuals can make a compliant in a safe manner.

New regulated activities

A number of definitions have been inserted into S7 of POCA mainly dealing with new types of activities now covered by POCA as relevant financial business as well as updating others.

The new activities now covered are;

- Art market participants
- Letting agents; and
- Tax Advisors.

5MLD also brings about changes with respect to the mandatory registration and regulation of providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers across the EU. As early as 2018, however, Gibraltar had already legislated for the regulation of entities in the distributed ledger technology space through earlier amendments to POCA and other financial services legislation.

Customer Due Diligence (CDD)

The application of CDD measures is extended to include new forms of electronic identification measures (S10(a)). See also new definitions inserted into S7 which explains these in more detail.

Electronic ID is also captured in amendments made to S25 (Record Keeping) and Schedule 7.

Lower Limits for CDD on certain e-money products

The definition of e-money now included in S7 excludes "monetary value" referred to in Article 1(4) and (5) of the E-Money Directive namely;

(1) services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;

(2) payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

This now clarifies that CDD is not required to be performed on these e-money products.

Identification of Ultimate Beneficial Ownership

Amendments also made to s.10(b) in respect of CDD measures reiterate the more specific requirements below.

Legal entities
The update made to S7(1A)(a)(ii) alters how the Ultimate Beneficial Owner (UBO) of a corporate body is recorded.

The requirement to drill down to a natural person who owns or controls the legal entity remains unchanged (paragraph (i)). However, if after having exhausted all possible means, no person is identified under (i) or there remains a doubt that the person identified under (i) is the UBO, the RFB must take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official. Once again, the emphasis here is on natural persons and verification, not just identification. RFBs are now also required to keep records of the actions taken and document and difficulties encountered during the verification process.

Trusts
In the case of trusts the UBO definition (S7(1A)(b)) now applies in respect of more than one settlor, trustee and protector and not, as was previously, in the singular.

Application of CDD

Amendments to S11(2) expands the triggers for when CDD measures need to be applied, which are extended from the previous requirement of when the circumstances of the customer changes to also require this when;

- reviewing the UBO data held;
- pursuant to the Income Tax Act; or
- pursuant to the Tax (Mutual Administrative Assistance) Act 2014.

UBO Register extracts

RFBs are also now required (S11(4A)) to obtain an copy of the extract from the Register of Beneficial Owners or proof of registration of the same whenever CDD is required to be applied to a trust, corporate or legal entity which is itself required to register its UBO data in the register.

Enhanced Due Diligence (EDD)

The requirement to examine, as far as is reasonably possible, the background and purpose of transactions is now triggered if any ONE of the following conditions is met (S17(3));

(a) they are complex transactions;
(b) they are unusually large transactions;
(c) they are conducted in an unusual pattern;
(d) they do not have an apparent economic or lawful purpose, and in particular, a relevant financial business shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

S17 now also includes specific requirement for transactions and business relationships with high-risk countries (as defined in S17(1)(b) by the European Commission). The following EDD measures must be applied in those cases;

(a) obtain additional information on the customer and on the beneficial owners;
(b) obtain additional information on the intended nature of the business relationship;
(c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owners;
(d) obtain information on the reasons for the intended or performed transactions;
(e) obtain the approval of senior management for establishing or continuing the business relationship; and
(f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Supervisory authorities may give directions to RFBs to apply more or additional mitigating measures for these transactions and/or business relationships (s.17(7)). These additional measures are now set out in Schedule 8 and may require a person to whom a direction is given (a "relevant person") to undertake the following:

(a) enhanced due diligence;
(b) ongoing monitoring;
(c) systematic reporting; or
(d) limiting or ceasing business.

Supervisory authorities may also require external audits in respect of branches or subsidiaries of a RFB where these are located in a high-risk country (s.17(8)).

Correspondent Banking with 3rd country respondents I high-risk countries

Supervisory authorities of financial or credit institutions which have correspondent banking relationships with correspondents in high-risk countries may issue directions to review, amend or terminate such relationships (S17A(2)).

AMENDMENTS TO REGISTER OF ULTIMATE BENEFICIAL OWNERS REGULATIONS 2017 (RUBOR)

UBO data to be adequate, accurate and current

R8A of RUBOR now not only requires the disclosure to the corporate or legal entity of the UBO but also for the UBO to provide it with any information which is reasonably required for it to comply with Regulation 6 (adequate, accurate and current) within 15 days of becoming a UBO.

Express trusts UBO data

Amendments made to R9(4) now address the plurals as well as singularities of settlors, trustees, protectors and beneficiaries.

Access to the Register of UBOs

By replacing in r.26(1)(d) "a person or organisation that demonstrates a legitimate interest" with "a member of the public" the Register of UBOs is now a public register. However, members of the public are limited to the following information in respect of a UBO;

- the name;
- the month and year of birth
- the nationality;
- the country of residence;
- the nature and extent of the beneficial interest.

Access to this information is via an electronic portal https://ubosearch.egov.gi and requires pre-registration and the payment of a small fee being £2.50 per search in line with r. 29 and the new r.29A.

5MLD measures for trusts other than those with a tax consequence in Gibraltar to file information on the private register of trusts have been identified and legislative measures bringing these into effect have been drafted, but are not yet signed into law as of the date of this newsletter. This is expected to occur once the Government has concluded its private consultation with the Association of Trust and Company Managers.

Duty to report inconsistencies

As mentioned above, RFBs now have to obtain an extract/confirmation of registration from the UBO register (Register) or a foreign register for legal entities with which they a have a business relationship (S11(4A) of POCA). R26A of RUBOR makes it a requirement, when it is apparent to the obliged entity (RFB) that the information in the register is materially inconsistent with any information in its possession, for the RFB to report this to the Registrar within 30 days (R26A). These 30 days can be extended with the consent of the Registrar.

There is no doubt that neither POCA nor RUBOR exempts the RFB from conducting its own CDD to identify the UBO and the extract from the Register is not a replacement of UBO requirements but works in the opposite direction to ensure that the data in the Register is adequate, accurate and current.

There is no obligation on the RFB to inform the legal entity of these inconsistencies, but it is at liberty to do so. It is up to the Registrar to address reported inconsistencies with the legal entity until they have been clarified to his satisfaction, and under further changes to r.26 the Registrar may take such measures as he considers necessary or expedient to clarify the inconsistencies, including (but not limited to) placing such notice in the Register as he considers appropriate.

Bank Account and Safe Deposit Registers

RUBOR now also provides for the establishment of a central automated system (i.e. a central register or data retrieval system), allowing access to information on the persons who control or hold payment accounts, bank accounts and safe-deposit boxes (R41B to R41I).

All credit institutions and providers of safe custody services must therefore establish and maintain systems which enable it to respond to a request for information by a relevant authority (meaning GFIU, RGP, HMC and the FSC (r.41I(c)).

The following data may be requested for bank accounts (R41D(2));

(a) the name of the account holder;
(b) where the account holder is an individual, the date of birth of the account holder;
(c) where the account holder is an individual, the address of the account holder;
(d) where the account holder is a firm, the address of its registered office and, if different, its principal place of business;
(e) the name of any person purporting to act on behalf of the account holder;
(f) the name and date of birth of any individual with a beneficial interest in the account or the account holder;
(g) the address of any individual with a beneficial interest in the account or the account holder;
(h) where the beneficial interest in the account holder is held by a firm, the address of its registered office and, if different, its principal place of business;
(i) the International Bank Account Number (IBAN) of the account;
(j) any other number by which the individual account is identified by the credit institution;
(k) the date of opening of the account;
(l) if the account has been closed, the date of closing; and
(m) any other numbers which are specific to an individual who is mentioned in sub-paragraphs (a) to (c) or (e) to (g) and which may be used to verify that individual's identity (such as a passport or driving licence number) contained within any documents or information obtained by the credit institution to satisfy the customer due diligence requirements in sections 10, 10A, 11 and 17 to 22 of POCA.

In respect of safe-deposit boxes the following information may be requested (R41E(2));

(a) the name of the customer to whom the safe-deposit box was or is made available;
(b) where the customer is an individual, their date of birth;
(c) where the customer is an individual, their address;
(d) where the customer is a firm, the address of its registered office and, if different, its principal place of business;
(e) the name of any person (except for employees of the provider of safe custody services) who the provider of safe custody services knows holds, or held, a key for the safe-deposit box, or has or has had access to the safe-deposit box in any other way;

(f) the date on which the safe-deposit box was made available to the customer and, if appropriate, ceased to be available; and

(g) any other numbers which are specific to an individual who is mentioned in sub-paragraphs (a) to (c) and (e) and which may be used to verify that individual's identity (such as a passport or driving licence number) contained within any documents or information obtained by the provider of safe custody services to satisfy the customer due diligence requirements in sections 10, 10A, 11 and 17 to 22 of POCA.

R. 41F, however, imposes significant restrictions on information requests, namely;

1. Only a relevant authority (see above) may request information;
2. the GFIU may only request information for a purpose connected to one of its functions;
3. the Royal Gibraltar Police, HM Customs, and the Financial Services Commission may only request information for one (or more) of the following purposes-
    a. to investigate money laundering, terrorism (within the meaning of section 4 of the Terrorism Act 2018), or terrorist financing;
    b. to investigate whether property has been obtained through any conduct mentioned in sub-paragraph (a); or
    c. to carry out its supervisory functions (where the relevant authority carries out a supervisory function).
4. Only an appropriate officer specifically authorised to make requests may make a request on behalf of that authority.
5. A senior officer of the relevant authority must approve every request in writing, and must only extend approval upon being satisfied that the request complies with the requirements of r.41F and is proportionate to the purpose or purposes of the request.

AMENDMENTS TO THE NATIONAL COORDINATOR FOR ANTI-MONEY LAUNDERING AND COMBATTING TERRORIST FINANCING REGULATIONS 2016.

National Risk Assessment (NRA) & Statistics

A summary of any NRA is now required to be made public (R7(3)).

The uses of the NRA have been expanded to include reporting on the national efforts and resources allocated to combat money laundering and terrorist financing as well as the institutional structure and broad procedures of the AML/CFT regime including human and financial resources available (R8(f) & (g)).

The gateways for the NCO to receive information for the purposes of the NRA is now also extended to the Commissioner of Income Tax (R10(a)). The data available to the NCO is also opened up through amendments made to R12.

AMENDMENTS TO THE SUPERVISORY BODIES (POWERS ETC.) REGULATIONS 2017

Cooperation between supervisory bodies

Supervisory bodies charged with supervision and regulation of relevant financial business are obliged to provide cooperation to their international counterparts where cross border business takes place (r.9) and also with their equivalent authorities (r.9A). This includes conducting inquiries on behalf of a requesting supervisory authority or law enforcement authority and exchanging information obtained through such inquiries with the requesting supervisory authority or law enforcement authority.

REVISED CONFIDENTIALITY PROVISIONS ARE ALSO INTRODUCED.AMENDMENTS TO THE TERRORISM ACT 2018.

Amendments introduced to the Terrorism Act reflect primarily the new activities caught by 5MLD and the definitions have been updated accordingly to capture:

- Provision of tax advice,
- Letting agency work;
- Trading in artistic works (including operating a freeport which stores artistic works);
- Distributed Ledger Technologies.

This newsletter has been published by;

The National Coordinator for Anti-Money Laundering and the Combatting of Terrorist Financing
HM Government of Gibraltar
40 Town Range
Gibraltar

March 2020