AML TENDER

JUST/2018/JACC/PR/CRIM/018

ANNEX 7

USERS' MANUAL

22 February 2021

PUBLISHERS

European Lawyers Foundation
Fluwelen Burgwal 58
2511 CJ – The Hague
The Netherlands
+31 612 990 818
www.elf-fae.eu
info@elf-fae.eu

Council of Bars and Law Societies of Europe
Rue Joseph II, 40
1000 – Brussels
Belgium
+32 2234 6510
www.ccbe.eu
info@ccbe.eu

TABLE OF CONTENTS

USERS' MANUAL

FOREWORD

This training manual (the users' manual) has been prepared for lawyers participating in training on anti-money laundering (AML) and counter terrorist financing (CTF) rules at EU level. There is a corresponding manual available (the trainer's manual) for those who are providing the training.

Both manuals are products of a contract awarded by the European Commission to the European Lawyers Foundation (ELF) and the Council of Bars and Law Societies of Europe (CCBE) on the 'Development of organisation of training for lawyers on Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) Rules at EU level' (Service contract JUST/2018/JACC/PR/CRIM/0185).

The following describes the European Commission's objectives in putting this contract out to tender:

'The general objective of the contract is to train, raise awareness and promote the dissemination among lawyers of the key principles and concepts of the EU AML/CTF rules. The purpose of the contract is to analyse, assess and support lawyers' needs by increasing their awareness on their role and obligations in the fight against money laundering and financing of terrorism under the Directive.

The specific objective is that the training programme reach the largest possible audience of lawyers throughout the Union. In particular, the training activities may help the lawyers concerned to answer how they can best:

- *access and understand relevant AML/CTF obligations; reflect on the ways lawyers and law firms may be misused in the context of money laundering and terrorist financing;*

- *reflect on practices lawyers and law firms can adopt in their particular jurisdiction and in accordance with the relevant bar rules, to ensure the highest ethical standards of the profession are maintained;*

- *identify the problem that may arise in the interpretation of specific provisions in the light of hypothetical and actual cases and in view, in particular, of the continuity of their business relations with their clients and other considerations.'*

Prior to developing the training manuals, the consortium of partners developed a training needs assessment (TNA) and a training strategy based on answers to a questionnaire enquiring about each Member State's current practices in respect of training on AML/CTF rules at EU level for lawyers. The questionnaire was completed by all 27 EU member bars of the CCBE plus the UK.

It is worth recalling the background to the AML/CTF directives as they affect lawyers. Money laundering and terrorist financing represent serious threats to life and society and result in violence, fuel further criminal activity, and threaten the foundations of the rule of law. Given a lawyer's role in society and inherent professional and other obligations and standards, lawyers must at all times act with integrity, uphold the rule of law and not become involved in any criminal activity. This requires lawyers to be constantly aware of the threat of criminals seeking to misuse the legal profession in pursuit of money laundering and terrorist financing activities.

Lawyers and law firms must ensure that they are aware of and comply with their AML/CTF obligations, stemming from:

(i) the essential ethics of the legal profession including a fundamental obligation not to support or facilitate criminal activity, as well as national laws along the same lines; and

(ii) the requirements of EU law.

All EU lawyers must be aware of and continuously educate themselves about the relevant legal and ethical obligations that apply, and the risks that are relevant to their practice area and their clients. This is particularly so as AML/CTF activities by criminals are rapidly and constantly evolving to become more sophisticated. Awareness, vigilance, recognising red flag indicators and caution are a lawyer's best tools in assessing situations that might give rise to concerns of money laundering and terrorist financing.

The aim of this manual is to help lawyers undergoing training in the field of AML/CTF to understand the full extent of their legal and ethical obligations, along with their vulnerability to risks relating to involvement in AML/CTF activities.

INTRODUCTION

The framework of national AML/CTF law in each Member State is based on the 4th AML directive as amended by the 5th AML directive.

The training material outlined in this manual is prepared on the basis of what is applicable and obligatory for all lawyers throughout the EU, and therefore statutory references will be to the provisions of the 4th AML directive as amended by the 5th AML directive, rather than to national legislation which may be more familiar to many lawyers.

As AML/CTF legislation is enacted nationally through implementation of the directives, there may be differences in the implementation in each Member State. However, all Member States must - as a minimum - comply with the provisions of the directive. This manual has been conceived in such a way as to be easily adapted to the national contexts of the different Member States. It is proposed that, by carefully referring in this manual to the articles of the 4th AML directive (as amended) as mentioned above, it will be easy for users to identify the local context. Whenever

the 4th AML directive is mentioned, it will always be the version as amended by the 5th directive, and throughout this manual it is called 'the directive'.

In addition, the context and contents of national risk assessments should also be kept in mind, since the conditions underlying money laundering risks will vary from Member State to Member State. The FATF keeps a record of national risk assessments. Given these national differences, such risk assessments do not form part of this users' manual.

The EU provisions are the source of national implementing provisions, and if there is ever any conflict regarding the applicable provisions, the EU provision prevails. Part of the aim of this manual is to emphasise that the AML/CTF regime is an EU wide framework with common obligations for lawyers in the EU, and to provide legal certainty in this regard. However, this manual needs to be used in conjunction with domestic laws, which may, for instance, go further than the minimum standards often set in the directive.

There are three publications which have proved useful in the preparation of this manual, and whose material has been used as a source of reference:

(1) 'A lawyer's guide to detecting and preventing money laundering', published by the CCBE, the International Bar Association (IBA) and the American Bar Association (ABA) in 2014

(2) 'Guidance for a risk-based approach for legal professionals', published by the Financial Action Task Force in 2019

(3) Legal Sector Affinity Group Anti-Money Laundering Guidance for the Legal Sector, published in 2020

All three are very useful publications, although the first two guides were not published with the specific framework of current European legislation in mind. Their intended audience is lawyers worldwide, and they deal in essential principles. In addition, the first guide (CCBE-IBA-ABA) is now some years old, and some underlying circumstances may have shifted. As for the UK guide, it was published while the UK was still in the transitional period before its departure from the EU.

DEFINITIONS

The concept of AML/CTF cannot be understood without understanding how its main component parts are defined in EU legislation.

What is money laundering?

Money laundering and terrorist financing are defined in the directive through a series of activities below:

Article 1

3. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

4. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

5. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.

6. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 may be inferred from objective factual circumstances.

Article 1.3 (d) is of particular importance, in that the lawyer as advisor must avoid the pitfall of abetting or facilitating the offence. There are a number of steps which the lawyer can and should take to avoid this, as discussed later.

What is terrorist financing?

Terrorist financing is defined in Article 1.5 accordance with offences that are themselves defined in another EU decision, the Council Framework Decision 2002/475/JHA. This Framework Decision was itself amended by a subsequent decision (2008/919/JHA), and has now been replaced by Directive (EU) 2017/541 on combating terrorism.

In essence, a terrorist offence as referred to in Article 1.5 is a combination of objective elements (such as murder, bodily injuries, hostage taking, extortion, committing attacks, or a threat to commit any of the above) and subjective elements (such as acts committed with the objective of seriously intimidating a population, destabilising or destroying the structures of a country or international organisation, or making a government abstain from performing actions).

Terrorist financing is the provision or collection of funds with the intention of being used to carry out terrorist acts, whether by terrorist organisations or by individuals acting alone or in small networks.

Lawyers should be aware that terrorist financing can involve funds from legitimate or illegitimate sources – ranging from personal donations to the proceeds of criminal activity such as drug dealing, extortion or human trafficking. It may also originate from funds raised via the diversion or exploitation of natural resources.

Concealment of the destination of legitimate funds to be used for criminal purposes is, in effect, money laundering in reverse.

Are lawyers covered by the EU's AML/CTF regime, and if so, for which activities?

Article 2 of the directive specifically mentions that it is applicable to independent legal professionals. It also mentions the specific activities which are covered by the directive (Article 2.1 (3) (b)).

Article 2

1. This Directive shall apply to the following obliged entities:

…

(3) the following natural or legal persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors, and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity;

(b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies, foundations, or similar structures;

Therefore, 'independent legal professionals' carrying out the activities listed in Article 2.1 (3) (b) (i)-(v) above, which are seen as at risk of money-laundering, are covered by the duties listed in the directive, meaning that those lawyers who exclusively carry out work that is not listed in Article 2.1 (3) (b) (i)-(v), such as litigation, or maybe the work of some in-house lawyers or lawyers

working for public authorities, will not be covered by the duties in the directive. For example, an in-house lawyer may work for a bank and the bank itself is the obliged entity.

There are other professions which are not included in the definition above, but which are also covered by the obligations of the directive under Article 2, such as tax advisors 'and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity', and trust or company service providers. A lawyer providing such services would also be included within the directive's obligations.

A lawyer who is employed by a legal entity is covered specifically by Article 46 (1) of the directive, which says that the legal entity is then under the obligations of the directive:

> ***Article 46 (1)***
>
> *Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.*

Further definitions of specific AML/CTF provisions will follow in the text where appropriate.

A RISK-BASED APPROACH

General

A lawyer's duties under the 4th AML directive are subject to a risk-based approach, which is an important principle within EU AML legislation, determining the scope and extent of the activities required.

Essentially, a risk-based approach means that lawyers should identify, assess and understand the ML/TF risks to which they are exposed and – based on the risks identified and their extent - take the required AML/CFT measures effectively and efficiently to mitigate and manage the risks. More briefly, there should be a targeted approach focused on where the risk lies.

Such an approach enables:

- the allocation of resources to where the risks are higher
- the minimising of compliance costs and burdens on clients
- greater flexibility to respond to emerging risks as ML/TF methods change

The relevant core provision of the directive is Article 8:

Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

2. The risk assessments referred to in paragraph 1 shall be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

3. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

4. The policies, controls and procedures referred to in paragraph 3 shall include:

(a) the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;

(b) where appropriate with regard to the size and nature of the business, an independent audit function to test the internal policies, controls and procedures referred to in point (a).

5. Member States shall require obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

The consequences of this provision are that lawyers must:

- take appropriate steps to identify, assess and understand the ML/TF risks their own law firm faces, and

- have documented policies, controls and procedures that enable the law firm to manage, monitor and mitigate effectively the different risks that have been identified, covering at least the items listed in Article 8 (4) (a).

The risk assessment should be at the level not only of the practice as a whole, but also at the level of each client and each matter raised by a client. For the practice as a whole, elements such as the law firm's client demographic and type of services are typical risk factors, and risk reviews should be undertaken when these factors change in a material way.

Record keeping is very important throughout the AML/CTF process: of policies and procedures as above, of decisions made, of suspicions and disclosures, and of relevant documents and conversations.

Article 46 (1) of the directive lays down further duties on Member States in relation to staff employed in the law firm – they must be made aware of the firm's policies, including on data protection, and they must be trained on AML/CTF.

Article 46

1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

Those measures shall include participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

A risk-based approach can be effectively implemented by lawyers using certain procedures. All of this will be explained in further detail in the pages which follow, but can be generally summarised in the following bullet-points:

Example

Client reception procedure

- Identification and verification of the identity of each client on a timely basis (particularly if the client identity changes)
- Identification, and reasonable measures taken to verify the identity, of the beneficial owner
- Understanding of the client's circumstances and business, depending on the nature, scope and timing of services to be provided. This information can be obtained from clients during the normal course of instructions

Considering whether to take on the client

- After completing the client reception procedure, consideration of whether there is a risk for the lawyer of committing the substantive offence of money laundering though assisting the client
- A risk assessment undertaken of any red flags present and clarifications sought from the client, including on the verification of identity, to decide whether to proceed, or continue, with the engagement

Ongoing monitoring of the client

- Continual monitoring of the client's profile for signs of money laundering and terrorist financing, particularly if the client is a politically exposed person (PEP) or from a higher risk country

- Adoption of the risk-based approach of evaluating money laundering and terrorist financing risks by client, type of legal service, funds and client's choice of lawyer

How to conduct a risk assessment

When carrying out a risk assessment for a practice, lawyers are advised to take into account:

- information on money laundering and terrorist financing risks made available by the national supervisory authority in the light of its own risk assessment

- risk factors relating to:

    - clients, such as whether the practice has a stable client base (less likelihood of risk) or a high client turn-over (more likelihood of risk); in which sectors they operate (real estate or arms industries, for instance, can bring more likelihood of risk); and clients with high cash turnover businesses (more likelihood or risk)

    - the countries or regions in which the practice operates – see section on high-risk third countries below

    - products or services, such as whether the practice is involved in helping clients with real estate transactions, creation or management of trusts, companies and charities (all bring more likelihood of risk)

    - transactions – see examples in the point immediately above

    - delivery channels, such as cash payments

- the nature of any issues raised by previous suspicious transaction reports made by the practice

- consideration of:

    - the National Risk Assessment, FATF mutual evaluations, or publicly available materials in respect of the risks in the countries in which the practice operates

    - the EU's Supra-National Risk Assessment

- any other material, for example, press articles highlighting issues that may have arisen in particular jurisdictions

Once the risks have been assessed, effort should be directed towards mitigating factors or reasonable controls that can be implemented to manage the risks and reduce their significance to a proportionate and acceptable level where possible (obviously, if they cannot be reduced to such a level, the lawyer should consider not proceeding with the matter). There are a number of potential mitigating factors to consider as policies in appropriate cases, for instance:

- probing the source of funds in higher risk cases
- prohibiting the use of the practice's client account without accompanying legal services
- restricting cash payments, for instance above a certain limit both at the office or in the bank account
- keeping up-to-date with emerging issues
- conducting further investigation if a client simply requests the practice to undertake the mechanical aspects of setting up a legal entity, without seeking legal advice on the appropriateness of the entity's structure

However, a risk assessment for the whole practice is separate from a risk assessment for a particular case. Regardless of the risk assessment for the practice, each separate transaction which is covered by the scope of Article 2.1 (3) (b) (i)-(v) of the directive as listed above should also be risk-assessed, taking into account:

- the purpose of the transaction or business relationship
- the size of the transactions undertaken by the client
- the regularity and duration of the business relationship

Many of the same risks which have arisen in the practice-wide assessment may be relevant regarding a particular transaction, and so are not repeated again.

Generally, engagement by the principals and managers of law firms (regardless of size) in AML/CTF is an important aspect of the application of the risk-based approach, since such engagement reinforces a culture of compliance, ensuring that staff adhere to the policies, procedures and processes to manage the risks effectively.

Size of firm

Lawyers in small or solo practices may need a different approach to a risk based assessment on their law firms, given that they are likely to have fewer resources to dedicate than much larger firms.

Consideration should be given to the resources that can be reasonably allocated to implement and manage an appropriately developed risk assessment.

A sole practitioner would not usually be expected to devote a level of resources equivalent to those deployed by a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls, with an assessment proportionate to the scope and nature of the practice and its clients.

Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of time to conducting risk assessments.

It may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large law firm having a diverse client base with different risk profiles.

However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may also be regarded by criminals as more of a target for money launderers than large law firms. That is why legal professionals in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a risk-based assessment.

For instance, regarding the size of the firm, a significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular legal professional. This factor must be considered in the context of the legal professional's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice.

CUSTOMER DUE DILIGENCE (CDD)

Introduction

CDD involves the following activities (further amplified below), on the grounds that you are in a better position to identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you:

- you must identify the client and verify their identity, unless the identity of the client is already known to you;

- you must identify where there is a beneficial owner who is not the client and take reasonable measures to verify the identity; and

- you must assess and where appropriate obtain information on the purpose and intended nature of the business relationship or occasional transaction.

The circumstances in which CDD must be undertaken are listed in Article 11 of the directive:

Article 11

Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (12), exceeding EUR 1 000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

The full description of CDD measures is contained in Article 13:

Article 13

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council (14) or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer. Where the beneficial owner identified is the senior managing official as referred to in Article 3(6)(a) (ii), obliged entities shall take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process;

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

The last element to be mentioned in this context is that 'business relationship' is defined by Article 3 (13) of the directive as follows:

Article 3

(13) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration;

Timing

Article 11 makes clear that CDD must be undertaken either when establishing a business relationship or when carrying out certain occasional and defined transactions. Article 14 clarifies that CDD must be undertaken before either of these events, although Member States may allow verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if necessary, so as not to interrupt the normal conduct of business, and where there is little risk of money laundering or terrorist financing – but still as soon as practicable.

There is no obligation to conduct CDD for retainers involving activities outside the scope of the directive. However, many law firms do conduct CDD on all new clients, regardless of the nature of the matter. This enables clients to pass more easily from a law firm's non-regulated to regulated activities, and also makes it less burdensome on law firms to monitor continuously the transition between occasional transaction and business relationship.

There is a special timing exception for lawyers regarding CDD, contained in Article 14 (4):

Article 14

4. Member States shall require that, where an obliged entity is unable to comply with the customer due diligence requirements laid down in point (a), (b) or (c) of the first subparagraph of Article 13(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the FIU in relation to the customer in accordance with Article 33.

Member States shall not apply the first subparagraph to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

Lawyers need to be aware that the exception is strict, applying to advice and litigation work only, and not to transactional work.

There is also a duty to conduct ongoing monitoring, according to Article 14 (5) 'at appropriate times to existing customers on a risk-sensitive basis, or when the relevant circumstances of a customer change, or when the obliged entity has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s)'.

The obvious circumstance for such ongoing monitoring is if the lawyer is asked to undertake a transaction which does not fit in with the client's known resources or patterns of behaviour. Regardless, it is a good practice to operate a system of regular review and renewal of CDD. It is also a good practice to record having undertaken such monitoring, should questions arise later.

Level

Article 13 of the directive lays down the general requirements for CDD, as follows:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer.

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

If someone is acting on behalf of the client, then the lawyer must also verify that that person is authorised to do so, and identify and verify the identity of that person.

Annex I of the directive provides a non-exhaustive list of risk variables that lawyers must consider when determining to what extent to apply CDD measures:

Annex 1

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity or duration of the business relationship.

As mentioned before, AML/CTF activities are risk-based. There are two levels of CDD, depending on the level of risk involved: simplified and enhanced CDD. More detail of the general provisions above will be given under these two levels below. It is recommended that all procedures be recorded.

Simplified due diligence (SDD)

SDD is appropriate when the lawyer determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account the specific case-based risk assessment. With simplified due diligence, the lawyer must obviously identify the client, and, particularly with an unknown client, the following questions should be considered:

- name, address and telephone number
- client's past and present employment background
- place and date of birth
- past and current residential address
- business address and phone numbers
- marital status
- names and other identification data of spouse(s) and children
- name and contact details of the client's accountant
- past criminal record
- pending litigation
- tax returns

Evidence of identity can include:

- identity documents such as passports and photocard driving licences

- other forms of confirmation, including assurances from persons within the regulated sector or those in your practice who have dealt with the person for some time

In most cases of face to face verification, producing a valid passport or photocard identification should enable most clients to meet the AML/CTF identification requirements. Copies of these documents should be retained, either in original hard copies, as certified hard copies, as scans, or as copies with a note that the originals have been seen, as appropriate.

It is also good practice to have either:

- one government document which verifies either name and address or name and date of birth

- a government document which verifies the client's full name and another supporting document which verifies their name and either their address or date of birth

Where it is not possible to obtain such documents, consider the reliability of other sources and the risks associated with the client and the retainer. Electronic verification may be sufficient on its own as long as the lawyer uses multiple sources of data in the verification process.

If documents are in a foreign language, lawyers must take appropriate steps to be reasonably satisfied that the documents provide evidence of the client's identity.

If the lawyer does not meet the client, the lawyer must consider whether this represents an additional risk which should be taken into account in a risk assessment of the client, and the consequent extent of the CDD measures applied.

If the client is unable to provide standard verification, consideration should be given as to whether this is consistent with the client's profile and circumstances, or whether it might be evidence of ML or TF. If there are good reasons, alternative documentation can be considered.

There are sections below on high-risk third countries, politically exposed persons and other vulnerabilities to ML/CTF. They appear in enhanced due diligence because they require further steps, but a lawyer will only know about their existence if questions are asked about the client at the beginning, allowing the lawyer to decide which level of CDD is appropriate. In other words, an understanding of both levels is required in order to be sure under which category a particular client or transaction belongs. At the end of the section below on enhanced due diligence there is also a description of various risk factors, usually called ‘red flags’, to help distinguish between the two.

Annex II of the directive provides a non-exhaustive list of factors and types of evidence of potentially lower risk, which could lead to SDD, and are to be taken into account. They are divided into three categories – customer type, transaction type, and geography - as follows:

Annex II

(1) 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 point (3);

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance 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);

(3) Geographical risk factors — registration, establishment, residence in:

(a) Member States;

(b) third countries having effective AML/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 FATF Recommendations and effectively implement those requirements.

Once the business relationship is established, it should be continually monitored for trigger events which may create a requirement for further due diligence in future.

Regardless of the level of CDD employed, lawyers should develop internal policy and procedures so that CDD measures, including SDD, are consistently applied and that there is clear evidence of the approach taken. A lack of satisfactory procedures put lawyers at higher risk of committing money laundering offences, with sanctions possible.

Enhanced due diligence (EDD)

EDD is required when the risks are higher. Article 18 of the directive provides examples of higher risk transactions, where EDD is particularly required. The degree and nature of monitoring of the business relationship, in order to determine whether the transactions or activities appear suspicious, should be increased. The transactions are as follows:

- complex transactions
- unusually large transactions
- transactions conducted in an unusual pattern
- transactions without an apparent economic or lawful purpose

Annex lll of the directive goes on to provide a non-exhaustive list of factors and types of evidence of potentially higher risk, which could lead to EDD, and are to be taken into account. They are again divided into three categories – customer type, transaction type, and geography - as follows:

Annex III

(1) 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 point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(g) customer is a third country national who applies for residence rights or citizenship in the Member State in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities in that Member State.

(2) 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, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

(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;

(f) transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

(3) Geographical risk factors:

(a) without prejudice to Article 9, 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, for example, the Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

The division into three categories – customer, service and geography - is a helpful guide throughout the due diligence process.

A further helpful principle is that the extent to which a lawyer must obtain, review and obtain evidence of a client's financial position, or any other risk factor, is dependent upon the risk profile of the client or matter. In EDD situations, this requirement is more stringent. Certain checks are good practice in all cases – for instance, checking the source of funds and source of wealth is a useful practical tool for protecting a lawyer's practice generally.

Reliance on third parties

Article 25 of the directive allows Member States to permit lawyers (and other obliged entities) to rely on third parties to meet CDD requirements. Given the discretion afforded to them, different Member States may have different rules, which should be checked. However, the directive explicitly provides that 'the ultimate responsibility for meeting those [CDD] requirements shall remain with the obliged entity which relies on the third party'. Because of this, lawyers should always ask what CDD enquiries the other person has undertaken to ensure that they comply with the directive and the risk-based approach.

Article 26 restricts the third parties on which lawyers (and others obliged under the directive) may rely:

Article 26

1. For the purposes of this Section, 'third parties' means obliged entities listed in Article 2, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that:

(a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Directive; and

(b) have their compliance with the requirements of this Directive supervised in a manner consistent with Section 2 of Chapter VI.

In other words, the third parties must themselves either be subject to the obligations of the directive, or be subject to a regime which is consistent with the CDD, record-keeping and supervision requirements of the directive.

Member States are forbidden from allowing lawyers (and other obliged entities) from relying on third parties established in high-risk third countries (see more on them below). Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the EU where they fully comply with the group-wide policies and procedures in accordance with the directive's requirements on group-wide policies and practices (Article 45).

Overall, lawyers should ensure that the CDD information provided is not out of date, and be aware that the risk assessment of the person being relied on may not match the lawyer's own. It may not always be appropriate to rely on another person, and lawyers should consider reliance as a risk in itself. In general, lawyers should satisfy themselves that the third party:

- has a good reputation
- is regulated, supervised and monitored
- has measures in place for compliance with CDD and record-keeping requirements
- has necessary information concerning country specific risks in its country of operation

Written policies, controls and procedures

It is important that lawyers have written policies, controls and procedures as part of the risk assessment of their practices, and particularly in relation to CDD.

These are the areas which it is important or useful to record in writing:

- the lawyer's or law firm's understanding of the key AML/CTF risks faced
- the sources used in completing their AML/CTF risk assessment
- the level of personnel within the law firm permitted to exercise discretion on the policies and procedures, and the circumstances under which that discretion may be exercised

- the CDD requirements to be met for simplified, standard and enhanced due diligence (where standard falls between simplified and enhanced due diligence; it generally covers cases where there is a potential risk but it is unlikely that such a risk will be realised)
- when outsourcing of CDD obligations or reliance will be permitted, and on what conditions
- how you will restrict work being conducted on a file where CDD has not been completed
- the circumstances in which delayed CDD is permitted
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- decisions taken outside the usual policy, for instance if a decision is taken to adopt extra controls in relation to a client or matter

There are special rules for law firms (and other obliged entities) which are part of a group, as contained in Article 45

Article 45

1. Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

2. Member States shall require that obliged entities that operate establishments in another Member State ensure that those establishments respect the national provisions of that other Member State transposing this Directive.

3. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum AML/CFT requirements are less strict than those of the Member State, their branches and majority-owned subsidiaries located in the third country implement the requirements of the Member State, including data protection, to the extent that the third country's law so allows.

…

5. Member States shall require that, where a third country's law does not permit the implementation of the policies and procedures required under paragraph 1, obliged entities ensure that branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the competent authorities of their home Member State. If the additional measures are not sufficient,

the competent authorities of the home Member State shall exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country.

In other words, where part of a group, the branches must share information within the group for AML/CTF purposes. The branches must also comply with the national AML/CTF provisions of the Member State in which they are based.

If the branch is in a third country with lower AML/CTF standards, the branch must follow the AML/CTF rules of the Member State of the law firm, to the extent allowed by the local law of the third country. If the third country does not permit the law firm's policies and procedures to be implemented, the branches must apply additional AML/CTF measures and the law firm must inform its own competent authorities accordingly. Where these additional measures are not sufficient, the Member State must exercise additional supervisory actions, with the power to request the law firm to close down the branch if necessary.

As always, lawyers should regularly review and update their group-wide policies, controls and procedures and maintain a written record of any changes made. Lawyers should also keep a written record of the steps taken to communicate the group wide policies, and any changes to them, to their staff.

Record keeping

Quite separately from written procedures, Article 40 of the directive makes the keeping of records obligatory. These records need to be kept for 5 years after the end of a business relationship with the client or after the date of an occasional transaction. The requirement covers both CDD and the identification of transactions. 5 years is the minimum time specified in the directive, but lawyers should check their national laws as to whether a longer time is necessary locally.

Regarding CDD, lawyers must keep a copy of the documents and information which are necessary to comply with CDD requirements, including, where available, not only hard copies but also information obtained through electronic identification means, relevant trust services or any other secure, remote or electronic, identification process accepted by relevant national authorities.

Regarding the transaction, lawyers must keep the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions. The records should be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved), so they can serve as evidence in a possible prosecution.

The data kept under either heading must be deleted at the end of the 5 years, unless national law determines otherwise. In any case, the data can never be retained beyond 10 years.

Companies

A company is a legal entity in its own right, but conducts its business through representatives. Lawyers must identify and verify the existence of the company.

A company's identity comprises its constitution, its business and its legal ownership structure.

Lawyers should verify:

- its name
- its company number or other registration number
- the address of its registered office and, if different, principal place of business

If it is listed, lawyers should additionally verify:

- the law to which it is subject and its constitution
- the full names of the board of directors (or equivalent management body) and senior persons responsible for its operations

A listed company is likely to be a lower risk. If that is the assessment, it would be sufficient to obtain confirmation of the company's listing on the regulated market, such as:

- a copy of the dated page of the website of the relevant stock exchange showing the listing
- a photocopy of the listing in a reputable daily newspaper
- information from a reputable electronic verification service provider or online registry

For a subsidiary of a listed company, lawyers will need evidence of the parent/subsidiary relationship, such as:

- the subsidiary's last filed annual return
- a note in the parent's or subsidiary's last audited accounts
- information from a reputable electronic verification service provider or online registry
- information from the parent company’s published reports, including from their website

When already acting for the parent company, lawyers may refer to the CDD file for the existing client for verification of details for the subsidiary, provided that the existing client has been identified to the standards of the directive.

If the company is not listed on a regulated market, further verification may be required, as follows:

- a search of the relevant company registry
- a copy of the company's certificate of incorporation
- filed audited accounts

- information from a reputable electronic verification service provider

Where a company is a well-known household name, lawyers may consider that the level of ML/TF risks are low and apply CDD measures in a manner which is proportionate to that risk.

If the company is registered outside the EU, the same kind of documentation and verification should be sought. Clearly, the risks may be higher, and the lawyer may wish to consider having the documents certified by a person in the regulated sector or another professional whose identity can be checked by reference to a professional directory.

Trusts

Article 31 of the directive states that the provisions on trusts apply not only to trusts but also 'certain types of Treuhand or fideicomiso, where such arrangements have a structure or functions similar to trusts. Member States shall identify the characteristics to determine where legal arrangements have a structure or functions similar to trusts with regard to such legal arrangements governed under their law.' Lawyers will therefore have to check whether there are such trusts or trust-like arrangements recognised in their Member States.

Article 3 (6) – see under 'Beneficial ownership' below – defines a list of the beneficial owners in the case of trusts. Under the common law notion of a trust, it has no legal personality and cannot in itself therefore be a client. The client may be one of the parties identified under Article 3 (6) such as:

- the settlor
- the trustee(s)
- the protector(s) or
- one or more of the beneficiaries

Determining which of these groups may be the client(s) will decide to whom the lawyer owes a duty of care and who will receive the benefit of the advice.

BENEFICIAL OWNERSHIP

Article 3 (6) defines what is meant by a beneficial owner, which is vital for all that follows:

Article 3

(6) 'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council;

(ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(b) in the case of trusts, all following persons:

(i) the settlor(s);

(ii) the trustee(s);

(iii) the protector(s), if any;

(iv) the beneficiaries or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);

Articles 30 and 31 of the directive deal with the beneficial ownership of various entities which may be clients of a law firm, on the basis that it is important that lawyers understand who are the real people behind a particular transaction, whatever entity may present itself as client.

Under Article 30, Member States are now required to have beneficial ownership registers, to which lawyers (among others) will have access. Of course, these will only have details of entities

incorporated in the EU, and not outside it. Although a register is obligatory, other aspects are voluntary, for instance whether a fee will be charged for information from the register, or whether disclosure of certain information would subject the beneficial owner to serious risks.

Article 30 (8) also stresses that a risk-based approach means that a lawyer should not rely exclusively on information from the register.

In general, whether the entity is incorporated in the EU or outside it, the kind of information that a lawyer will need from an entity client is the following:

- name of the entity, where it is registered, its registered number, its registered office and principal place of business
- names of board of directors or members of equivalent management body
- the senior persons responsible for the operations
- the law to which the entity is subject
- the legal owners
- the beneficial owners, including through shares, voting rights, ownership interest, bearer shareholdings, or control via other means
- the governing documents

Obviously, if any of the above data changes during the business relationship, it should be impressed on the client that the changes need to be notified to the lawyer, since they might impact on the risk assessment.

Article 31 deals with trusts and other types of legal arrangements, such as fiducie, certain types of Treuhand or fideicomiso, where such arrangements have a structure or functions similar to trusts.

The second paragraph of Article 31 (1) includes this obligation regarding trusts within the EU:

Article 31 (1)

Each Member State shall require that trustees of any express trust administered in that Member State obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. That information shall include the identity of:

(a) the settlor(s);

(b) the trustee(s);

(c) the protector(s) (if any);

(d) the beneficiaries or class of beneficiaries;

(e) any other natural person exercising effective control of the trust.

This information is also to be included in the beneficial ownership register of the Member State in which the trustee (or equivalent to trustee) resides or is established. But if the trustee (or equivalent) is based outside the EU, then the information must be contained in the beneficial ownership register of the Member State where the trustee (or equivalent) enters into a business relationship or acquires real estate in the name of the trust.

All the same conditions apply regarding access to the information as already mentioned above in relation to the beneficial ownership register, including that a risk-based approach means that a lawyer should not rely exclusively on information from the register.

The amount of information that should be obtained by the lawyer from the client will depend on which role the lawyer is playing. If the lawyer is establishing or administering the trust, company or other legal entity, or is acting as a trustee or director of the trust, company or other legal entity, the lawyer will be required to understand the general purpose behind the structure and the source of funds in the structure, in addition to being able to identify the beneficial owners and controlling persons.

A lawyer who is providing other services (e.g. acting as registered office) to a trust, company or other legal entity will be required to obtain sufficient information to be able to identify the beneficial owners and controlling persons.

A lawyer who is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by another legal professional or accountant or trust or company service provider or relevant extracts from the trust deed itself to enable the lawyer to identify the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control.

Obviously, care needs to be exercised during the CDD process of a beneficial owner. The client may, for instance, be an agent, through a power of attorney or in the capacity of a bankruptcy administrator. Lawyers should be alert to the possibility that purported agency relationships are being utilised to facilitate a fraud.

A proportionate approach is recommended. For instance, in the case of a complex company, it would be disproportionate to conduct independent searches across multiple entities at multiple layers of a corporate chain to see whether, by accumulating very small interests in different entities, a person finally achieves more than a 25 per cent interest in the client corporate entity. Instead, lawyers must be satisfied that they have an overall understanding of the ownership and control structure of the client company.

Both Articles 30 and 31 have provisions that require discrepancy reporting, meaning that obliged entities must report any discrepancies that they find between the beneficial ownership information available in the central registers and the beneficial ownership information available to them as obliged entities. This applies to information on company and other beneficial ownership registers.

There is no duty actively to seek out such discrepancies, and the duty also does not apply where the information is subject to lawyer-client confidentiality or where the discrepancy is not material (such as only an initial for a middle name rather than the full name). The discrepancy can be

reported to the client first, to allow the client quickly to amend the discrepancy. If a decision is made not to report a discrepancy, for instance because it is not material, it is advised nevertheless to record what action has been taken.

HIGH-RISK THIRD COUNTRIES

Article 18a of the directive has detailed instructions about how to deal with clients from high-risk third countries. The Commission is mandated to identify those countries which have strategic deficiencies in their regime on AML and CTF, with the aim of protecting the integrity of the EU financial system. The most recent list was compiled on 7 May 2020. Annex 1 lists the countries in that list.

Country risk factors are obviously a prominent factor in the overall risk assessment. Conversely, where clients or beneficial owners of clients are based or operate businesses in low risk jurisdictions, this should also be reflected in a risk assessment.

Lawyers should note that there may be other jurisdictions that present a high risk of money laundering that are not on the European Commission list of 'high risk third countries'. For instance, rankings of corruption provided by Transparency International (a global NGO that fights corruption), and reports collated annually by The World Bank may be further useful resources.

And further, although this section deals with countries on the high risk list, there may also be countries, individuals or groups which are subject to ‘sanctions, embargos or similar measures’ as mentioned in (3) of Annex III, for which EDD will also be necessary. The EU and the United Nations keep such lists, as may individual Member States.

The additional factors enumerated in Article 18a for EDD on high-risk third countries focus mainly on additional information required from the client, and additional monitoring of the relationship.

POLITICALLY EXPOSED PERSONS (PEPS)

The definition of a PEP is given in Article 3 (9) of the directive:

Article 3

(9) ‘politically exposed person’ means a natural person who is or who has been entrusted with prominent public functions and includes the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials

There is a focus on PEPs because OECD member states are concerned that PEPs have used their political position to corruptly enrich themselves. There will be a PEP relationship also where a PEP is a beneficial owner of a client and where a client or its beneficial owner is a family member or known close associate of a PEP. Family members and close associates are also defined in the directive, as follows:

Article 3

(10) 'family members' includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

(c) the parents of a politically exposed person;

(11) 'persons known to be close associates' means:

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

Article 20 of the directive lays out the special EDD measures that a lawyer should take regarding a PEP:

(1) have in place appropriate risk management systems, including risk-based procedures, to determine whether the client or the beneficial owner of the client is a PEP

Lawyers do not have to conduct extensive investigations to establish whether a person is a PEP. It is enough to have regard to information that is in the lawyer's possession or publicly known. Many law firms use subscriber services that can run checks against PEP databases. What action to take depends on the overall risk assessment of the lawyer's practice.

Since the global existence of PEPs is wide and constantly changing, there are some basic indicators which may provide evidence, as follows:

- the lawyer receiving funds from a government account
- correspondence on official letterhead from the client or a related person
- news reports and internet searches

Lawyers also do not need actively to investigate whether beneficial owners of a client are PEPs. However, where a beneficial owner is known to be a PEP, lawyers should consider on a risk-based approach what extra measures, if any, need to be taken when dealing with the client.

(2) obtain senior management approval for establishing or continuing business relationships with PEPs

'Senior management' is defined in Article 3 (12) 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'. It need not, in all cases, be a member of the equivalent in a law firm of the board of directors, and so could be:

- the head of a practice group
- another partner not involved with the particular file
- the partner supervising the particular file
- the person responsible for compliance with AML/CTF in the firm
- the managing partner.

(3) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with PEPs

'Source of funds' is different to 'source of wealth'. 'Source of funds' relates to the place from which the client's funds are sent, and how and from where the client obtained the money in order to be able to send it. 'Source of wealth' relates to how the client's entire body of wealth or overall assets arose – for example, through inheritance, property sale, or investment profit. The 'source of wealth' assessment is fundamental to an AML/CTF assessment.

If the person is a known PEP, their financial interests may already be available on a public register.

Otherwise, questions asked of a client should be sufficient, with all steps recorded as usual. The type of documentation accepted to verify source of either funds or wealth should depend on the level of ML/TF risk presented by the client. The higher the risk, the more comprehensive and reliable should the documents be that a lawyer obtains. The kinds of documents which should be considered include: bank statements, wills, full payslips, audited financial accounts showing funds disbursed to the client, sales/purchase agreements, receipts of other transactions, proof of income from share capital, business activities, a bequest or gift.

Checking source of wealth in a low or medium risk client may mean no more than asking and recording the answers. As the risk rises, so should the level of questions and documentation sought.

Although this advice is included here under a heading related to PEPs, lawyers should also consider following it as a part of ongoing monitoring of any business relationship, whether high risk or otherwise. As mentioned earlier, checking the source of funds is a useful practical tool for protecting a law firm's practice generally.

(4) conduct enhanced, ongoing monitoring of those business relationships.

The kind of enhanced monitoring would be, for example, ensuring that funds paid by the client come from the nominated account and are for an amount commensurate with the client's known wealth. If not, further questions need to be asked.

NON FACE-TO-FACE CLIENTS

If a client is a natural person and is not physically present for identification purposes, this is a factor to be taken into account when assessing the risk level of ML or TF, and the consequent extent of any EDD measures.

Obviously, a client which is not a natural person can never be physically present for identification and will be represented by an agent. Although the absence of face-to-face meetings with agents of such a client is a risk factor, this does not automatically imply EDD must be undertaken. The overall risk must be assessed.

RED FLAGS

In addition to the above recognised categories, there are various circumstances which should put a lawyer on alert, usually called red flags.

Again, these are divided into the three risk categories already mentioned: client, transaction, geography. The following examples are selected from 'A lawyer's guide to detecting and preventing money laundering', published by the CCBE, the International Bar Association (IBA)

and the American Bar Association (ABA) in 2014, which is worth reading in full for its lists of red flags. Geographical examples can be found in the previous section under high-risk third countries.

Client

- use of intermediaries without good reason
- avoidance of personal contact for no good reason
- reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction
- use of false or counterfeited documentation
- the client is a business entity that cannot be found on the Internet
- the client is unusually familiar with the ordinary standards provided for by the law in satisfactory customer identification, data entries and STRs, or asks repeated questions on related procedures
- the parties are connected without apparent business reason or of an unusual age for executing
  parties or not the same as the persons actually directing the operation

Transaction

- no good explanation for the use of cash
- the source of funds is unusual e.g. multiple bank accounts, foreign bank accounts, transfer through higher risk country
- no good explanation for an unusually short repayment period or mortgages being repeatedly repaid significantly prior to the initially agreed maturity date
- no good explanation for a an excessively high or low price attached to assets being transferred
- no good explanation for a large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, or the activity of the client
- the source of funds is unusual because of third party funding either for the transaction or for fees/taxes with no apparent connection

Geography

- countries/areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them

- countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling

- countries subject to sanctions, embargoes or similar measures issued by international organisations such as the EU or the United Nations

- countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and in relation to which financial institutions should give special attention to business relationships and transactions

USE OF TECHNOLOGY

Lawyers may use technological solutions for their CDD obligations as follows:

- electronic means to verify an individual's identity

- corporate registry and beneficial ownership checkers

- electronic tools to screen clients against sanctions, PEP and adverse media watchlists

Such use does not absolve lawyers from personal responsibility, which will remain throughout with the lawyer. As a result, lawyers' staff using the tools should be appropriately trained, and lawyers themselves should develop an in-depth understanding of how the tools work.

The use of electronic means to verify identity can save a firm's resources, and may be as, or indeed more, secure than traditional paper documents. However, lawyers should be alert to various risks:

- cyber and data security

- fraud

- the possibility of human error through an input mistake

- the level of the risk presented by the client or the transaction

- the need to tie the presenting client to the electronic identity found

- the recent nature, trustworthiness and multiplicity of sources used by the electronic provider

- the reliability, independence and transparency of the provider, and whether it is certified by a public authority or part of a public scheme, is a member of a recognised industry body and complies with recognised international standards in the field

In dealing with corporate registries and beneficial owner checkers, the risk level should determine whether independent evidence should be sought, given that such registries are usually compiled using data from the entities themselves. The registered information may also not give a full picture, and care should be taken for how often the data is required to be refreshed.

Regarding client screening against sanctions, PEP and adverse media, the level of risk will again be the determining factor. For lower risk cases or practices, free or off-the-shelf solutions may be acceptable. For higher risk cases, consideration should be given to how broad the screening should be (for instance, beneficial owners, directors of companies), its frequency and the reliability of systems used in terms of input, age of information and completeness of data. A proper screening tool should be able to screen and identify names and other datasets with minor alterations such as reverse order, partial text and abbreviations, or those in non-Latin scripts, such as Chinese characters or commercial code data.

REPORTING OBLIGATIONS

Introduction

The reporting of suspicious transactions lies at the heart of the AML/CTF regime established by the directive. The principal obligation comes from Article 33:

Article 33

1. Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly:

(a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and

(b) providing the FIU directly, at its request, with all necessary information.

All suspicious transactions, including attempted transactions, shall be reported.

There are special provisions regarding lawyers, who fall within point 3 (b) of Article 2(1), as follows:

Article 34

1. By way of derogation from Article 33(1), Member States may, in the case of obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 33(1).

Without prejudice to paragraph 2, the designated self-regulatory body shall, in cases referred to in the first subparagraph of this paragraph, forward the information to the FIU promptly and unfiltered.

2. Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

In summary, these two provisions require a lawyer to inform the national Financial Intelligence Unit (FIU) when the lawyer 'knows, suspects or has reasonable grounds to suspect' that the funds which form part of the transaction are the proceeds of criminal activity or are related to TF. Member States may allow Bars to take over the reporting duty, and this has happened in certain Member States. There is also an exemption on reporting for lawyers in very strictly limited circumstances – when they are ascertaining the legal position of their client or defending or representing the client in judicial proceedings.

The lawyer is not supposed to continue to act for the client after making a suspicious transaction report (STR) to the FIU, other than in very limited circumstances:

Article 35

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with point (a) of the first subparagraph of Article 33(1) and have complied with any further specific instructions from the FIU or the competent authorities in accordance with the law of the relevant Member State.

2. Where refraining from carrying out transactions referred to in paragraph 1 is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation, the obliged entities concerned shall inform the FIU immediately afterwards.

Finally, the lawyer should obviously become acquainted with the national procedures for sending STRs to the FIU.

A discussion about the relationship between these reporting obligations, including the ban on tipping off which is discussed separately below, and lawyer-client confidentiality is discussed in the section on lawyer-client confidentiality below.

Tipping off

There is one aspect of the reporting obligations which is very significant for lawyers, and that is the anti-tipping off provision in Article 39:

> ***Article 39***
>
> *1. Obliged entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with Article 33 or 34 or that a money laundering or terrorist financing analysis is being, or may be, carried out.*

In other words, a lawyer is forbidden from telling the client about a suspicious transaction report (STR) that the lawyer has passed to the FIU. There are sanctions for those who breach these requirements (see below). However, there is one exception to this general rule under Article 39 (6):

> ***Article 39***
>
> *6. Where the obliged entities referred to in point (3)(a) and (b) of Article 2(1) seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1 of this Article.*

In other words, if a lawyer is trying to dissuade the client from undertaking a money laundering activity, that does not amount to tipping off the client (even if the client may guess the lawyer suspects that the transaction may be tainted by money laundering). The lawyer still appears to be under a duty to make the STR, but can at the time continue with efforts to dissuade the client.

Article 39 (6) does not impose a legal obligation on a lawyer to seek to dissuade a client from engaging in illegal activities. Bearing this in mind, the relationship between lawyers' activities in Article 39 (6) on the one hand (dissuade the client), and Article 33 (duty to make an STR) and Article 35 (refrain from continuing to act) on the other may be best understood in the following sequence. Article 33 contains the obligation to make an STR; in such cases, lawyers must refrain from continuing to act until the decision of the FIU (Article 35). Any potential effort to seek to dissuade the client from engaging in illegal activities shall not be considered as an offence against Article 39 (6). Nevertheless, lawyers may not tip off their clients about the STR.

Once lawyers have submitted an STR, they should seriously consider stopping to act for the client immediately after making the STR, even if the directive does not provide for such an obligation. A lawyer might be accused later on of having known about illegal activities, even if the FIU does not give a negative response. In other words: the submission of an STR may be used against the lawyer in further legal proceedings.

If a lawyer succeeds in dissuading the client from engaging in an illegal activity, then there is no longer an obligation to file an STR.

'Knows, suspects or has reasonable grounds for suspicion' – and the meaning of words in general

These are the key words from Article 33 (1) (a) for the lawyer to consider. Given that there are offences in relation to failure to report – see below under 'Sanctions' – the meaning of these words is important.

'Knows' may be thought to be rather straight forward. Ordinarily, knowledge means actual knowledge. A question arises as to whether lawyers wilfully shutting their eyes to the truth may amount to knowledge. Jurisdictions could have their own interpretations on this point, but the *prima facie* standard should be that nothing less than actual knowledge will suffice.

The test for 'suspects' is a subjective one. A lawyer who thinks a transaction is suspicious should not be expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. There should be no requirement for the suspicion to be clear or firmly grounded on specific facts, but there should be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation. The lawyer may have noticed something unusual or unexpected, and after making enquiries, the facts do not seem normal or make commercial sense. There does not need to be evidence that money laundering is taking place in order to have suspicion.

The red flags previously highlighted provide guidance on a number of standard warning signs, which may give cause for concern. If the lawyer has not yet formed a suspicion, but simply has cause for concern, for instance arising out of one of the red flags, the lawyer may ask the client - or others - more questions. It could depend on what the lawyer already knows, and how easy it is to make enquiries.

The test for 'has reasonable grounds for suspicion' contains the same mental element as for suspicion, except that here there is an objective test. Were there factual circumstances from which an honest and reasonable lawyer should have inferred knowledge or formed the suspicion that the client was engaged in money laundering?

This raises another important issue. The guidance on the meaning of these words can only go so far at a European level, because domestic laws may define these words in a particular way, and maybe slightly differently in each Member State.

That applies also to other words found in the reporting obligations – for instance, 'ascertaining the legal position' or 'judicial proceedings' in the phrase found in Article 34 on exemption from reporting of 'ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings'.

In all these cases, it is important for lawyers to know the exact wording used both in the version of the directive in their national language, and also in the national implementing legislation and how it is ordinarily interpreted. The national legislation cannot depart from the EU-wide standard set in the directive, and if it does the directive prevails, but the extent of the words might nevertheless be somewhat different between Member States.

'Criminal activity'

According to Article 33 (1) (a), the lawyer is obliged to make an STR 'where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing'.

The words 'criminal activity' are defined in Article 3 (4) of the directive:

> ***Article 3***
>
> *(4) 'criminal activity' means any kind of criminal involvement in the commission of the following serious crimes:*
>
> *(a) terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out in Titles II and III of Directive (EU) 2017/541;*
>
> *(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;*
>
> *(c) the activities of criminal organisations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA;*
>
> *(d) fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests;*
>
> *(e) corruption;*
>
> *(f) all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;*

The most important section of Article 3, since it will be the test for most transactions on which lawyers will advise, is (f) above, the 'all offences' catch-all. However, it does not catch all. Although it covers tax crimes, the only offences to which it applies are those which are capable of attracting the sentences mentioned under (f), namely punishable by a sentence of more than a year. Where a Member State has a minimum threshold for offences, the definition changes to being a sentence for a minimum of more than 6 months.

Suspicions regarding offences which fall outside that definition are not reportable. Clearly, lawyers will have to acquaint themselves with the list of offences in their national legislation.

DATA PROTECTION

The General Data Protection Regulation (GDPR - Regulation (EU) 2016/679) applies to data under the directive. A full explanation of the GDPR is beyond the remit of this guide. However,

lawyers will need to bear in mind its provision in relation to all the data that they process relating to a client.

Article 41 of the directive deals with data protection issues:

Article 41

2. Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited.

3. Obliged entities shall provide new clients with the information required pursuant to [the GDPR] before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of obliged entities under this Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of this Directive.

4. In applying the prohibition of disclosure laid down in Article 39(1), Member States shall adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to:

(a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or

(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

A number of consequences flow from these provisions, and from the general application of the GDPR.

First, a lawyer may not use the data obtained under CDD, or any other provision of the directive, for any other purposes, such as marketing or for profit.

Second, the legal basis for the lawyer's handling of the data is not the client's consent, and does not depend on the client's consent. Article 6 of the GDPR provides 6 lawful bases for processing data, one of which is client's consent. The others can be gleaned from the text of Article 6 itself, below:

Article 6, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks

But there are two other bases, both of which apply to the lawyer's data processing. One is where 'processing is necessary for compliance with a legal obligation to which the controller is subject'. Since the directive requires certain data to be obtained and retained by the lawyer – see Article 40 of the previous section – the legal basis for the lawyer in AML/CTF can fall under the 'legal obligation' mentioned in Article 6 (1) (c).

But it could also fall under Article 6 (1) (e) where 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. That is because Article 43 specifically declares that 'The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under [the GDPR]'.

Third, there is an exemption to a client's right of access to data under the GDPR in relation to the tipping off provisions. Tipping off has a clear relationship with data protection, since if the client has a right to see that a tipping off report has been made, it defeats the purpose of the prohibition on tipping off.

Article 23 of the GDPR already foresees such a possible restriction, and the preamble to the GDPR specifically mentions such a restriction, saying 'This is relevant for instance in the framework of anti-money laundering'.

In consequence, the directive clearly says that Member States must take action in this respect in relation to tipping off data (hence the reference to Article 39), by passing legislation restricting the client from the right of access to such data. Lawyers will need to be aware of the content and scope of the particular legislation in this regard in their Member State.

LAWYER-CLIENT CONFIDENTIALITY

Introduction

The provisions outlined above in Articles 33, 34, 35 and 39 not only go to the heart of the AML/CTF regime, but they also touch on one of the core principles of the lawyer-client relationship, namely lawyer-client confidentiality (using this general term to cover the general notions of professional secrecy and legal professional privilege), and the relationship of full confidence which should exist between a lawyer and client.

The essential EU text on the meaning and consequence of lawyer client confidentiality comes from the AM&S case (*AM & S Europe Limited v Commission of the European Communities*, Case 155/79):

> *'Community law, which derives from not only the economic but also the legal interpenetration of the Member States, must take into account the principles and concepts common to the laws of those States concerning the observance of confidentiality, in particular, as regards certain communications between lawyer and client. That confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it.'*

The case was revisited by the court over twenty years later in *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v Commission of the European Communities,* Joined Cases T-125/03 &T-253/03. Its essential principle, as outlined above, was confirmed in the later case, where the court also noted that the principle is 'closely linked to the concept of the lawyer's role as collaborating in the administration of justice by the courts'.

This is, in fact, an internationally recognised principle. The International Bar Association has published International Principles on Conduct for the Legal Profession, and Principle 4 states:

> '*A lawyer shall at all times maintain and be afforded protection of confidentiality regarding the affairs of present or former clients, unless otherwise allowed or required by law and/or applicable rules of professional conduct.*'

Lawyer-client confidentiality goes by different names and is governed by different rules in different jurisdictions.

For instance, in some jurisdictions, lawyer-client confidentiality laws and rules expressly impose obligations on the lawyer. In others, protection of confidential information from disclosure is achieved by the creation of "privileges" (also called exemptions) from the ordinary rules requiring information to be disclosed.

However, the underlying principle is the same everywhere: a lawyer is prevented (by law in many countries) from disclosing information given to them by their client in confidence to any third party, including governmental and judicial authorities.

There is also a general rule that the protection provided by lawyer-client confidentiality does not apply when a lawyer is knowingly assisting, aiding or abetting unlawful conduct of their clients – in this case, to launder money or to assist with terrorist funding. The lawyer would almost certainly be committing a criminal offence. The lawyer would also normally be disciplined by the professional regulatory authority concerned.

European case law

The reporting obligations under the directive do not conflict with this principle as understood in European law. This has been decided in a couple of cases, one before the Court of Justice of the European Union and one before the European Court of Human Rights.

In the case of *Ordre des barreaux francophones et germanophone and Others v Conseil des ministres,* Case C-305/05 before the Court of Justice of the European Union, one of the orders of the Belgian Bar brought a case questioning the conflict. But the court decided that the reporting obligations do not infringe the right to a fair trial as guaranteed by Article 6 of the European Convention on Human Rights and Article 6(2) of the Treaty on European Union.

The reason given was that the reporting obligations apply to lawyers only in so far as they advise their client in the preparation or execution of certain transactions – essentially those of a financial or transactional nature. As a rule, the nature of such activities is such that they take place in a context with no link to judicial proceedings and, consequently, those activities fall outside the scope of the right to a fair trial, which was the basis of the claim.

The court added that as soon as the lawyer is called upon for assistance in defending the client or in representing the client before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings, that lawyer is exempt from the reporting obligations, regardless of whether the information has been received or obtained before, during or after the proceedings. The court stated that an exemption of that kind safeguards the right of the client to a fair trial.

There was a similar case brought before the European Court of Human Rights: *Michaud v France* (Application no. 12323/11). This related to Article 8 of the European Convention on Human Rights, and the court concluded that, although Article 8 of the Convention protects 'the fundamental right to professional confidentiality', requiring lawyers to report suspicions did not amount to excessive interference with that right.

It based its decision on the general interest served by combating money-laundering, and on the guarantee provided by the exclusion from the scope of the obligation of reporting provided by Article 34 (2) (in the course of activities connected with judicial proceedings, or in lawyers' capacity as legal counsel). In addition, French law has put in place a filter to protect professional confidentiality, by ensuring that lawyers do not submit their reports directly to the FIU, but to the president of the Bar.

Aside from European level cases, there may be national cases which bear on the implementation of the directive locally, such as the Belgian Constitutional Court case on reporting suspicious transactions (Decision n° 114/2020 of 24 September 2020)

Conclusion

The interplay between the directive, lawyer-client confidentiality and the European-level case law means that an STR must be made in accordance with the specific circumstances outlined in the directive and the case law to ensure that there is no breach of the European Convention on Human Rights or the Treaty on European Union. If the lawyer does not report when required, then such non-reporting lays the lawyer open to prosecution for an AML criminal offence (see below).

However, the directive's requirements operate only within certain parameters:

- to those within the definition of which lawyers and transactions are covered by the directive in Article 2 (1) (3)

- even if included within that definition, there are exemptions from reporting contained in Article 34 (2)

- there are other important definitions regarding reporting, such as that for 'criminal activity', which is the trigger for the STR in the first place (dependent on how individual Member States have defined the crime of money laundering)

Outside those strict boundaries, the directive's requirements on reporting do not apply, and the usual rules of lawyer-client confidentiality do apply. Lawyers also need to be aware of whether their jurisdiction has taken advantage of the derogation contained in Article 34 (1), which allows the lawyer to report suspicions to the Bar, and for the Bar to be responsible for onward transmission to the FIU.

Lawyer-client confidentiality may only be assumed not to have been violated where an STR has been made in strict accordance with the requirements of Article 33 of the directive. Therefore lawyers should not submit an STR for self-protective and precautionary reasons alone - if they do so, they run the risk of violating confidentiality obligations.

CROSS-BORDER ISSUES

Several issues may arise on a cross-border basis as a result of a lawyer working for clients in other jurisdictions or with a presence in other jurisdictions.

Within the EU

Given that the directive is EU-wide, its minimum standards are to be implemented everywhere. However, some Member States have gone beyond the minimum, and in any case different jurisdictions have adopted different methods – for instance, in some cases the lawyer has to make an STR direct to the FIU, and in others to the Bar. That means that there is no alternative but for the lawyer to be familiar with the other Member State's AML regime, probably most securely achieved by advice from a lawyer within that Member State.

Specific problems arise in a number of areas:

- reliance on third parties in another Member State for CDD – the requirements of Article 26 of the directive have already been mentioned

- lawyer-client confidentiality provisions – not only may the STR be made in different ways as just mentioned, but the scope and application of lawyer-client confidentiality may be different, and so needs to be carefully checked

- documents may be in a foreign language, or relate to institutions with which the lawyer may not be familiar, which obliges the lawyer to take appropriate steps to be reasonably satisfied that the documents in fact provide evidence of what is alleged, for instance the client's identity

SANCTIONS

Introduction

Article 59 of the directive says that Member States must ensure that there are administrative sanctions at least for breaches that are serious, repeated, systematic, or a combination thereof, of the requirements laid down for the following headings:

- customer due diligence (Articles 10 to 24)

- suspicious transaction reporting (Articles 33 to 35)

- record-keeping (Article 40)

- internal controls (Articles 45 to 46)

Article 59 goes on to say that, in these cases, the minimum sanctions must be the following:

Article 59 (2)

… the administrative sanctions and measures that can be applied include at least the following:

(a) a public statement which identifies the natural or legal person and the nature of the breach;

(b) an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct;

(c) where an obliged entity is subject to an authorisation, withdrawal or suspension of the authorisation;

(d) a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities;

(e) maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000.

In terms of factors to be taken into account when deciding the level of the sanctions, Article 60 (4) says:

Article 60

4. Member States shall ensure that when determining the type and level of administrative sanctions or measures, the competent authorities shall take into account all relevant circumstances, including where applicable:

(a) the gravity and the duration of the breach;

(b) the degree of responsibility of the natural or legal person held responsible;

(c) the financial strength of the natural or legal person held responsible, as indicated for example by the total turnover of the legal person held responsible or the annual income of the natural person held responsible;

(d) the benefit derived from the breach by the natural or legal person held responsible, insofar as it can be determined;

(e) the losses to third parties caused by the breach, insofar as they can be determined;

(f) the level of cooperation of the natural or legal person held responsible with the competent authority;

(g) previous breaches by the natural or legal person held responsible.

Article 61 contains protections for whistleblowers who notify the authorities of breaches of the AML/CTF provisions.

Clearly, lawyers will need to be conversant with their own domestic laws, administrative or criminal, regarding breaches of the AML/CTF provisions, since they may go further than the above minimum standards.

Requirements for an offence

Although the wording of the offences is left to Member States to fit into their national legal systems, it can be assumed that for the main offences, for instance regarding a failure to make an STR, the prosecution will have to prove that the property involved is criminal property – in other words, property or funds gained through criminal activity as defined in Article 3 (4). This means that the prosecution will have to prove that the property was obtained through criminal conduct and that, at the time of the alleged offence, the lawyer knew or suspected that it was.

For the failure to disclose offences, lawyers will have to disclose if they had knowledge, suspicion or reasonable grounds for suspicion. These terms have already been further defined earlier in this manual under ‘Reporting obligations’.

ANNEX 1 – LIST OF HIGH RISK COUNTRIES

This list may change – see here

No	High-risk third country
1	Afghanistan
2	The Bahamas
3	Barbados
4	Botswana
5	Cambodia
6	Democratic People's Republic of Korea (DPRK)
7	Ghana
8	Iran
9	Iraq
10	Jamaica
11	Mauritius
12	Mongolia
13	Myanmar/Burma
14	Nicaragua
15	Pakistan
16	Panama
17	Syria
18	Trinidad and Tobago
19	Uganda
20	Vanuatu
21	Yemen
22	Zimbabwe