

Directives

Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 in Strasbourg, France on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

“Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development” (1).

“In order to increase vigilance and mitigate the risks posed by [large cash payments that are vulnerable to money laundering and terrorist financing], persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 10,000 or more” (6).

“Legal professionals...should be subject to this Directive when participating in financial or corporate transactions, including when providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing” (9).

Tax crimes are included as “criminal activity” in this Directive (11).

“New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering” (19).

“The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk-based approach should be used.... It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively” (22).

“The results of risk assessments should, where appropriate, be made available to obliged entities in a timely manner to enable them to identify, understand, manage and mitigate their own risks” (25).

“In addition, to identify, understand, manage and mitigate risks at Union level to an even greater degree, Member States should make available the results of their risk assessments to each other, to the Commission and to EBA, EIOPA and ESMA” (26).

“All Member States have, or should, set up operationally independent and autonomous FIUs to collect and analyze the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing” (37).

“Persons that merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution and persons that provide credit institutions or financial institutions solely with messaging or other support systems for transmitting funds or with clearing and settlement systems do not fall within the scope of this Directive” (47).

“Money laundering and terrorist financing are international problems and the effort to combat them should be global” (48).

“The EU Financial Intelligence Units' Platform (the ‘EU FIUs Platform’), an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between

FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level” (55).

“This Directive respects the fundamental rights and observes the principles recognized by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defense” (65).

Chapter 1: General Provisions

Section 1: Subject Matter, Scope, and Definitions

Article 1

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).

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.

Article 2

The Directive applies to credit institutions, financial institutions, and natural and legal persons acting as auditors, external accountants, and tax advisors.

Article 3

Credit institution

Financial institution- an undertaking other than a credit institution, an insurance undertaking, an investment firm, a collective investment undertaking marketing its units or shares, an insurance intermediary, branches of financial institutions

Property- assets of any kind and legal documents or instruments in any form

Criminal activity- any kind of criminal involvement in the commission

Self-regulatory body- a body that represents members of a profession and has a role in regulating them, in performing certain supervisory and monitoring type functions and in ensuring the enforcement of the rules relating to them

Beneficial owner- any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted (cases differ for corporate entities, trusts, and foundations)

Trust or company service provider- any person that provides to third parties the formation of companies or other legal persons; arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to any other legal person or arrangement; arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with Union law or subject to equivalent international standards

Correspondent relationship- provision of banking services by one bank as the correspondent to another bank as the respondent and/or the relationships between and among credit institutions and financial institutions

Politically exposed person- natural person who is or who has been entrusted with prominent public functions such as heads of state, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties; 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; members of courts of auditors or of the boards of central banks; ambassadors and high-ranking officers in the armed forces; members of the administrative, management or supervisory bodies of State-owned enterprises; directors, deputy directors, and members of the board or equivalent in an international organization

Family members- spouse, children and their spouses, parents

Person known to be close associates- natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements or any other close business relations; natural persons who have sole beneficial ownership of a legal entity or legal arrangement

Senior management- 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

Business relationship- 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

Gambling services- service which involved wagering a stake with monetary value in games of chance, including those with an element of skill

Group- group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation

Electronic money

Shell bank- credit institution or financial institution

Article 4

Member States shall, in accordance with the risk-based approach, ensure that the scope of this Directive is extended in whole or in part to professions and to categories of undertakings.

Article 5

Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, within the limits of Union law.

Section 2: Risk Assessment

Article 6

The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

This assessment should cover the areas of the internal market that are at greatest risk, the risks associated with each relevant sector, and the most widespread means used by criminals by which to launder illicit proceeds.

Article 7

Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date.

It shall use the risk assessment to improve its AML/CFT regime, identify sectors or areas of lower or greater risk of money laundering and terrorist financing, to assist it in the allocation and prioritization of resources to combat money laundering and terrorist financing, to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing, and to make appropriate information available promptly to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments.

Article 8

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. These policies shall include 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.

Section 3: Third Country Policy

Article 9

Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper functioning of the internal market.

Strategic deficiencies of high-risk third countries include the legal and institutional AML/CFT framework of the third country (criminalization of money laundering and terrorist financing, measures relating to customer due diligence, requirements relating to record keeping, and requirements to report suspicious transactions), the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing, and the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.

Chapter II: Customer Due Diligence

Section 1: General Provisions

Article 10

Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks.

Article 11

Member States shall ensure that obliged entities apply customer due diligence measures when establishing a business relationship, when carrying out an occasional transaction that amounts to 15,000 euro or more or constitutes a transfer of funds, when carrying out occasional transactions in cash amounting to 10,000 euro or more when people are trading goods, when carrying out transactions amounting to 2,000 euro or more in gambling services, when there is a suspicion of money laundering or terrorist financing, and when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 12

A Member State may allow obliged entities not to apply certain customer due diligence measures with respect to electronic money.

Article 13

Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

Article 14

Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

Section 2: Simplified customer due diligence

Article 15

Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.

Article 16

When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, Member States and obliged entities shall take into account at least the factors of potentially lower risk situations.

Article 17

Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

Section 3: Enhanced customer due diligence

Article 18

Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

Article 19

Cross-border correspondent relationships with a third-country respondent institution credit institutions and financial institutions of Member States should gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; access the respondent institution's AML/CFT controls; obtain approval from senior management before establishing new correspondent relationships; document the respective responsibilities of each institution.

Article 20

With respect to transactions or business relationships with politically exposed persons, Member States shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner of the customer is a politically exposed person and apply the following measures in cases of business relationships with politically exposed persons: obtain senior management approval for establishing or continuing business relationships with such persons, take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons, and conduct enhanced, ongoing monitoring of those business relationships.

Article 21

Member States shall require obliged entities to take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy.

Article 22

Where a politically exposed person is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organization, obliged entities shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

Article 24

Member States shall prohibit credit institutions and financial institutions from entering into, or continuing, a correspondent relationship with a shell bank.

Section 4: Performance by third parties

Article 26

Third parties means obliged entities listed in Article 2, the member organizations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Directive and have their compliance with the requirements of the Directive.

Chapter III: Beneficial Ownership Information

Article 30

Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their *beneficial* ownership, including the details of the beneficial interests held.

The persons or organizations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

Chapter IV: Reporting Obligations

Section 1: General Provisions

Article 32

Each Member State shall establish an FIU in order to prevent, detect, and effectively combat money laundering and terrorist financing.

Each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyze, request and disseminate specific information.

Article 35

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.

Article 38

Member States shall ensure that individuals, including employees and representatives of the obliged entity, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

Section 2: Prohibition of disclosure

Article 39

Obligated 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 or that a money laundering or terrorist financing analysis is being, or may be, carried out.

Chapter V: Data Protection, Record-Retention, and Statistical Data

Chapter VI: Policies, Procedures, and Supervision

Section 1: Internal procedures, training, and feedback

Article 46

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.

Section 2: Supervision

Section 3: Cooperation

Article 51

The Commission may lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Union.

Article 57

Differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.

Section 4: Sanctions

Article 62

Member States shall ensure that competent authorities establish effective and reliable mechanisms to encourage the reporting to competent authorities of potential or actual breaches of the national provisions transposing this Directive.