European Commission

Explanatory Meeting on

Chapter 4 :
FREE MOVEMENT OF CAPITAL
-
ANTI MONEY LAUNDERING

DG Justice and Consumers
European Commission

These slides accompany the explanation of the acquis to Albania and North Macedonia and can only be used for that purpose. Their content is subject to further development of the acquis and interpretation by the Court of Justice of the European Union.

European Commission

EU Legislation

- **European framework built around the international FATF standards**
- **Objective: integrity and stability of financial system**
- **Approach:**
  - ensure traceability of financial transactions
  - Identification of clients (Customer due diligence measures - CDD)
- **Historical evolution:**
  - 1st AMLD (1990): laundering of proceeds of drug trafficking by banks
  - 2nd AMLD (2001): laundering of proceeds of all crimes by banks and designated professions (e.g. lawyers, notaries, high value dealers)
  - 3rd AMLD (2005): terrorist financing and risk based approach
  - 4th AMLD (2015): comprehensive regime adapted to new ML/TF risks
  - 5th AMLD (2018): improving for increased transparency of beneficial ownership information and new tools for fighting terrorist financing

The EU acquis

- **Directive** (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing **(4th AML Directive)**
- **Directive** (EU) 2018/843 **(5th AML Directive)** amending **Directive** (EU) 2015/849
- **Delegated Regulation** (EU) 2016/1675 (HRTC)
- **Delegated Regulation** (EU) 2018/1108 (RTS CCP)
- **Regulation** (EU) 2015/847 on information accompanying transfers of funds

⇨ **Transposition of the 4AMLD by 25 June 2017, amendments of 5AMLD by 20 January 2020**

⇨ **Directive of minimum harmonisation**

Directive (EU) 2015/849 and Directive (EU)2018/843 (4th and 5th AMLD)

Elements of the AML DIRECTIVES

- risk-based approach
- coverage of tax crimes
- coverage of gambling sector → *beyond FATF requirements*
- cash payments of 10.000 € or more → *beyond FATF requirements*
- customer due diligence (CDD)
- Politically Exposed Persons (PEPs) → *beyond FATF requirements*
- information on beneficial owner → *beyond FATF requirements*
- reinforcement of sanctioning powers → *beyond FATF requirements*
- Cooperation between Financial Intelligence Units
- Bank account registers → *beyond FATF requirements*
- European Supervisory Authorities (ESA)
- EU list on high risk third countries

➡ **Minimum harmonisation**

Scope of AMLD (1) – Obliged entities:

- Credit and financial institutions as defined under EU law
- lawyers, notaries, accountants, auditors, tax advisors, tax related services provided other than tax advisors
- trust and company service providers
- casinos and gambling providers,
- dealers in goods when payments are made in cash in excess of 10.000 €
- real estate agents, letting agents (monthly rent exceeding 10.000 €)
- Traders of work and art (auction houses/art galleries) and storing carried out by freeports (transactions exceeding 10.000 €)
- Virtual currency exchange platforms and wallet services providers in virtual currencies

Scope of AMLD (2)

- **Money laundering**
  - proceeds of all serious crimes that are hidden/converted, <u>including tax crime</u>
  - Broad definition of proceeds of "criminal activity"
  - Activities which generated the proceeds outside the territory of the EU are covered as well

- **Terrorist Financing**
  - Illegitimate but also legitimate sources of funds used for TF

Main obligations imposed by AMLD

- **Identification and verification of identity** of customer and the "Beneficial Owner" of legal entities
- **Ongoing monitoring** of transactions by obliged entities
- **Obligation to report suspicious transactions** to a Financial Intelligence Unit (FIU) prior to execution of a transaction
- Prohibition to inform clients about reporting of suspicious transactions (**non-tipping off**)
- **Record keeping, internal procedures, training, staff protection**
- **Supervision**, **cooperation between EU FIUs**, and **sanctions**

- Minimum harmonisation: MS can adopt stricter rules within the limits of EU law

Customer due diligence measures

- **Prohibition of anonymous accounts/relationship with a shell bank**
- **Identify and verify the identity of customers**
  - For natural persons
  - For legal entities or arrangements: the "beneficial owner"
- **If not, prohibition to enter into a business relationship**
- **Monitoring of transactions**
- **Anonymous transactions (e.g. prepaid cards)**
  - Identification of user for all transactions >150€ at the point of sell or >50€ when prepaid instrument used on-line
- **Keep copy of supporting documents for 5 years after the end of the business relationship (possible to extend by another 5 years)**

Who is the Beneficial Owner?

Identification of Beneficial Owner (BO) – i.e. the natural persons who ultimately controls/owns the entity must be found

- Beneficial owner for **companies**:
  - 25% ownership threshold
  - direct or indirect control
  - If no suspicion and no other person can be identified: senior manager

- Beneficial owner for **trusts**:
  - Settlor, trustee, protector, beneficiaries of the trust or any other natural person exercising ultimate control

BO Identification

1. **All corporate and other legal entities/trusts and legal arrangements within the MS required to hold adequate, accurate and current information on their BO**
2. **BO information has to be submitted to obliged entities, Trustees or persons holding equivalent positions shall disclose their status and provide BO information to OEs in a timely manner**
3. **BO register for legal entities (Art. 30) / legal arrangements (Art. 31)**

- **BO information for legal entities has to be held in a "central register" (e.g. business, commercial, public register)**
  - OEs shall not exclusively rely on the information stored in the register
  - Discrepancies between BO information in central register and the BO available to OEs shall be reported
- **Similarly BO Information of express trusts/similar arrangements shall be kept in a central BO register**
  - Also includes information on trustees residing outside the EU

Risk-based approach

- Clearly understand ML/TF risks and adapt system to nature of risks. Evidence-based measures at four levels:
  - **European Union** → identify, understand and mitigate risks
  - **Member States** → identify, understand and mitigate risks
  - **Supervisors** → concentrate resources on areas where risks of ML/TF are greater
  - **Obliged entities** (risk-based factors) → identify, understand and mitigate risks

- Make CDD-rules more risk sensitive – based on indicative and non-exhaustive risk factors:
  - **enhanced measures** where risks are bigger
  - **simplified measures** where risks are demonstrated to be lower

Enhance Customer Due Diligence (EDD)

- Obliged entities shall be required to apply **EDD** in certain cases:

  - Transactions with clients in third country identified as "high risk"
  - Cross-border correspondent relationship with third countries
  - Transactions involving Politically Exposed Persons (and family members)
  - Complex and unusually large transactions which have no economic or lawful purpose

Politically Exposed Persons (PEPs)

- A "politically exposed person" refers to a natural person who is or has been entrusted with prominent public functions
- Definition covers foreign and domestic politically exposed persons (illustrative list of functions, Art. 3(9))
- Also includes "family members" and "close associates"
- obliged entities have to carry out enhanced CDD:
  - senior management approval
  - establish source of wealth and funds
  - conduct enhanced monitoring

EU policy towards High-Risk Third Countries (HRTC)

- COM to identify third countries having strategic deficiencies in their AML/CFT regimes (Art. 9)
- Methodology with assessment criteria
- Obliged entities need to apply enhanced CDD with clients established in those countries (Art. 18)
  - Strong checks/controls of financial transactions
  - Mandatory and optional list of checks
- Delegated Act to identify those countries based on criteria set in 4AMLD

Methodology on high risk third countries

- Methodology issued on 22 June 2018 (SWD(2018)362)
- Implements Art. 9 of 4AMLD by applying following approach:
  1. FATF lists as a baseline
  2. EU autonomous assessment to complement it:
     - **Scoping out of +200 jurisdictions**
     - **Planning and prioritisation**
     - **Assessment: based on AMLD criteria**

       Analysing 8 key areas: criminalisation of ML/TF, CDD in financial sector, CDD in non-financial sector, Beneficial ownership, sanctions, powers of authorities, international cooperation, targeted financial sanctions.
     - **Listing**
     - **Follow-up**

➡ **First results by end 2018/early 2019**

Delegated Regulation 2016/1675

- Obliged entities must apply EDD when having a business relationship involving HRTC listed in Regulation 2016/1675

- Delegated Regulation 2016/1675 based on FATF lists, i.e.
  - Compliance document
  - Public statement

- Delegated Regulation to be replaced by a new Act early 2019:
  - FATF as a baseline
  - Additional countries based on EU autonomous assessment

AML/CFT supervision

1. **Cooperation and requirements**:

- AML/CFT Supervision of obliged entities through strong cooperation of national competent authorities
  - Confidentiality
  - Information sharing
- Cooperation with prudential supervisors (incl. MoU with ECB)

2. **Supervisory tasks and powers**:

- Registration/licensing obligation for all OEs
- Fit and proper tests for management function positions
- Powers for onsite and offsite inspections
- Powers to apply sanctions in case of breach

Sanctions

- Public statement identifying the natural/legal person and the nature of the breach (information shall remain on competent authorities website for 5 years after its publication)
- Order requiring the natural/legal person to cease and to desist from repetition of that conduct
- Withdrawal or suspension of authorisation
- Temporary ban against any person discharging managerial responsibilities in an OE/any natural person, held responsible for the breach, from exercising managerial functions in OEs
- Max. administrative pecuniary sanction of at least twice the amount of benefit derived from the breach or at least 1 million EUR
- Credit and financial institutions:
  - Legal persons: 5 million EUR or 10% of the total annual turnover
  - Natural persons: 5 million EUR or equivalent in national currency

European Commission

Financial Intelligence Units (FIUs)

- **Function of the FIU (receiving, analysing, disseminating)**

- **Powers of FIUs**
  - Obliged entities have to report STRs prior to execution of transaction
  - Power of suspending transactions
  - Direct access to any information held by obliged entities (even if this OE did not report an STR)
  - Access to bank & payment account register (to be set up)
  - Access to BO register for companies / trusts
  - Access to information reg. persons owning real estate (incl. land registers where existing)

- **Cooperation between EU FIUs**
  - Information sharing regardless of predicate offence/if predicate offence is not identified
  - Exchange of information through secure channel: FIU.Net

fiu.net

Bank and Payment Account Registers

- **Centralised bank account registers or data retrieval systems at MS level**
  - Bank accounts
  - Payment accounts
  - Safe deposit boxes

- **Direct access to Financial Intelligence Units + access to competent AML/CFT authorities**

European Commission

Beneficial Ownership Registers

- Registration of BO for legal persons & all legal arrangements
- Covers also legal arrangements of third countries entering into a business relationship / acquiring real estate
- Access to Competent authorities + wider access to registers:
  - **Legal entities: fully public access**
  - **Trust: legitimate interest**
- Interconnection of national BO registers by 2021
- Verification mechanisms to be put in place
  - Verification mechanism to ensure BO data is accurate
  - Include reporting of discrepancies

BO

BO Register – Transparency of BO information (1)

LEGAL ENTITIES

- **Scope**: legal entities incorporated in MS territories (incorporated = "in accordance with national law" recital 14)
- **"Details of beneficial interests held"** = whether the BO has direct/indirect control, 25% of shares, voting rights, senior manager – approach confirmed by new (ii) of Article 30 (1) (a)
- **National central register** (e.g. commercial/company registers)
- **Verification mechanisms** – including at least **check of discrepancies**

⚠ Directive not prescriptive: verification mechanisms to improve the quality of the BO information.

As a minimum: through the checks of discrepancy between information collected in the context of the CDD and the information held in the register – and NCA reporting

Many options for the verification of the BO information: reliance on the authority in charge of the registers; reliance on obliged entities in the context of the discrepancies checks; reliance on the public.

BO Register – Transparency of BO information (2)

LEGAL ENTITIES

- **Public access**: without restriction for FIUs and competent authorities; in the framework of CDD for obliged entities; any member of the general public

⚠ Scope of information accessible:

- restrictive list of information applicable to the general public only
- FIUs, competent authorities and obliged entities should have access to complete set of information

Online registration and payment of a fee possible for all entities asking for access to BO register (incl. FIUs and CAs); access free of charge when cross-border request from other MS' FIU

- **Exemptions clause:** limited list of circumstances under which access can be refused, detailed evaluation expected from MS, annual statistical data shall be reported to COM
- **Data retention:** BO information should remain available for 5-10 years after the entity has been struck off from the register
- **Consultation of BO register by OEs:** mandatory not exclusively

BO Register – Transparency of BO information (3)

LEGAL ARRANGEMENTS

- **Scope**: trusts/other types of legal arrangements having a structure or functions similar to trusts (fiducies, certain Treuhand or fideicomiso)
  - MS to determine the other structures similar to trusts and notify COM, COM to issue report on similar structures
- **Availability of information in national central register:**
  - In MS where the trustee is established or resides
  - If residence outside the EU: MS where the trustee enters into a business relationship or acquires real estate
  - If multiple business relationships in different MS: proof of registration in one MS
- **Access to register:**
  - FIUs and competent authorities without restriction
  - Obliged entities in the framework of CDD
  - any person that can demonstrate a legitimate interest
  - any person that files a written request when the trust owns a non-EU company

⚠ Trusts owning a EU company will be registered under the BO register for companies (Art. 30)

BO Register – Transparency of BO information (4)

LEGAL ARRANGEMENTS

- **Exemption clause:** limited list of circumstances under which access can be refused, detailed evaluation expected from MS, annual statistical data shall be reported to COM
- **Data retention:** BO information should remain available for 5-10 years after grounds for registration have ceased to exist (i.e. the trustee has ceased to conduct business relationships)
- **Consultation of the BO register by obliged entities:** mandatory not exclusively
- **Verification mechanisms** to check discrepancies

Directive not prescriptive: same arguments as in provisions for companies

Whistleblower and Staff protection

- **Protection against hostile effect or discriminatory employment actions for STR reporting**
  - Possibility to present complaints in a safe manner to competent authorities
  - Right to effective remedy

- **Provision of effective and reliable mechanisms that encourage reporting to competent authorities of AML/CFT breaches**
  - Secure communication channels
  - Confidentiality
  - Protection of personal data
  - Independent and anonymous reporting channels within OEs

Next steps: COM follow up work

- Comprehensive report on measures taken by MS and actions to address new risks
- Report on Beneficial Ownership
  - **Mechanism for collecting BO information for companies incorporated in 3rd countries**
  - **Lowering of indicative 25% threshold for BO identification**
- Report on interconnection of land and property registers and bank account registers (2020)
- Assessment of cooperation between FIUs including "coordination and support mechanism" (EU FIU) by mid 2019

Implementing Measures

Regulatory Technical Standards

- Regulatory Technical Standards on **group-wide procedures** to manage AML/CFT-risks
  - Still in the drafting stage

- **Commission Delegated Regulation EU/2018/1108** of 7 May 2018 supplementing Directive EU 2015/849 on **Central Contact Points**
  - E-money institutions and payment services providers
  - Standards on the criteria for the determination of a central point appointment and its functions (home/host)
  - Adopted and published in OJ

Regulation 2015/847/EU on information accompanying transfers of funds (FTR)

Objective

- Define rules on the information on payers and payees, accompanying transfers of funds
- Implement FATF Rec 16 on wire transfers
- Regulation directly applicable in Member States (harmonised)

Obligations for the payment service provider of the payer

- Acquisition of "complete information" on the payer
  - Name, address, payment account number, official personal document number, customer identification number or date and place of birth or unique transaction number
- Acquisition of "complete information" on the payee
  - Name and payment account number or unique transaction identifier
- Verification of the accuracy on the information provided before the transaction can be conducted
  - Based on documents, data and information from a reliable and independent source
- In case of a transfer from an account:
  - Verification is deemed to have taken place if the payer's identity has been verified in relation to the opening of the account, according to Directive 2015/849.
- Keep records for five years of complete information on the payer

Transfers of funds within the EU

- Where both the PSP of the payer and the PSP of the payee are situated in the Union
  - Transfers shall be accompanied by at least the payment account number of both the payer and the payee or the unique transaction identifier where applicable

This provision is specific to the EU

<u>However:</u>

- The PSP of the payer, if requested by the PSP of the payee, has to make available
  - complete information on the payer or payee (within three working days) in case transaction > 1000 EUR
  - the name, payment account number of the payer/payee or the unique transaction identifier (within three working days) in case transaction < 1000 EUR
- If transfer < 1000 EUR, the PSP of the payer does not need to verify the information on the payer, unless
  - Funds have been transferred in cash or anonymous electronic money
  - PSP has reasonable grounds to suspect ML or TF

Transfers of funds from the Union to outside the Union

- The transfers must be accompanied by complete information on the payer
- **Batch file transfers** from a single payer to payees having their PSPs outside the EU
  - The obligation does not apply to the individual transfers bundled together, provided that:

    The individual transfers carry the **verified name, address, payment account number, official personal document number, customer identification number or date and place of birth of the payer and the name and payment account number of the payee or a unique transaction identifier**
- Transfers **of less than 1000 EUR** must only be accompanied by name and account number of payer/payee or a unique transaction identifier
  - PSP of the payer does not need to verify the information on the payer, unless
    - Funds have been transferred in cash or anonymous electronic money
    - PSP has reasonable grounds to suspect ML or TF

Obligations on the Payment Service Provider of the payee

- Duty to detect whether the transfer is accompanied by complete information on the payer and the payee
- Effective procedures (incl. ex-post/real-time monitoring) must be in place to detect whether the following information on the payer is missing:
  - For transfers from <u>within the Union</u>:
    - the payment account number of the payer/payee or a unique identifier
  - For transfers from <u>outside the Union</u>:
    - complete information on the payer as well as name and payment account number of the payee
    - for batch file transfers, complete information on the payer and the name and payment account number of the payee in relation to that transfer
- If transfers > 1000 EUR: PSP of the payee has to verify information on payee through a reliable, independent source
- If transfers < 1000 EUR: the PSP of the payee does not need to verify the accuracy of the information on the payee, unless
  - Pay-out in cash or anonymous electronic money
  - ML/TF suspicion

Transfers with missing or incomplete information on the payer

- If the PSP of the payee becomes aware that information on the payer is missing or incomplete, it has to:
  - Reject the incoming transfer, or
  - Ask the PSP of the payer for complete information
- If the PSP of the payer repeatedly fails to supply the required information, the PSP of the payee shall take appropriate steps, including initially (i.a.)
  - Issuing of warnings
  - Setting of deadlines
- Subsequently, the PSP of the payee has to decide whether to:
  - Reject future transfers from that PSP
  - Restrict the business relationship
  - Terminate the business relationship

Other obligations applicable to the transfer of funds

In any event, the PSP of the payee has to:

- **Apply anti-terrorist freezing measures** (Regulations 2001/2580/EC, 200/881/EC and 2010/356/EU)

- **Apply the AML/CFT measures set out in Directive 2015/849/EU** including:
  - Assessing possible suspicions and reporting them to the Financial Intelligence Unit (FIU) (missing or incomplete information is a factor for this assessment)

- **Keep records for five years** of any information received on the payer

Obligations on intermediary payment service providers

The intermediary payment service provider must:

- **Ensure that all information received on the payer is kept with the transfer**
- Implement **effective procedures** to detect whether the **information on the payer and the payee in the messaging or payment and settlement system is complete**
- Establish **effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information**
- If it becomes aware that **information on the payer/payee is missing or incomplete**, it shall **reject the transfer** or **ask for the required payer/payee information before or after the transmission of the transfer**
- If a PSP **repeatedly fails to provide the required payer/payee information,** the intermediary PSP shall **take steps initially including the issuing of warnings and setting of deadlines before either rejecting any future transfers or restricting/terminating the business relationship with the PSP**

Sanctions

- Sanctions shall be consistent with those laid down in AML Directives
  - Application to both legal persons and natural persons
  - **Legal persons** can be held liable for breaches by any person acting individually or as part of an organ of that legal person
  - Sanctions shall also apply to **natural persons** (i.e. members of the management body and any other person who is responsible for a breach)
- Competent authorities shall have the necessary powers to impose sanctions and measures
- Sanctions shall be published without undue delay, including type and nature of the breach as well as the identity of the persons responsible for them

Agreements with countries/territories outside the territory of the EU (Art. 24)

- **France**: COM Implementing Decision 2018/1803 has been adopted on 20 November 2018 (authorizing France to conclude agreements with **St.-Barthélemy, St.-Pierre-et-Miquelon, FR-Polynesia, Wallis and Fortuna**)
- **France:** COM Decision 2010/259/EU of 4 May 2010 continues to apply (authorizing France to conclude an agreement with the **Principality of Monaco**)
- **UK:** COM Decision 2008/982/EC of 8 December 2008 continues to apply (authorizing the UK to conclude agreements with **the Bailiwick of Jersey, the Bailiwick of Guernsey and the Isle of Man**)
- **Denmark:** COM Implementing Decision 2012/43/EU (authorizing Denmark to conclude an agreement with **Greenland** and the **Faroe Islands**) – internal consultation for the repeal of the decision, no conclusion taken yet