FINANSTILSYNET

The FSA's Guide to the Act on Measures to Prevent Money Laundering and Financing of Terrorism (the AML Act)

November 2020

Contents

Part 1 – Scope and definitions

1. Introduction

The FSA's guide on the Act on Measures to Prevent Money Laundering and Financing of Terrorism (the AML Act) are aimed at undertakings and persons covered by the AML Act (Executive Order no. 380 of 2 April 2020 on preventive measures against money laundering and terrorist financing). The guide deals with how such undertakings and individuals can meet the requirements of the AML Act and includes rules in the area of money laundering and terrorist financing, although how there can be links to other regulatory areas is also mentioned.

Undertakings and persons must therefore be aware that there can be requirements in other legislation that must also be fulfilled.

This guide replaces the guide dated 11 October 2018 on the Act on Measures to Prevent Money Laundering and Financing of Terrorism (the AML Act).

The AML Act implements the EU's 4th and 5th Anti-Money Laundering Directives (Directives 2015/849/EU of the European Parliament and of the Council of 20 May 2015 and 2018/843/EU of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing) and is also based on recommendations from the Financial Action Task Force (FATF), of which Denmark is a member.

The FSA has gathered information on the area of money laundering and terrorist financing on its website: https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask.
The guide uses "undertakings" as a common term for undertakings and persons covered by the Act.

The AML Act is based on a consideration that undertakings covered by the Act must have a risk-based approach and establish their own rules for how they comply with anti-money laundering legislation. The examples in the guide should be seen as a way in which undertakings can find inspiration for compliance with the requirements of the Act. However, the examples are not an expression of the only way undertakings can meet the requirements of the Act, and should not be regarded as an exhaustive list for compliance with its requirements.

The guide cannot be the sole contribution to an undertaking's risk-based approach to compliance with the Anti-Money Laundering legislation. Undertakings should not only assess their own situation, but also seek inspiration in national and supranational risk assessments, along with reports from, for example, the European Banking Authority (EBA) and FATF where relevant.

The following undertakings are subject to the AML Act:

1) Banks.
2) Mortgage credit institutions.
3) Stockbroker undertakings.
4) Life insurance companies and multi-employer occupational pension funds.
5) Savings banks.

6) Providers of payment services and issuers of electronic money, cf. Annex 1, nos. 1-7, of the Payments Act.
7) Insurance brokers, when they provide life insurance or other investment-related insurance.
8) Other undertakings and persons who commercially perform one or more of the activities mentioned in Annex 1, although cf. Section 1 (4) of the Act. See Section 1.1. on other persons and undertakings covered by the AML Act.
9) Branches, distributors and agents of foreign undertakings in Denmark that carry out activities in accordance with nos. 1-7, 10 and 11.
10) Investment management companies and managers of alternative investment funds, provided such undertakings have direct customer contact.
11) Danish UCITS and alternative investment funds, provided such undertakings have direct customer contact.
12) Operators of a regulated market that has been authorised in Denmark to be an auction platform in accordance with Commission Regulation (EU) no. 1031/2010 of 12 November 2010 on the timing, administration and other aspects of auctions of allowances for greenhouse gas emissions pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community.
13) Persons authorised to bid directly in auctions subject to Commission Regulation (EU) no. 1031/2010 of 12 November 2010 on the timing, administration and other aspects of auctions of allowances for greenhouse gas emissions pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community, not already covered by nos. 1 and 3.
14) Lawyers,
    a. when providing assistance in the form of advice on, or conducting transactions for their clients in connection with
        i. the purchase and sale of real estate or undertakings,
        ii. administration of their client's funds, securities or other assets,
        iii. opening or administration of bank accounts or security deposits,
        iv. provision of necessary capital to set up, run or manage undertakings, or
        v. set up, run or manage undertakings, foundations etc., or
    b. when on a client's behalf and expense, they carry out a financial transaction or a transaction concerning real estate.
15) Auditors and audit firms approved under the Danish Act on Approved Auditors and Audit Firms (the Auditor Act).
16) Real estate agents and agencies, including when they act as middlemen in connection with the rental of real estate.
17) Undertakings and entities that otherwise commercially provide the same services as the groups mentioned in numbers 14-16, including auditors not authorised under the Auditor Act, tax advisors, external accountants and any other person that undertakes to provide assistance, tax assistance or advice as its most important business.
18) Providers of services to undertakings, cf. Section 2 (12). See Section 1.3 on registration with the Danish Business Authority (DBA).
19) Currency exchange companies; although cf. Section 1 (4) of the Act.
20) Providers of games; although cf. Section 1 (5) of the Act.
21) Danmarks Nationalbank, to the extent it carries out activities corresponding to those of the institutions mentioned in no. 1.

22) Undertakings and persons that commercially store, trade in, or act as agents for the sale of works of art, including galleries and auction houses, where the value of the transaction or of a number of interrelated transactions constitutes DKK 50,000 or above.
23) Providers of currency exchange between virtual currencies and fiat currencies.
24) Providers of virtual wallets.

Item 6) above covers undertakings that issue electronic money or provide payment services, and that are subject to the requirement for authorisation as a payment institute or e-bank or limited authorisation to provide payment services or issue e-money according to the rules in the Payment Services Act. Undertakings that only provide account information services, cf. Section 60 of the Payment Services Act are not covered. Undertakings that provide payment services, but that are not covered by a requirement for authorisation according to the Payment Services Act, e.g. those undertakings covered by Section 5, nos. 14-17 of the Payment Services Act, are not covered.

In relation to item 22), not all types of art are covered by the AML Act. Reference is made to the DBA's quick guide (https://erhvervsstyrelsen.dk/quick-guide-kunstbranchen) for further information on which types of art are covered, as well as what has to be paid special attention to when storing, trading in or brokering trade in works of art.

In relation to item 23), "virtual currency" is a digital expression of value that is not issued or guaranteed by a central bank or a public authority and is not necessarily tied to a legally created currency. A virtual currency does not have the same legal status as currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically. A "fiat currency" is defined as a legal means of payment issued by a central bank.

Item 24) above covers a unit that provides services to protect private cryptographic keys on behalf of its customers in order to keep, store and transfer virtual currencies. A private cryptographic key is defined as a means of having access to a virtual currency in a given location. If a private cryptographic key is lost, the ability to move the virtual currency to another location is lost.

1.1. Other undertakings and persons subject to the AML Act – Annex 1

Reference to the AML Act: Section 48 (1) and Annex 1. Reference to the 4th Money Laundering Directive: Article 3 (2) letter a. Reference to other legislation: The Financial Business Act, Annexes 1 and 2.

Section 1 (1), no. 8 of the AML Act is a collective provision which includes undertakings which commercially provide one or more of the financial activities listed in Annex 1 without the activity concerned being covered by Section 1 (1) nos. 1-7.

Annex 1 of the AML Act is a compilation of Annex 1 and 2 of the Financial Business Act, which lists banks and credit institution activities. However, credit information agencies and other undertakings in connection with the transfer of money and credit facilities are not covered by Annex 1 of the AML Act.

Annex 1 of the AML Act shall be interpreted in accordance with the Financial Business Act as regards the financial activities in which the annexes coincide.

If An undertaking exercises one or more activities in Annex 1 of the AML Act, it must be registered with the FSA. See Section 1.2 on money laundering registration with the FSA.

See also Section 1.1 on other undertakings and persons subject to the AML Act.

1.1.1. Acceptance of deposits and other repayable funds

This includes undertakings that service the public, and that commercially provide deposits and other repayable funds without having to have authorisation as a bank or savings company.

Deposits and other repayable funds are deposits for which the depositor is entitled to recover its claim in full.

1.1.2. Loan undertakings

Loan undertakings include consumer credit, mortgage loans, factoring, discounting and trade credits (including forfaiting). All types of lending activity are covered. The sub-paragraphs mentioned are examples that do not imply any restrictions on the types of loan covered. Loan undertakings include loans made to businesses and private individuals. Brokering of loans is not covered.

1.1.3. Financial leasing

"Financial leasing" is defined as those types of lease in which the lessee carries the financial risk of the leased equipment's estimated residual value on termination of the lease.
The leaseholder undertakes to pay a leasing charge during the term of the lease, which is an instalment payment against the "underlying loan" in the leasing company.
Leased items often have a residual value at the end of the lease agreement. The lease agreement therefore often states that the lessee is obliged to assign a buyer of the equipment to the estimated residual value on demand.

Operational leasing is another lease form that is not covered by the AML Act. Operational leasing places the risk of the residual value of the leased item on the lessee upon termination of the lease. At the expiry of the lease agreement, the lessee returns the equipment to the leasing company, whereupon the leasing company bears the risk that the leased item can attract the estimated residual value. At the end of an operational lease agreement, the leased item has a significant estimated residual value.

1.1.4. Issuing and administrating other means of payment (e.g. traveller's cheques and bank drafts), when the activity is not subject to the Payment Services Act

This covers the issuing and administration of other means of payment, when the activity is not subject to the Payment Services Act. This means that, for example, the issuing of travellers' cheques and bankers' drafts is covered. The list is an example and is therefore not exhaustive.

1.1.5. Guarantees and collateralisation

Loans given against collateral, e.g. invoice financing or lending against a mortgage on real estate, property or securities are covered. Guarantees of any kind are covered. However, it is a prerequisite that the activity is performed commercially, e.g. a surety insurance company.

1.1.6. Transactions at the customer's expense

The transactions at the customer's expense that are covered, are:

a) money market instruments (cheques, bills, certificates of deposit, etc.),
b) the currency market,
c) financial futures and options,
d) currency and interest rate instruments,
e) securities.

"Money market instruments" are defined as those instruments that are usually traded on the money market, for example treasury bills, which are short-term debt instruments issued by the state.

1.1.7. Participation in issuing securities and provision of related services

This includes, for example, contributing to a listing on a regulated market.

1.1.8. Advisory services for undertakings regarding capital structure, industrial strategy and related matters, as well as advisory and services relating to mergers and acquisitions of undertakings

This includes listing and investment of shares and equity-linked securities through regulated marketplaces, private placements of unlisted shares, major secondary share placements through regulated marketplaces, and advisory services in connection with mergers and takeovers. This type of business is also called "merchant banking".

1.1.9. Money broking

"Money broking" is defined as undertakings that broker contact between undertakings that want to borrow money, and undertakings that want to lend money. "The money market" is a collective term for the financial markets for assets involved in short-term loans/lending with a maturity of one year or less.

1.1.10. Portfolio management and advisory services

If An undertaking carries out commercial portfolio management and advisory services on the purchase and sale of securities, and is not covered by the types of undertakings specifically mentioned in Section 1 (1) of the AML Act, the company is covered by the Act for that part of its activity that relates to portfolio management and advisory services.

The "portfolio management and advisory services" activity includes portfolio and investment advisory services, when an undertaking provides personal recommendations to a customer, either on request or on the investment firm's own initiative, for one or more transactions related to financial instruments. It is thus this type of activity that is covered by the rules of the AML Act.

1.1.11. Storage and administration of securities

Management in this context differs from "portfolio management and advisory services", in that management requires a discretionary mandate to buy and sell securities from the customer without their consent for each transaction.

1.1.12. Bank box rental

Bank box rental is covered by Annex 1 of the AML Act.

The provision of bank box rental requires registration according to the AML Act, as a box can be used to store cash, precious metals and other high value physical objects. See Section 1.2 on money laundering registration with the FSA.

If the company only offers storage of e.g. furniture, luggage, vehicles and the like, it is not included in Annex 1 of the AML Act. Similarly, short-term, occasional storage, such as a hotel provides to its customers, is not covered.

1.2. Money laundering registration with the FSA

Reference to the AML Act: Section 1 (1), nos. 8, 23 and 24, and Section 48 (1) and (2). Reference to the 4th Money Laundering Directive: Article 47 (1). Reference to the 5th Money Laundering Directive: Article 1 (1), no. 29.

Undertakings that commercially intend to pursue one or more activities listed in Annex 1 of the AML Act must register with the FSA.

Registration with the FSA is a prerequisite for the company to perform the activity in question. This means that undertakings that conduct business in accordance with Annex 1 or in accordance with Section 1 (1), nos. 23 and 24, without having registered, or that have been refused registration, are engaging in an illegal activity.

The registration obligation is implemented to enable the FSA to supervise undertakings performing one or more of the activities mentioned in Annex 1 on a commercial basis, or the activities covered by Section 1 (1), nos. 23 and 24. Undertakings that are already covered under other legislation under the supervision of the FSA need not be registered pursuant to Section 48 (1).

Registration is required even if the activity is not the undertaking's main activity. However, the company need not be registered if all that is involved are individual business transactions that logically relate to its main activity. For example, the term "commercially" does not include investment of surplus liquidity by an undertaking when the purpose is passive asset management, for example current investment of surplus liquidity in listed shares or bonds.

"Commercially" is defined as:

1) That the activity is offered to third parties ("customers"), or
2) that the activity is such that it represents an insignificant part of the undertaking's revenue.

Integrity assessment

An undertaking applying for registration with the FSA cannot be convicted of a criminal offence that can give rise to a potential risk of registration being abused. The FSA can revoke the registration if An undertaking is subsequently found guilty of such an offence.

The FSA must assess whether persons or members of the management and the beneficial owners of undertakings to be registered with the FSA comply with the requirements for integrity. Those undertakings

and persons covered by the provision must provide the FSA with the information necessary for the FSA to assess whether the requirements are met.

The FSA performs assessment especially with regard to ensuring that the undertakings referred to, including members of the management and beneficial owners performing one or more activities in Annex 1, have not previously been convicted of any financial crime.

The FSA has a duty to decline registration of An undertaking, if that company, its management or beneficial owners have been convicted of a criminal offence that can give rise to a potential risk of registration being abused.

The purpose of the provision is to minimise the risk of money laundering in the undertaking and the channelling of money for terrorist purposes by preventing persons with a controlling influence over the undertaking from using the undertaking for criminal purposes.

In principle, only criminal offences related to the above types of crime that are part of the FSA's assessment. Tax evasion may lead to registration being declined, given that tax evasion is included in the definition of money laundering. See Section 2.1 on definitions, money laundering.

1.3. Registration with the Danish Business Authority (DBA)

Reference to the AML Act: Section 1 (1), no. 18, Section 2 (1), no. 12, Section 57 (2) and Section 58. Reference to the 4th Money Laundering Directive: Article 47 (Article 2 (1), no. 3, letter c). Reference to other legislation: Executive Order on notification and registration of providers of services to undertakings in the DBA's register for combatting money laundering.

Undertakings providing services to other undertakings, cf. Section 2, no. 12, are obliged to register with the DBA in its register for combatting money laundering as a condition for being able to perform such activities.

The background to mandatory registration is that providers of services to undertakings are considered to be particularly vulnerable to the risk of being abused by their customers in the context of money laundering and terrorist financing.

It should be noted that lawyers and law practices, accountants and audit undertakings, along with real estate agents and real estate agencies covered by Section 1 (1), nos.14-16 of the AML Act need not register in the DBA's register for combatting money laundering, even if they provide the same services as covered by the obligation to register.

It should also be noted that bookkeepers, tax advisors etc., covered by Section 1 (1), no. 17 of the AML Act must be registered, unless they provide at least one of the services referred to in Section 2, no. 12.

To be subject to the duty to register, the company must provide at least one of the following services:

1) *Setting up companies, undertakings or other legal persons.*
    a) The provision includes setting up companies, undertakings and other legal persons. Assistance for setting up voluntary associations etc. will therefore also be covered.

    b) The registration obligation applies to all forms of commercial assistance for the preparation of documents, contact with authorities and registration of companies or the like. What is decisive is therefore not whether the person concerned carries out the actual notification or registration with the DBA, but whether that person does the actual work involved with setting-up.

    c) This provision only covers commercial services provided to third parties.

2) *Virtual office sharespaces*
    a) This provision covers anyone providing a domicile address, or other address which is similarly intended as a contact address, and related services for An undertaking.

    b) "*Related services*" are defined as services that relate to the running of the company. For example: reception, telephone service, mail forwarding, business administration, bookkeeping or similar.

    c) The provision includes only "virtual customers" that are not physically located at the address.

    d) If An undertaking has both virtual and physical customers, it is only the virtual customers that are covered by the scope of the AML Act.

    e) It is believed that the risk of money laundering and terrorist financing is high in the case of virtual customers, as the customer can hide or obscure its identity.

3) *Professional board members*
    a) The provision covers anyone acting as or that arranges for another person to act as a member of management in An undertaking, or who partakes in a partnership or a similar position in other undertakings.

    b) Professional board members include, for example, anyone working as a board member or director of An undertaking. The decisive factor is that the board member acts on behalf of third parties, and that it is not employment or appointment in the traditional sense.

    c) Included in the provision are persons who, in a start-up phase, act as directors of a foreign company to be established in Denmark, for example.

4) *Managers or administrators of a trust, foundation or similar legal arrangement*
    a) The provision covers anyone acting as, or that arranges for another person to act as, the custodian or administrator of a foundation, trust or a similar legal arrangement.

    b) The definition includes trustees, i.e. the persons appointed by the founder of a trust to manage the funds in the trust.

5) *Nominees*

a) The provision covers persons acting as, or that arrange for another person to act as, the nominee for third parties, unless this concerns An undertaking whose ownership shares etc. are traded in a regulated market or equivalent which is subject to disclosure in accordance with EU law or equivalent international standards.

b) The definition includes, for example, persons acting as representatives of the shareholder, or that arrange for others to do so, i.e. "nominees" who register shares in their own name in the shareholders' register, but when the shares are held by others.

Services offered commercially
For the service to be covered by the duty of registration, it must be offered commercially.

"Commercial" is defined as the services being offered on market-like terms, and that the company normally receives remuneration for its services.

It is not decisive whether the service in question is profitable or whether there is no payment in a specific situation. Individual provision of the services in question which cannot be classified as commercial will not be covered.

Integrity assessment
An undertaking or person applying for registration with the DBA cannot be convicted of a criminal offence that can give rise to a potential risk of their position being abused. Furthermore, the company cannot have requested/is currently undergoing reconstruction proceedings or bankruptcy proceedings.

The DBA must determine whether persons, including members of the management and beneficial owners of undertakings to be registered with the DBA, comply with the requirements for integrity and suitability. The undertakings and persons covered by the provision must provide the DBA with the information necessary for the Authority to determine whether the requirements are fulfilled, including information on subsequent changes.

The DBA's assessments are focused on ensuring that the undertakings referred to, including members of the management and the beneficial owners, providing services covered by Section 2, no. 12, have not previously been convicted of a financial crime which implies a risk of abuse of the services offered, and in such cases, the DBA is required to decline registration of the company.

Note that the requirement for honesty regarding crimes, similarly applies to management members and beneficial owners of undertakings, as well as to persons covered by Section 1 (1), no. 17, including tax advisors and bookkeepers, cf. Section 57 (2) of the AML Act.

The DBA also has a duty to decline registration of An undertaking if a member of its management has requested or is undergoing reconstruction proceedings, bankruptcy proceedings or debt relief.

The purpose of the provision is to minimise the risk of money laundering in the undertaking and the channelling of money for terrorist purposes by preventing persons with a controlling influence over the undertaking from using the undertaking for criminal purposes.

In principle, only criminal offences related to the above types of crime are part of the DBA's assessment. Tax evasion may lead to registration being declined, given that tax evasion is included in the definition of money laundering. See Section 2.1 on definitions, money laundering.

The DBA can revoke registration if the company, a member of its management or a beneficial owner is subsequently subject to conditions which would lead to refusal of registration. In addition, the DBA can revoke registration if new members of an undertaking's top or general management or new beneficial owners do not provide the Authority with the information necessary for the Authority to assess whether they are covered by section 58 (2) or (3). The DBA can also revoke registration if the company or person is guilty of a serious or repeated violation of the AML Act.

1.4. Exemptions

1.4.1. Undertakings performing activities in Annex 1 to a limited extent, and currency exchange

Reference to the AML Act: Section 1 (4).

Reference to the 4th Money Laundering Directive: Article 2 (3).

Referring Executive Order: no. 1358 of 30 November 2017 on which undertakings and persons may be exempted from the Act on Preventive Measures against Money Laundering and Financing of Terrorism (the AML Act).

In the Executive Order1 on which undertakings and persons can be exempted from the AML Act, are undertakings that perform financial activities to a limited extent, or exempted or partially exempted.

The exemption Executive Order only covers undertakings covered by Annexes 1, nos. 1 and 4-12 of the AML Act, and currency exchange companies.

The Executive Order exempts such undertakings from certain requirements in the KYC procedures, specifically Section 10, no. 1 and Sections 14 and 18.

Exemption is conditional on the risk of money laundering and terrorist financing being limited, and that the activity is performed occasionally or to a very limited extent.

The Executive Order sets out six cumulative conditions. This means that all conditions must be met in order for the company to be covered by the exemption:

1) The overall activity must be limited, and cannot exceed the following amounts on an annual basis:
   a) EUR 70,000 for undertakings that perform the activities mentioned in Annex 1, nos. 1 and 4-12 of the Act.
   b) EUR 15,000 for currency exchange companies.
2) The financial activity must be limited on a transaction basis, and cannot exceed the following amounts:

1 No. 1358 of 30 November, 2017

a) EUR 1,000 for activities mentioned in Annex 1, nos. 1 and 4-12 of the Act.
b) EUR 500 for currency exchange companies.

3) The financial activity must not be the main activity of the company or person, and cannot exceed 5 percent of the total turnover of the company or person concerned per year.
4) The financial activity must be an ancillary business directly related to the undertaking's or the person's main activity.
5) The main activity of the company or person must not be an activity covered by Section 1 (1), nos. 14-18 and 20 of the AML Act.
6) The financial activity can only be offered to customers who are covered by the undertaking's main activity.

Re. 1) The first condition covers the undertaking's total revenue. This must not exceed the threshold value in points a or b.

Re. 2) The second condition includes the size of each transaction. Transactions include individuals and multiple transactions that appear to be interrelated.

If the company carries out more than one of the activities mentioned under no. 1 or no. 2, the lowest amount applies. This means that if the company provides currency exchange and another activity covered by Annex 1, nos. 1 or 4-12, e.g. deposit accounts, it is the threshold of EUR 500 that determines whether the individual transaction exceeds that. If it exceeds EUR 500, the company cannot be exempted from the AML Act.

Re. 3) This condition covers that the activity must not be the main activity of the company, and that the activity cannot exceed 5 percent of the undertaking's total revenue per year.

Re. 4) This condition covers the activity being an ancillary business, which means that the activity must be associated with the undertaking's main activity.

Re. 5) This provision covers activities provided by lawyers or law practices when they are covered by Subsection (1), no. 14, auditors and audit undertakings, real estate agents, real estate agencies, providers of services, providers of games and undertakings that commercially provide the same services as the persons and undertakings referred to. These cannot be exempted in accordance with Section 2 (2) of the Executive Order.

Re. 6) This condition covers activities that are not offered to the public, but only to the undertaking's customers who are customers in relation to the undertaking's main activity. The condition is therefore linked to the fact that the activity must be ancillary to the undertaking's main activity. Therefore, the activity cannot be offered to customers other than those who are customers for the undertaking's main activity.

Undertakings covered by the Executive Order must notify the FSA when they use the exemption. Notification must be given in writing every year.

1.4.2. Simplified requirements for KYC procedures for issuers of electronic money

Reference to the AML Act: Section 21 (2).

Reference to the 4th Money Laundering Directive: Article 12 (1).
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 7.

Reference: Executive Order no. 311 of 26 March 2020 on simplified requirements for the KYC procedure pursuant to the Act on Preventive Measures against Money Laundering and Terrorist Financing (the AML Act) for issuers of electronic money.

The Executive Order on simplified requirements for the KYC procedure under the AML Act exempts banks from the KYC procedures in Section 11 (1), nos. 1-4 and Section 14, when they issue electronic money, as well as certain other issuers of electronic money.

Five cumulative conditions follow from the Executive Order. This means that all conditions must be met in order for the company to be covered by the exemption:

1) the payment instrument is not reloadable or has a maximum monthly payment transaction limit of EUR 150, which can only be used in Denmark,
2) the maximum electronic amount stored cannot exceed EUR 150,
3) the payment instrument can only be used for the purchase of goods or services,
4) the payment instrument cannot be financed by anonymous electronic money, and
5) the issuer must perform sufficient monitoring of transactions or business connections to be able to detect unusual or suspicious transactions.

A payment instrument that is not reloadable, cf. no. 1, can include a gift card, the value of which cannot be increased once it has been issued.

The exemption concerning implementation of certain parts of the KYC procedure for electronic money providers does not apply to cash redemption or cash withdrawal of the monetary value of electronic money, if the redeemed amount exceeds EUR 50, or in the case of payment transactions initiated via the Internet or similar, when the amount paid exceeds EUR 50 per transaction.

2. Definitions

2.1. Money laundering

Reference to the AML Act: Section 3.

Reference to the 4th Money Laundering Directive: Article 1 (3).

Reference to other legislation: Sections 290 and 290 a of the Criminal Code.

"Money laundering" is defined as:

1) To unlawfully receive or obtain for oneself or others a share in economic proceeds or funds obtained by means of a criminal offence.
2) To unlawfully conceal, store, transport, assist in the disposal of or otherwise subsequently to act to secure the economic proceeds or funds obtained by means of a criminal offence.
3) Attempt at or participation in such actions.

There is no minimum value for when a situation is covered by the definition of money laundering.

The definition also covers acts by the person who committed the criminal offence from which the proceeds or funds originate. This is called "self-laundering", which is not punished under Danish law according to the general provision on handling stolen goods in Section 290 of the Criminal Code, because punishment for the underlying crime adequately deals with criminal liability for later related acts. Self-laundering, however, is covered by the provision on money laundering in Section 290 a of the Criminal Code, which only concerns money laundering.

Whether the actions which yield financial gain or the funds to be laundered were carried out in Denmark is not a decisive factor for determining whether money laundering is involved. Money laundering is deemed to exist even when the actions which yield financial gain or the funds to be laundered were carried out in the territory of another Member State or a third country.

The AML Act's definition of money laundering complies with Section 290 on receiving stolen goods and Section 290 a on money laundering in the Criminal Code.

> **§ 290.** Any person who unlawfully accepts or acquires for himself or for others a share in profits, which are obtained by a punishable violation of the law, and any person who unlawfully by concealing, storing, transporting, assisting in disposal or in a similar manner subsequently serves to ensure, for the benefit of another person, the profits of a punishable violation of the law, shall be guilty of receiving stolen goods and liable to a fine or imprisonment for any term not exceeding one year and six months, unless the situation is covered by Section 290 a.
> Subsection (2). When the receiving of stolen goods is of a particularly aggravated nature, especially due to the commercial nature of the offence, or due to the extent of the obtained or intended gain, or where a large number of offences have been committed, the penalty may be increased to imprisonment for any term not exceeding six years.
> Subsection (3).Punishment pursuant to this provision cannot be imposed on a person who accepts profits as ordinary subsistence from family members or cohabitants, or any person who accepts profits as a normal payment for ordinary consumer goods, articles for everyday use, or services.
>
> **Section 290 a.** Money laundering is punishable with fines or imprisonment for up to 1 year and 6 months for any person who converts or transfers money directly or indirectly derived from a criminal offence to conceal or obscure the illegal origin.
> Subsection (2). When money laundering is of a particularly aggravated nature, especially due to the commercial or professional nature of the offence, or due to the extent of the obtained or intended gain, or where a large number of offences have been committed, the penalty may be increased to imprisonment for any term not exceeding eight years.

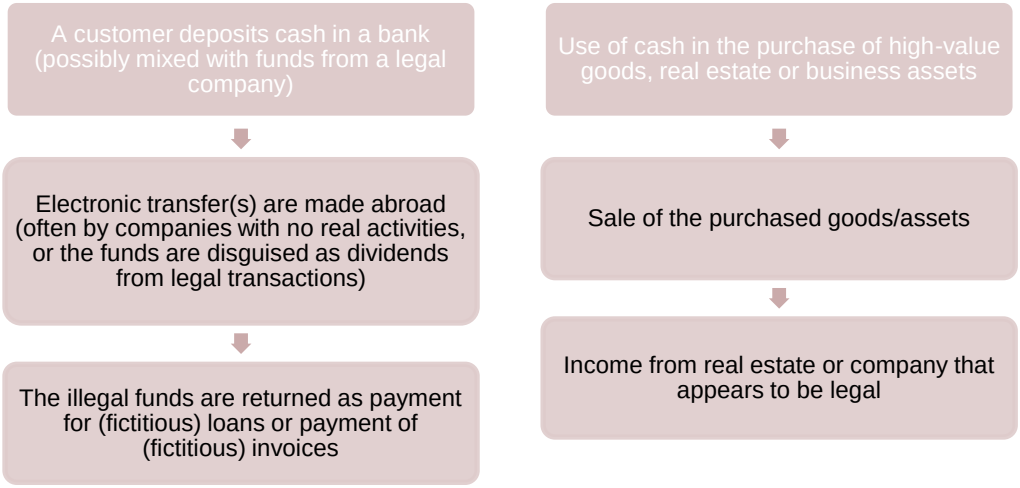
Re. 1) A characteristic feature of money laundering transactions and activities is that they aim to conceal the origin of funds through a camouflage process. It is not a requirement that the process be complicated, and in many cases the customer can have participated in a minor part of the process.

Re. 2) A crime includes violations of the Criminal Code, of special legislation and similar matters committed abroad for which there is statutory criminal liability. Tax evasion is a violation of tax, customs or duty legislation, obtaining or potentially obtaining unlawful gain.

In terms of criminal law, money laundering is covered by Sections 290 and 290 a of the Criminal Code, which concerns proceeds from all criminal offences.

Re. 3) Money laundering is also defined as an attempt to perform or participate in acts such as those mentioned in nos. 1 and 2. Attempts and participation are defined in accordance with Chapter 4 of the Criminal Code.

Below are examples of when money laundering can occur:



2.2. Terrorist financing

Reference to the AML Act: Section 4.

Reference to the 4th Money Laundering Directive: Article 1 (5).

Reference to other legislation: Sections 114 and 114 b of the Criminal Code.

"Terrorist financing" is defined in Section 4 of the AML Act. The definition is consistent with the definition in section 114 b of the Criminal Code, as regards acts covered by Section 114 of the Criminal Code, which define terrorism.

Section 114 b of the Criminal Code defines terrorist financing as the situations in which

1) financial support is directly or indirectly provided for,
2) the direct or indirect provision of or collection of funds for, or
3) the direct or indirect provision of money, other assets or financial or other similar services to a person, group or association committing or intending to commit acts covered by Section 114 or Section 114 a.

2.3. Ban on cash transactions

Reference to the AML Act: Section 5. Reference to the 4th Money Laundering Directive: Article 2 (1), no. 3, letter e and Article 11, letter d

Undertakings not covered by Section 1 (1) of the AML Act are subject to a ban on cash transactions laid down in Section 5 of the AML Act.

This means that business owners not covered by the AML Act's rules cannot receive cash payments of DKK 50,000 or more, regardless of whether payment takes place at once or as several payments which appear to be interrelated.

"Cash payments" are defined as payment in cash, i.e. physical money. The ban on cash transactions does not therefore cover e.g. payment by debit card, or a customer paying money into his/her own account, and then transferring that money to a dealer's account.

The ban includes sales that take place commercially. The ban includes not only the sale of items by a business owner, but also, for example, the provision of services and sales of real estate by business owners.

The ban applies even if the business owner receives cash payments at DKK 50,000 or more outside the country's borders.

Business owners who are not covered by Section 1 (1) are therefore only subject to the ban on cash transactions in Section 5 and the ban on EUR 500 banknotes. See Section 2.5.

The ban is based on the fact that large cash payments increase the risk of money laundering and terrorist financing.

2.3.1. Internally-related payments

The ban does not only cover individual payments, but also payments that appear to be interrelated, if the total amount is DKK 50,000 or more. This is to prevent the ban from being circumvented.

This does not mean that regular payments are subject to the ban as such, but if payment of, for example, rent on a property or a car, or payment of e.g. water and heating supply for a single period comprise DKK 50,000 or more, such payments will be subject to the ban on cash transactions.

If payment by instalments is involved, e.g. in connection with the purchase of belongings or real estate, or in connection with payment for a contract or travel, the individual instalments will be interrelated and the ban on cash transactions will affect instances when the total payment is DKK 50,000 or more. If, for example, a number of cash payments relate to the same invoice and the payments amount to DKK 50,000 or more, the ban will be violated.

In its judgment of 24 April 2019 in case 174/2018 (U 2019.2445 H), the Supreme Court ruled on when payments can be considered to be interrelated. According to the judgment, the ban will be violated when a business owner receives an individual cash payment of DKK 50,000 or more, regardless of whether the payment covers the purchase of one or more items, and regardless of whether the individual purchases may be interrelated. Furthermore, it is also irrelevant whether there has been separate invoicing of the individual purchases.

In the opinion of the FSA, it would be contrary to the ban if several payments that total DKK 50,000 or above are or appear to be interrelated. These payments do not have to be made at once when they relate to several different goods or services purchased under the same agreement. The condition on interrelation can be met if the payment covers several purchase agreements that are related, e.g. by virtue of a purchasing pattern or discount agreement.

It also follows from the FSA's view of the judgment that if a transaction is made under DKK 50,000, and the same customer returns later the same day without connection or relation to the day's first purchase and makes another purchase, whereby the sum of cash payments on the same day from customer exceeds DKK 50,000, there will be no breach of the ban on cash transactions.

2.4. Counterfeit money

Reference to the AML Act: Section 6.

Reference to other legislation: Article 6 (1) of the Council’s Regulation 2009/44/EC of 18 December 2008 on the amendment of Regulation 2001/1338/EC on the establishment of measures necessary to protect the Euro against counterfeiting, which contains a similar commitment in regard to Euro banknotes and Euro coins.

Undertakings that take part in the sorting and distribution of banknotes and coins to the public have a duty to take all notes and coins they know or have grounds to believe are false out of circulation, and to hand them to the police. The same applies to undertakings whose activities consist of washing notes and coins of different currencies.

The requirement of the AML Act does not include euro banknotes and coins, because a corresponding requirement for euro banknotes and euro coins is laid down in a regulation on measures necessary to protect the euro against counterfeiting. The regulation includes a requirement for the undertakings covered to ensure that euro banknotes and coins received by the company which the company will return into circulation to check them for authenticity, and that undertakings ensure that counterfeit euro banknotes and euro coins are identified and surrendered to the competent national authorities. See reference in the box above.

The requirement in the AML Act is therefore stipulated with regard to other types of currencies other than euro, including Danish kroner, also being subject to the obligation to surrender suspected counterfeit banknotes and coins immediately to the police.

2.5. Ban on the use of EUR 500 banknotes

Reference to the AML Act: Section 6 a.

Undertakings and persons are subject to a ban on the use of EUR 500 banknotes, which is laid down in Section 6 a of the AML Act. The ban on the use of EUR 500 banknotes covers all undertakings and persons and is thus not only aimed at undertakings covered by the AML Act. The ban applies regardless of whether the use of EUR 500 banknotes is part of a commercial activity or for private purposes.

The ban means that EUR 500 banknotes cannot be used, including handed out, handed in, exchanged, used as a means of payment or transferred, in Denmark. Only the use of EUR 500 banknotes in Denmark is covered by the ban. The provision has no significance for the use of EUR 500 banknotes in countries other than Denmark. The actual possession of EUR 500 banknotes is not covered by the ban, and it is thus not illegal to be in possession of EUR 500 banknotes, e.g. for use when travelling abroad for legitimate purposes such as holidays, business trips or the like.

Use
"Use" is defined as any activity in which one or more EUR 500 banknotes are transferred from one legal or natural person to another legal or natural person, regardless of the circumstances surrounding the transfer.

Cases in which a bank withdraws an amount in kroner in an account equal to the value of a EUR 500 banknote and then hands a EUR 500 banknote to the customer would be a violation of the ban.

Similarly, if a customer hands a EUR 500 banknote to a bank to be paid into the customer's account will also be a violation of the ban. The receipt and subsequent exchange of a EUR 500 banknote for other banknote values, or for another currency at banks and currency exchange companies etc., will also be a use in violation of the ban.

Any payment with a EUR 500 banknote will be a use in violation of the ban, including, e.g., payment with EUR 500 banknotes in supermarkets and other businesses. Purchases between non-business owners when a payment is made with a EUR 500 banknote, are also covered by the ban. Thus, both the transfer and receipt of EUR 500 banknotes in connection with the sale of an asset between two private parties are covered, and transfer of a EUR 500 banknote, e.g. in the form of a gift will be a transfer in violation of the ban, both in relation to giving and receiving the EUR 500 banknote.

However, the ban does not apply in cases when transfer of EUR 500 banknotes takes place in connection with a change of residence, e.g. the estate of a deceased person or a bankruptcy estate involving the distribution of their assets.

Part 2 – Risk assessment and management

3. Risk assessment

Reference to the AML Act: Section 7 (1). Reference to the 4th Money Laundering Directive: Article 8 (2), 1st paragraph.

The company must perform risk assessment of its inherent risk of money laundering and terrorist financing. "Inherent risk" in this connection is defined as the risk that exists for An undertaking to be abused for money laundering and terrorist financing. Initially, the precautions An undertaking may have taken to counter risk will not be taken into account.

Risk assessment must be performed based on the undertaking's business model, and identify which areas of the business are exposed to the risk of money laundering and/or terrorist financing, the size of those risks and how they can manifest themselves. An undertaking's "business model" is defined in this context as a combination of:

1) the customer types it has,
2) the products, services and transactions it offers customers,
3) the delivery channels it uses to provide products and/or perform services,
4) countries or geographic territories where its commercial activities are conducted,
5) the undertaking's organisation and
6) its corporate structure.

Risk assessment forms the foundation on which An undertaking can determine which business areas should be prioritised to avoid it being abused for money laundering and terrorist financing, and which operational procedures need to be put in place for the individual business areas. Risk assessment will thereby form the foundation for how the company designs its policies, procedures and controls, cf. Section 2 below.

A risk-based approach specifically means that the company has to identify and assess the inherent risk of being abused for money laundering or terrorist financing. The company can thus use its resources in areas where the risk is greatest.

Risk assessment must be based on relevant documents, such as the supranational and national risk assessment, experience gained via media and working with authorities etc., and especially the undertaking's own experience from customer monitoring etc. There are links to national and supranational risk assessments on the FSA's website, along with other links to documents that can be advantageously used in a risk assessment.2

The content and scope of risk assessment must be proportionate to the undertaking's risk factors, its size and scope of business. Risk assessments must be regularly updated to reflect the undertaking's current risk profile. The company must determine when a risk assessment has to be updated. In principle, risk

2 https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Links-vedr-hvidvask

assessment must be updated annually. It must also be updated when the undertaking's business model is significantly changed, or changes in new national or supranational assessments are deemed to be able to affect the risk assessments, also cf. Section 1.4 on exemption Executive Orders.

The figure below illustrates the process from identifying inherent risk to when residual risk is identified, when the company has made a decision on policies and procedures etc. The remaining risk once risk-mitigating measures have been included in the assessment can be regarded as residual. Refer to the description below.

As the figure below illustrates, there is inherent risk in an undertaking's business model of being abused for money laundering and terrorist financing. This can change if the company decides to change its business model, e.g. if it decides to change the composition of customer types, product types or delivery channels etc. If the company decides to generally remove certain risk factors from its business model in that way, it can reduce the inherent risk. The opposite applies if the company is exposed to new, or higher risk factors as the result of new products or new customer types. If and when the business model is changed and is fixed in place, the new, actual inherent risk is what the company must base its business procedures, policies and controls on.

The undertaking's policies and controls are its risk-mitigating measures, i.e. what the company does to achieve effective prevention, limitation and control of the risks of money laundering and terrorist financing. The residual risk the company runs of being abused for money laundering or terrorist financing is the risk that can remain, even with effective prevention, limitation and control.

Risk assessment does not need to be complex or wide-ranging, especially for undertakings with a simple business model, e.g. those which only sell few and simple products. The most important thing is that the company covers all risks. The objective is for assessment to act as an operational and applicable tool

that creates overview and an understanding of the undertaking's inherent risks, and what measures are necessary to limit them.

A risk assessment can be prepared by a central unit in a group/company with branches established in one or more countries, for example the parent company, but it is a requirement that the risk assessment is adapted to the individual legal entity's or branch's business model, including their risks and rules in the country they are established. The risk assessment must also be supported by information that is relevant to the legal entity or branch in question in the group. See Section 5 for groups.

3.1. Methods and documentation

The company must identify its risk factors, assess them individually and relationships between them. When performing assessment, the company must determine to what degree the risk factors identified affect the overall inherent risk. The company then has to specifically determine where and to what degree such factors can contribute to the company being abused for money laundering or terrorist financing, from a holistic perspective.

One way An undertaking can assess its overall risks, can be to weight the individual risk factors. Assessing risk factors must be based separately on the risk of money laundering and terrorist financing, as they can be different. Consequently, the company must take into account both aspects in its risk assessment. For example: a product can have a low risk of money laundering but a higher risk of terrorist financing. One example is small money transfers abroad. In principle, small, single transfers will represent low risk of money laundering, as only small amounts are involved. But a feature of terrorist financing is that there can be small transfers made to countries or geographical territories where terrorist activity takes place. The illegitimate purpose of such transfers is easier to conceal, when only small amounts are involved. That's why it is important that the company can assess its risks, bearing in mind that the risk factors for money laundering and financing terrorism respectively are not always of the same character.

The company must gather sufficient data to be able to identify all its risk factors. Section 7 (1) of the AML Act lists the risk factors that the company must take into account in its overall assessment. The Act's list of risk factors is not exhaustive, and undertakings must therefore be able to identify other relevant risk factors to the extent necessary. In its assessment of individual risk factors, An undertaking can also find that some factors are irrelevant to it, and therefore has no or a very limited inherent risk in relation to those particular risk factors. It is therefore relevant that the company compares such limited risks with other risk factors facing it, to be able to determine whether those factors can affect each other.

The company must document its assessment of its risk factors. That documentation must be linked to the undertaking's business mode, which also forms the basis of assessment. Risk assessment therefore requires a sufficiently thorough analysis of the business model. The company can use its own knowledge, experience from data gathers, customer knowledge, products in demand etc., as part of the documentation for its overall assessment. Furthermore, documentation of risk assessment must be based on the undertaking's thoughts and decisions based on supranational and national risk assessment, and/or in other relevant forms of documentation within the field, e.g. information issued by FATF, EBA and trade associations, along with management reports, e.g. on corruption, information from trustworthy or public or commercial sources and Part 2 of the guide, concerning the rules on risk assessment and risk management within money laundering, cf. the introductory section. The company can gain inspiration for relevant material from the FSA's website.3

3 https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Links-vedr-hvidvask

Documentation can be compiled by the company saving all details and documents it uses for its assessments, and notes the conclusions it reaches. The company can also document in internal information, observations, documents etc., in national or supranational assessments, reports, statistics etc. For instance, it can use supranational risk assessment of a specific product type to determine whether that product incorporates a risk of money laundering or terrorist financing, and thus assess and document the product's influence on the undertaking's risk profile.

3.2. Risk factors

Reference to the AML Act: Section 7 (1), 1st and 2nd paragraph. Reference to the 4th Money Laundering Directive: Article 8 (1).

When the company assesses its risk factors, it can seek help from Annexes 2 and 3 of the AML Act, which outlines situations that can be an indication for limited and high risk respectively. The annexes are not exhaustive. In addition, the company can assess its risk factors as listed below. Regardless of whether a risk factor is high or low in principle, the company must make its own assessments and monitor its customers in accordance with the rules of the AML Act.

3.2.1. Customer types

The company must assess its customer types as one of its risk factors. According to Section 7, risk assessment has to be based on the company and its overall risk profile, whereas according to Section 11, it will be based on its individual customers. See Section 13, on risk assessment – KYC procedures. The company can incorporate factors and general experiences from its Section 11 assessments in its overall risk assessment, but it is important that the company can differentiate between the different principles of the provisions, and therefore make independent assessments based from both provisions. The risk assessment in Section 7 must therefore be based on specific evaluations of individual customers.

Assessment can be generally based on to what extent the customer types are legal physical or legal persons, and then on their professional and commercial activities, reputation, conduct and, for legal persons, their beneficial owners. The assessment must be conducted at a general level. When using Section 7 assessment, the company must therefore not assess individual customers or beneficial owners. The company could, for example, assess to what degree a customer portfolio of legal persons with beneficial owners located abroad can affect the overall risk profile.

If the customers are legal persons, it will be relevant to look at their business types, and at which rules they are subject to. For example: listed companies can generally be regarded as limited risk, due to them being subject to a special duty to inform in accordance with EU law, whereas money transfer companies or currency exchange companies can generally be regarded as higher risk.

Several factors are relevant when An undertaking analyses its customer segment as a risk factor. For instance, it can be assessed whether a customer type:

1) is connected to a sector associated with a high risk of money laundering or terrorist financing,
2) is connected to a sector with large amounts of cash in circulation, or
3) includes politically exposed persons.

Analysis of customer types can also focus on:

1) The purpose of incorporating the company.
2) Whether the customer is subject to a duty to provide information according to some other legal requirement, which ensures greater transparency of the company type.
3) Whether the company has customer types with transactions in/to/from a country deemed to not have effective anti-money laundering and terrorist financing measures, or if the company has customer types that are undertakings established in such a country.
4) Whether the company has customer types that are undertakings established in a country with a high level of corruption.

The above points for an assessment are an inspiration for risk assessments, and not an expression of either a mandatory or exhaustive list. The company is responsible for determining its own assessment points.

3.2.2. Products, services and transactions

When An undertaking has to risk-assess its own products, services and/or transactions, it can determine whether they can be expected to be used for money laundering or terrorist financing, including:

1) to what degree the products, services and transactions are suitable to provide anonymity,
2) to what degree the products, services and transactions are complex and
3) the value and size of the products, services and transactions.

When determining whether the product, service or transaction is suitable for providing anonymity, the company can assess to what degree the recipient can conceal its identity. This can be the case for example, if the product or service consists of buying/selling of bearer shares or transactions with no direct contact to or awareness of the final recipient of securities or cash, etc.
When looking at the complexity of the products, services and transactions, An undertaking can assess:

1) whether the transactions with the product/service involve multiple parties or jurisdictions
2) whether the products, services or transactions give the customer the opportunity to receive payments from a third party, and that can be done from an unknown or non-associated third party, and
3) whether extraordinary payments can be made that are not regular and which do not depend on a fixed pattern, for example early repayment of a loan.

When determining the value and size of products, services and transactions, the company can assess to what extent the products or services involve cash handling/cash payments, and to what degree there are high transaction values/many transactions or the possibility of the same, e.g. whether a premium level or cap has been determined, which can limit the risk.

Products, services or transactions that, in principle, are limited risk, can include:

1) Life insurance policies with an annual low premium.
2) Pension schemes for employees with contributions paid directly from wage deductions.
3) Portfolio management when authority is only given to trade on behalf of the customer, and when the customer has an account or deposit account with another financial undertaking.
4) Products where the risk are controlled by other factors, e.g. transparency in relation to ownership. Examples include mortgages, along with portfolio administration and advice.

For further examples, see Annex 2 of the AML Act.

Products, services or transactions with potential high risk can include:

1) Private banking, wealth management or the like, because these are product types which normally are offered to very wealthy customers. It can also be the name of a customer segment ranging from standard products to customers with customised products with complex corporate products. Factors within private banking, wealth management or the like that can be linked to increased risk include frequent deposits and withdrawals of funds. It may therefore be easier to hide an illegitimate amount in large assets, and experience shows that an attempt is often made to launder money by converting it to returns on securities. Furthermore, this is a product type that can often create very close contact and loyalty between advisor and customer, which can make the extra monitoring a risk product needs more difficult. It will, for example, also be complex in those instances when products are customers for specific customers, and represent very large transaction values. It will therefore be relevant for this product type to ensure that awareness of the origin of the funds and the customer's purposes with the proposed transactions and investments etc.
2) Individual money transfers or those transfers that involve no real customer relationship, and therefore no good customer knowledge or monitoring will be achieved.
   Abuse of the product can be revealed by making several small transfers, which individually do not look suspicious. Experience shows that this product type is used for terrorist financing.
3) Currency exchange, because this is a product which often involves no fixed business connection, which means no in-depth awareness of the customer's purpose and the origin of the funds can be ensured. Otherwise, there are transactions that often involve cash.
   Currency exchange has been know to be used for terrorist financing by exchanging Danish kroner to Euros or American dollars, physically sent for use as terrorist financing.
4) Products and services using new technologies, and where there is no experience of their use, nor sufficient awareness of the potential risks as a result.

For further examples, refer to Annex 3 of the AML Act. The national and supranational risk assessments also stipulate how money laundering and terrorist financing can occur, and where risks are high.

3.2.3. Delivery channels

The undertaking's transactions and delivery channels are also of key importance for an undertaking's risk assessment. Identification of an undertaking's delivery channels can allow general definition of:

1) how a business relationship with customers was established, and
2) how the company delivers its products, services and transactions to the customers.

An undertaking can also assess:

1) to what extent a business relationship consists of no physical contact with the customer or counterpart, and without e.g. digital security measures in place. Physical contact with a legal person can include when the legal person is represented by another person with proxy/authorisation,
2) which external parties/counterparts are needed to be able to deliver the product or perform the service, and
3) any parties or middlemen introduced, the undertaking's users and the nature of their connection to the company.

For example, the company can determine whether the customer was introduced by a third party, and what it knows about that third party, including whether the third party has effective procedures for combatting money laundering and terrorist financing, is based within the EU and subject to efficient supervision in that country, is subject to rules on the prevention of money laundering and terrorist financing.

Delivery channels that, when seen in isolation, can indicate a limited risk can include:

1) A business relationship entered into with physical contact with the customer or with electronic solutions to which there is considerable trust.
2) Ordinary deposits with no external delivery channel, i.e. when deposits are made such as wages paid in, and withdrawals via normal payment transactions.
3) Mortgage credit loans, when the customer is introduced to the mortgage credit institution by the customer's bank.

For further examples, see Annex 2 to the AML Act.

3.2.4. Country and geographical territories

The company must assess risks that can be associated with countries or geographical territories to which it has links. When the company has positive awareness of a customer segment or the customer's beneficial owners in relation to countries and geographical factors, it can include for example:

1) in which countries the customer types and/or beneficial owners are based
2) in which countries the customer types and/or beneficial owners run their business, and
3) in which countries the customer types have relevant personal or commercial links.

In its general risk assessment, the company must not assess specific customers, but deploy its knowledge of its customer types and the beneficial owners of customers. If, for example, the company has a customer segment in which the beneficial owners are located in a high risk country, this should be included in risk assessment of its risk factors in relation to countries and geographical territories:

As such, it is not necessary for the company to investigate individual customers or beneficial owners to be able to compile its risk assessment.

In connection with awareness of its customer types and analysing which countries they are based in or have their personal/commercial connections in, the company can assess the geographical factors, such as:

1) whether the country has sufficient rules designed to prevent and combat money laundering and terrorist financing
2) whether the country has an effective supervisory authority within the field
3) whether the customers have relationships to a country or geographic territory where money is generated with a high risk of money laundering, or with a high crime rate in the field
4) whether money is sent in relation to customers to countries where there are known terror activities
5) whether the company has foreign politically exposed persons as customers, and whether they have geographical links that could be deemed to be a sign of increased risk for money laundering or terrorist financing
6) whether the company has customers on EU sanction lists.

When the company has to evaluate the country's rules and effectiveness of its supervisory authorities, it can use FATF reports, black and grey lists, reports written by the FSRB and OECD, Transparency International's corruption list, and other sources.4

3.2.5. Sector-specific examples

This section contains specific examples of risk assessments. The examples can be used to support undertakings in their risk assessment, but undertakings themselves have to make their own specific assessments. The examples are expressions of situations that involve a risk, including high and limited risk. They are relevant because even a limited risk provides a reason why An undertaking should perform specific risk assessment.

Stockbroker undertakings:
The following example can illustrate a specific assessment for stockbrokers.

Stockbrokers must assess the products or services they provide. Annexes 4 and 5 of the Financial Business Act are therefore relevant to stockbrokers to identify them. Several products and services will represent limited risk seen in isolation, and should therefore be assessed in relation to the other risk factors, including the customer types and possible geographical links the stockbroker has. For example: a stockbroker can provide discretionary portfolio management in which the transactions are purely conducted via a bank, when the broker has sufficient confidence that there are effective procedures in place to combat money laundering and terrorist financing. A stockbroker can also offer discretionary portfolio management in which transactions take place via a group of securities traders, but when all transactions are settled directly on the customer's account and deposit account at the customer's bank following instructions from the stockbroker. In principle, such products will be deemed to involve limited risk, but if the product is provided to PEPs or other high-profile or foreign customers, the actual customer type can imply higher risk, which is why KYC procedures will be needed to ensure good, updated knowledge of the customers and the origin of their funds.

Financial leasing:
The following example can illustrate a specific assessment for undertakings providing financial leasing.

When providing financial leasing for vehicles, the company must bear in mind that this type of product/service can be abused for terrorist financing. A person can lease a car with no intention of returning, and then report the vehicle stolen with the intention of e.g. selling the vehicle for terrorist financing.

The person may also keep the vehicle to be used by a terrorist organisation in combat in conflict zones, or for terror attacks in western countries. If the intention of leasing a vehicle is to take it to a conflict zone, it will often be a large vehicle suitable for use in such areas, e.g. a large SUV, 4x4 or similar. An indicator of this customer type can be persons looking for a certain type of vehicle for use in conflict areas, as described above and/or who have not previously owned a vehicle.

A factor that can indicate limited risk for leasing products/services is when a low value product is involved.

Life insurance and pension undertakings:
The following example can illustrate a specific assessment for undertakings providing pension schemes:

4 https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Risikovurdering-af-lande

Pension schemes started as an employment benefit are always set up via an employer. The employer pays in its own and the employee's contributions to the scheme.

Therefore, the risk is generally very low for a mandatory pension scheme established as part of an employment relationship can be used for money laundering. This situation does not change even if the scheme offers the option of supplementary voluntary contributions and possible surrender, which can primarily be due to a taxation situation. The pension company will calculate labour market contributions when paying tax or duties upon disbursement.

There is a higher risk that pension schemes that are not tax-favoured can be used for money laundering compared to those that are tax-favoured.

An example of a non-tax-favoured scheme is a "Section 53 A pension scheme" according to Section 53 A of the Pension Tax Act.

Section 53 A schemes are often used in connection with foreign postings and the like, when an employee continues payment of contributions to a previous employer contribution scheme, but no longer has an income in Denmark to make use of the tax deduction. But the scheme can also be taken out privately, although it is less attractive to persons who are taxable in Denmark.

Because the funds are taxable, and which therefore have to be taxed at the time of disbursement, the policyholder and the pension company are free to agree a shorter disbursement period. Consequently, this implies a risk of the pension-taker seeking to use contributions to the scheme to launder funds originating from criminal activities, including tax fraud. This, along with a possible shorter disbursement period, mean that the scheme can be more attractive for money laundering attempts than other pension products.

Life insurance:
The following example can illustrate a specific assessment for undertakings providing life insurance:

Low premiums for a life insurance policy, as stated in Annex 2 of the AML Act can be viewed based on the undertaking's profile, the product and specific customer. What is considered a low premium in the individual company will therefore differ.

Group life schemes for private individuals tend to be large schemes with low premiums, but health details are often required when taking them out. The risk associated with group life insurance policies is limited, as a result of an insurance event having to occur before disbursement can be made.

The same applies for job market pension schemes/company pension schemes.

Providers of currency exchange between virtual currencies and fiat currencies:
For undertakings offering exchange between virtual currencies and fiat currencies, the following examples can illustrate a specific assessment:

When exchanging virtual currencies with enhanced anonymity – referred to as "Privacy Coins" – the undertaking must be aware that this type of product can be used for money laundering and terrorist financing to the same extent as cash. The undertaking's ability to determine the origin of the funds and

the purpose of the business relationship is limited, as the business relationship can send and receive these virtual currencies without leaving digital traces.

Similarly, there is a risk of exchanging virtual currencies that have undergone several exchanges in advance, with the aim of obscuring a pre-crime. Pre-crime is typically fraud (scams), ransomware and hacks. The previous exchanges to obscure the pre-crime can take place, for example, by using services such as "tumblers", "mixers" and "scramblers". However, a pre-crime can also be obscured without the use of a service, but by the fact that the virtual currencies are sent between a number of different addresses and possibly also split up into smaller sums before being exchanged for fiat currency.

Payment initiation services:
The following example can illustrate a specific assessment for undertakings providing payment initiation services:

A payment initiation service provider (PISP) initiates a payment order at the instruction of the user for the purpose of making a payment transaction from a payment account provided by a payment service provider other than the PISP. Unlike other providers of payment services, a PISP does not conduct payment transactions itself, and cannot hold or take possession of the user's funds. This may mean that the money laundering risk for a PISP may be limited, but it also means that a PISP should consider other risk factors than other providers of payment services.

Based on its business model, a PISP must consider which customers it enters into business relationships with. It can, for example, be an internet business that regularly receives payments for goods and services from customers via the payment initiation service. It can also be natural persons who use a PISP (often in the context of an account information service) to manage a number of different accounts, which may be maintained by several different account operators.

Payment initiation services are a new type of authorisation. There is therefore still a great deal of development in business models that can be covered by an authorisation. It will thus depend on the specific business model as to how a PISP must comply with its obligations under the AML Act. Regardless of the fact that the risk of money laundering may be limited, and that transactions are typically carried out via customer bank accounts, a PISP cannot rely solely on the fact that the account-holding institution is covered by the requirements of the AML Act.

A PISP initiates payments via an API or dedicated interface provided by the account operator, typically a bank. Due to its technical design, an API can restrict the information available to a PISP. This can be, for example, information about the identity of the owner of the account from which a payment is made. Regardless of whether a PISP is not obligated beyond what an API makes possible, it must continuously monitor and assess which transactions its customers initiate and whether these give rise to further investigation, cf. the duty to investigate in the AML Act.

As a rule, a PISP should always carry out a risk assessment of the customer relationship. In this context, a PISP should take into account geographical factors, for example if payments are made to or from a payment account maintained in a high-risk country. A PISP should also include matters concerning the customer, e.g. that the customer makes a number of payments to the same recipient, regardless of whether this is from the same or different accounts, that the customer makes large transactions, or that the customer's transactions are otherwise unusual.

3.3. Updating risk assessment

The undertaking's risk assessment must be regularly updated. That means that it must reflect the undertaking's current risk profile. How often it has to be revised is up to the undertaking to determine. It depends on specific risk assessment in relation to the business model. But in principle, risk assessment must be updated at least once annually.

An update of the undertaking's risk assessment can consist of the undertaking performing risk assessment, and finding that there is no reason to update it. Similarly, the undertaking may also find that it is only necessary to update parts of its risk assessment.

In exceptional circumstances, the undertaking can update its risk assessment at longer intervals, if the conditions and risk factors are static and do not change.

The undertaking can decide that a risk assessment has to be updated at fixed intervals. But it should at least be updated when there are significant changes in the undertaking's business model and/or risk factors, and when there are new national or supranational risk assessments with new assessments, even if the undertaking has set a fixed interval for its updates.

The undertaking can deviate from its fixed intervals, e.g. if it postpones updates for a few months when it is aware that new national risk assessments or the like will be imminently introduced.

If an undertaking has a business model in which risk factors can change often, that is complex or previous risk assessments have shown that it has a high inherent risk of money laundering or terrorist financing, the risk assessment ought to be updated more often, to ensure that it is in line with the relevant risk profile.

The principle of updating once annually means that the undertaking must determine whether updating of the risk assessment is needed as a minimum.

When a risk assessment is updated, the undertaking must determine whether and how its policies, procedures and controls also ought to be updated, to bring them into line with its overall and current risk profile.

If the undertaking has not changed its business model and no external risk factors have changed that make doing so necessary, the undertaking will probably have no need to change it policies, nor, perhaps, its procedures and controls.

The undertaking should regularly review its risk factors, including, for example, whether it has entered into business relationships with new customer types, has developed new products, new systems, or offers services in a new geographic territory. The undertaking must use these occasions to assess its risk factors to determine whether there have been any changes in the risks that will affect the actual risk profile. This should also be done regularly in line with the undertaking performing e.g. risk assessments as part of its KYC procedures in accordance with Chapter 3 of the AML Act.

The undertaking must be aware that if changes are made to its business model, e.g. if it decides to launch new products, services or use new delivery channels, the risk assessment should be updated before beginning to use these new technologies.

The undertaking's procedures and controls must ensure that new, general trends or changes in its risk factors are detected, and that relevant information sources are accessed.

4. Policies, business procedures and controls

Reference to the AML Act: Section 8 (1).

Reference to the 4th Money Laundering Directive: Article 8 (3) and (4).

Executive Order no. 1026 of 30 June 2016 on the management and governance of banks, etc.
Executive Order no. 1723 of 16 December 2015 on the management and governance of insurance companies, etc.

4.1. Background

Section 8 of the AML Act sets out requirements for written policies, business procedures and internal controls to be devised by the undertaking.

Policies in this context are the undertaking's overall decisions on how it will be organised and how tasks related to the prevention of money laundering and terrorist financing will be tackled on the basis of the understanding of the undertaking's risk profile achieved from the risk assessment.

Business procedures are the undertaking's specific, operational application of its policies, converting assessments into e.g. business procedures and work descriptions.

Controls are the means the undertaking uses to ensure observance of its decisions and business procedures within the field of money laundering. Furthermore, there must be independent internal control to ensure that checks are performed, that they are appropriate and effective. The controls must be described in the undertaking's policies and procedures.

See the figure below for an illustration of the process regarding the requirements of the AML Act on risk assessment and management. The process is simplified by dividing it into three parts.

The policies in the area of money laundering must be prepared on the basis of the risk assessment the undertaking has carried out in accordance with Section 7 (1). There are no formal requirements for the undertaking's policies and business procedures, but they must be in writing and must be accessible to and effective for the undertaking. They must at least include policies and business procedures for:

1) Risk management.
2) KYC procedures.
3) Subject to a duty to investigate, register and report.
4) Record keeping.
5) Employee screening.
6) Internal controls.

The fact that policies and business procedures must be in writing does not mean that they must be in paper form. They can be stored digitally. Because there are no format requirements, neither are there requirements on policies and business procedures for each part being formatted in separate documents. The overall objective is for the undertaking to assess and document its inherent risk, determine its overall strategic goals and operational methods to achieve them, and controls to ensure they are complied with.

The undertaking's policies, business procedures and controls within the money laundering area must be approved by the AML Officer with regard to whether they are sufficient to fulfil the requirements of the AML Act. The undertaking must be aware that there can be requirements in other legislation that its policies must also be approved by the Board of Directors. Undertakings required by other legislation to have a compliance function must appoint a Compliance Officer, who must impartially control and assess whether the undertaking's policies, procedures and controls are effective to prevent and combat money laundering and terrorist financing, and whether they are complied with. If an undertaking has an inde-

pendent internal audit function, it must further ensure compliance with the duty incumbent on the undertaking under Section 8 (1). To the relevant extent, undertakings must also appoint a member of the Executive Board, who must ensure that the undertaking complies with money laundering legislation.

In summary, this means that the undertaking can have up to four parts to ensuring that its policies, business procedures and controls are affective, and that it complies with the AML Act. For some small undertakings, only an AML Officer will be relevant, and for others with a compliance function requirement, the AML Officer can also be the Compliance Officer if the undertaking has legitimate justification given its size or composition of activities. In such instances however, the undertaking must focus on the tasks given to the AML Officer are not those that ought to be performed by its compliance department in principle. Therefore, it is necessary to at least ensure that employees are not involved in the execution of tasks that they check as part of their compliance tasks.

4.2. Policies

The undertaking's policies in the money laundering area must include identification, assessment and definition of its risk factors as conclusions of its risk assessment, and the overall strategic goals for prevention of money laundering and terrorist financing for the risks identified.

The undertaking's inherent and subsequent residual risk reflect its risk profile within the money laundering area. The undertaking's risk willingness will therefore lie in the business model it has developed. "Risk willingness" is defined as the undertaking opting to accept certain inherent risks in its choice and design of business model. It means that the undertaking runs must reduce its risk of being abused for money laundering and terrorist financing by deploying risk-reducing measures to bring residual risks down to an acceptable level. The residual risk the undertaking runs of being abused for money laundering or terrorist financing is the risk that can remain, even with effective prevention, limitation and control.

An example of the above is that if the undertaking chooses to provide services to countries with increased risk outside the EU, it must ensure efficient business practices that take into account the increased exposure to risks that the undertaking acquires by providing services to such countries. The undertaking can have a business model with a high inherent risk, but that will mean that it has to have appropriate resources and design effective politics, business procedures and controls that reduce the risks its business model implies to an acceptable level. Furthermore, the undertaking must ensure that customer monitoring is put into place, which is proportional to the risks it has.

The undertaking's policies must therefore include descriptions of the risk factors it is willing to accept, and instructions on how its strategic goals can be achieved.

As described above, risk willingness can be the undertaking considering whether there are product types it will not provide, or whether there are particular geographical territories it does not want to be based in.

The undertaking's policies must include consideration of:

1) identification and defining the risks it is willing to accept in its business model,
2) the principles for risk management,
3) the purpose of risk management,
4) the undertaking's risk areas,
5) risk willingness,

6) delegation of responsibility, and
7) the organisation of risk management within the undertaking.

The undertaking's policies must be written in one or more documents.

4.3. Business procedures

"Business procedures" within the money laundering area are defined as a description of the activities the undertaking executes to ensure it complies with the legislation, and that its policies and procedure are complied with.

Business procedures must be based on the undertaking's business model, policies and its individual circumstances. They must be an easily-deployable tool for the undertaking's employees, and must therefore clearly describe the business area, delegation of responsibility (including who is responsible for performing the individual tasks), and how they will be performed.

Business procedures must describe how the following areas are tackled in practice:

1) Risk management.
2) KYC procedures.
3) The duty to investigate, register and report.
4) Record keeping.
5) Employee screening.
6) Internal controls.

Business procedures must describe the individual activities for the tasks in each area. An example of this in relation to the duty to register can be a description of where employees in an undertaking must make their notes, e.g. on customer profiles in the undertaking's case management system, and which type of observations and information should be noted.

It is a requirement that the documentation of business procedures is easily accessible and clear to the employees.

4.3.1. Risk management

An undertaking's risk management within the money laundering area must be based on its business model and the risks the undertaking has identified from its risk assessment.

Risk management is the undertaking's awareness of risks, and how it will react to and deal with newly-discovered risks.

The undertaking must ensure that it is organised in a manner that ensures clearly-defined areas of responsibility, and that there are effective business procedures in place to identify, monitor and report on risks of the undertaking being or could be abused for money laundering or terrorist financing. In addition, the undertaking must have business procedures for how it handles identified breaches of undertaking policies and its business procedures.

Risk management also implies that the undertaking must track risk development within money laundering and terrorist financing, taking into account how they affect its risk assessment and thus also its policies, business procedures and controls.

4.3.2. Employee screening

The undertaking shall prevent employees abusing their position for money laundering and terrorist financing or participation in the same.

"Screening" consists of the following two elements:

1) Checking that employees do not have a criminal record that can increase the risk of them abusing their position.
2) Checking that employees have sufficient qualifications within the money laundering area to handle the position.

Re. 1) Check that employees do not have a criminal record that can increase the risk of them abusing their position.

Screening employees with a risk of abusing their position for money laundering or terrorist financing, including participation in the same, must be performed before they are employed. For example: the undertaking can check by asking the employee to produce their criminal record. Not all crimes increase the risk of the person abusing their position. For example: a sentence for financial crime and serious tax fraud will, in principle, mean a higher risk. A materiality consideration can therefore be performed in relation to which crimes do imply a higher risk.

But it is important that screening is always based on a risk-based approach, and is proportional to the employee's position and the function they will be fulfilling. The undertaking needs to take into account which functions are specifically relevant for the application of screening procedures.

It is not a requirement that all employees must be screened, but that the function an employee will be fulfilling must be looked at. For example: it will not be relevant for employees not performing functions that ensure compliance with the AML Act. But screening of employees will always be relevant when an employee performs a function where they can directly or indirectly abuse their position to participate in money laundering or terrorist financing. This will be relevant for example when:

1) Employees conduct KYC procedures.
2) Employees can carry out transactions.
3) Employees have been delegated tasks by the AML Officer.
4) Employees work in the undertaking's compliance function.
5) Employees work in the undertaking's internal audit or internal audit function.

Employees in senior and/or trusted positions will also be particularly relevant to screen.

The undertaking must also use risk-based grounds to ensure that it is informed if an employee is sentenced for a criminal act that can increase the risk of them abusing their position while employed. This can be done, for example, by:

1) the undertaking inserting a duty to inform in its employment contracts, obliging employees to inform the undertaking if they are sentenced for a crime during their employment, or
2) the undertaking regularly or at random asks its employees to produce their criminal record and retain proof of them being produced.

The proposed procedures are examples, and are therefore not an expression of the practice an undertaking is obliged to perform. The undertaking can determine itself which procedures are the most appropriate in relation to achieve the purpose of rules on screening, and that comply with data protection law. If the undertaking screens at regular intervals, it can determine the interval based on risk assessment.

An employee changing job within the undertaking can justify screening if not previously performed.

Employees can order their criminal record digitally from the police website if they have NemID.

Re. 2) Check that employees have sufficient qualifications within the money laundering area to handle the position. The requirement for screening also implies that the undertaking must ensure that employees possess the necessary qualifications within the money laundering area to be able to satisfactorily fulfil the position. However, these can be acquired by training after appointment. The undertaking must always ensure that its employees have the necessary ability, know-how and expertise to efficiently fulfil their function in the undertaking.

The undertaking's business procedures and internal controls must take into account that an employee may abuse his or her position, cf. Section 7 on training.

4.3.3. Internal controls

The undertaking must set up internal controls, which means it must ensure that it checks whether the requirements of the law are upheld within the money laundering area.

The undertaking must describe its controls in its business procedures and how it will document the controls performed. As such, there must a description of what a control is intended to ensure, how often it must be performed, how it will be performed and how it will be reported to the management and other units within the organisation. Reference is made to provisions on internal controls in the management Executive Orders.

When an undertaking has a Compliance Officer, controls must be performed as part of normal operations and by the Compliance Officer. This means that the first line control must be performed in the undertaking's business, while the second line control must be carried out concurrently by the Compliance Officer. How controls must be performed for other undertakings or persons must be determined. See Section 6.3 on Compliance Officer.

To ensure effective control, there must be a sufficient degree of independence between the person performing the control and the person subject to the control. In small undertakings, it can be sufficient for the direct manager to perform checks on employees, while in large undertakings it can be appropriate for checks to be performed by another department.

Internal controls consist of the following two elements:

1) verifying that undertaking policies and business procedures are complied with
2) verifying that the controls are carried out and are appropriate

Controls must be carried out at an appropriate interval to ensure that policies, business procedures and controls are complied with. Controls must be performed on the following areas:

1) Risk management.
2) KYC procedures.
3) The duty to investigate, register and report.
4) Record keeping.
5) Employee screening.

For example: controls can be performed by the undertaking making random checks on the various areas, and checking that business procedures within each area are complied with.

Undertakings must adapt their internal controls to the size of the undertaking and the risks associated with their business model. Undertakings that are run by only one person, e.g. a sole proprietorship without employees run by the proprietor, can therefore adjust their internal controls according to the size of the undertaking and the fact that there cannot be the same independence in internal controls as is possible when there are multiple employees. An example of internal controls in this type of undertaking include the owner making a series of random checks at fixed intervals, e.g. 2-3 times a quarter, and checks that the undertaking's business procedures have been complied with. It can e.g. be a check of whether sufficient customer knowledge procedures have been carried out, and correct material obtained as a result, and that sanction lists have been checked.

5. Groups

Reference to the AML Act: Section 9 (1) and (2) and Section 31. Reference to the 4th Money Laundering Directive: Article 45 (1).

Section 9 of the AML Act deals with group undertakings. This provision covers the relationship between several undertakings in a group, while Section 8 regulates individual undertakings in the group.

The requirements in Section 9 only apply to those parts of the group to which the AML Act applies to. See Section 1 (1) of the Act.

This means that if a subsidiary is not covered by the AML Act, there is no requirement that group policies and business procedures apply to that subsidiary.

The requirements in Section 9 do not apply to groups in which only subsidiaries are covered by the AML Act.

5.1. Exchange of information in groups

Undertakings in groups must have sufficient:

1) written policies for data protection, and
2) written policies and business procedures for the exchange of information within the group for combatting money laundering and terrorist financing.

Within the rules on the exchange of information, it is possible for undertakings in a group to exchange information if they comply with the group's business procedures in this regard, which must comply with

the requirements of the AML Act. Business procedures for the exchange of information in a group must be prepared in accordance with data protection legislation.

5.2. Group risk assessment, policies and business procedures

Risk assessment, policies and business procedures in a parent/principle company must cover the entire group, although only those parts of the group covered by the AML Act. This means that risk assessment, policies and business procedures can be devised by a central unit in the group, such as the parent/principle company. However, it is a requirement that they are adapted to the conditions of the individual legal entity or branch, including their business models and the risk status and rules of the country they are established in.

It is the responsibility of the parent/principle company to assess risk, devise policies and business procedures at group level.

Undertakings that are part of a group must implement the group's policies and business procedures. Overall, the policies and business procedures of the individual legal entity or branch must be in accordance with that of the parent/principle company.

Policies and business procedures of foreign undertakings with subsidiaries or branches established in Denmark must live up to the requirements of the AML Act with regard to matters that specifically concern Denmark. This means, for example, that risk assessments specifically concerning Denmark must be included.

Conversely, Danish groups with subsidiaries or branches in other countries must ensure that group policies and business procedures comply with the host country's (the country of incorporation) rules on preventive measures against money laundering and terrorist financing.

The rules on cross-border activities include a requirement that the parent/principle company ensures that its group policies, business procedures and controls for risk management, KYC procedures, the duty to investigate, record and notify, record keeping, screening of employees and internal controls comply with national regulations in the host country.

In addition, the parent/principle company must ensure that regular checks are performed on compliance with policies, business procedures and controls in the established undertaking. This can be done by random checks or visits to the undertaking.

The term "group" is defined in accordance with the Companies Act's definition of group.

6. Persons responsible and functions

The AML Act sets out requirements that a number of persons and functions fulfil the Act's requirements in different areas. Some of them apply to all undertakings subject to the requirements of the Act, whilst others only apply to financial undertakings.

The different responsible personnel and functions are described in the following.

Provision	Section 7 (2) (Section 8 (2))	Section 8 (3)	Section 8 (4)	Section 8 (5)
Function	**AML Officer**	**Compliance Officer**	**Internal auditors**	**Responsible Executive Board member**
When a responsible person must be appointed:	Appointed in undertakings covered by Section 1 (1), nos. 1-8, 10-11, 19, 23 and 24 of the AML Act.	Appointed when the undertaking is compelled by legislation to have a Compliance Function.	Applies to undertakings covered by Section 1 (1)-(7) and that have internal audit.	When deemed relevant, undertakings must appoint a member of the Executive Board responsible for implementation of the requirements in the AML Act.
Which tasks responsible personnel must fulfil:	Approve undertaking policies, business procedures and controls in the area of money laundering. Approve business relationships with customers domiciled in a high-risk third country (Section 17 (2)), with PEPs (Section 18 (3)) and with correspondent relationships (Section 19 (1), no. 3).	Independently check and assess whether the undertaking's business procedures and measures are effective.	Assess whether the undertaking's policies, business procedures and controls are appropriate and work satisfactorily in accordance with the requirements of the AML Act.	Ensure that the undertaking implements and complies with the requirements of the AML Act through effective policies, business procedures and controls.
Who is responsible:	An employee or a member of the general management who has the authority to make decisions on behalf of the undertaking.	Person at management level.	Internal auditor appointed by the Board of Directors.	A person who is a member of the Executive Board. In undertakings with only one director, it will automatically be that person.

6.1. AML Officer – the person appointed according to Section 7 (2)

Reference to the AML Act: Section 7 (2), Section 8 (2), Section 18 (3) and Section 19 (1), no. 3.

Reference to the 4th Money Laundering Directive: Article 3 no. 12, Article 8 (5), Article 19 (1), letter c, and Article 20 (1), letter b, (i).

The general management, which is often the Executive Board, must appoint an employee authorised to make decisions on behalf of the undertaking on approval of the undertaking's policies, business procedures and controls, and on approval of special customer relationships. The requirement applies to the following types of undertaking:

1) Banks.
2) Mortgage credit institutions.
3) Stockbroker companies.
4) Life insurance companies and multi-employer occupational pension funds.
5) Savings banks.
6) Providers of payment services and issuers of electronic money, cf. Annex 1, nos. 1-7, of the Payments Act.
7) Insurance brokers, when they provide life insurance or other investment-related insurance.
8) Undertakings performing commercial activities as stated in Annex 1 of the AML Act.
9) Investment management companies and managers of alternative investment funds, provided such undertakings have direct customer contact.
10) Danish UCITS and alternative investment funds, provided such undertakings have direct customer contact.
11) Currency exchange companies.

Subsidiaries of foreign undertakings are not covered by the requirement.

To fulfil the requirement, the person appointed must be actually involved in the undertaking's work with prevention of money laundering and terrorist financing.

The AML Officer can be a member of the undertaking's general management, or another employee. The AML Officer must be able to make decision concerning the undertaking's risk exposure within the money laundering area. The AML Officer's responsibilities and authority to approve does not relieve the undertaking's management of overall responsibility. The authority will ensure that the AML Officer has decision-making competence at management level when not a member of the management. There can also be instances of the AML Officer making a decision on approval of e.g. a business relationship with a politically exposed person opting to obtain further approval from the general management, because the risk profile of the politically exposed person represents a significant risk of money laundering or terrorist financing.

The requirements of the AML Act are that the AML Officer must have sufficient knowledge of the undertaking's risk profile and specific risk factors. In large undertakings, the CEO cannot be appointed, as that person will already have a considerable portfolio of tasks, and work at a level that is too high to effectively be able to fulfil the responsibilities set out in Section 7 (2).

The specific framework for the person's involvement will be determined by the undertaking itself. It is important that the person can take responsibility, has access to the undertaking's customer databases and other relevant information, including minutes from board meetings and audits.

6.2. The responsibilities of the AML Officer

The AML Officer must:

1) Have the authority to make decisions on behalf of the undertaking for approval of the following:
    a) policies, business procedures and controls (Section 8 (2))
    b) establishment and continuation of business relationships established in a country included in the European Commission's list of high-risk countries (Section 17 (2));
    c) establishment and continuation of business relationships with PEPs (politically exposed persons), their related parties and close collaborators (Section 8 (3))
    d) establishment of cross-border correspondent relationships (Section 19 (1), no. 3)
2) Have an understanding and insight into the undertaking's risks with regard to money laundering, and therefore be able to make decisions advantageous to the undertaking's combatting of money laundering and terrorist financing.

The undertaking should arrange the AML Officer's work such that employees and the senior management can consult with the AML Officer on all relevant areas, and be briefed as soon as there is anything new of relevance.

Furthermore, the AML Officer must be sufficiently independent and able to report directly to the Executive Board and Board of Directors on aspects within the area of money laundering and terrorist financing. It is important to emphasise that reporting to the Board of Directors is an option that the AML Officer must use if deemed necessary. There is therefore no general duty imposed on the AML Officer to report to the Board of Directors.

The AML Officer must follow the business procedures the undertaking has implemented within the area of money laundering and terrorist financing. In undertakings compelled to have a compliance function, the Compliance Officer shall investigate and perform independent checks that the procedures of the AML Officer are effective.

6.2.1. Delegation

The AML Officer can delegate the duties specified in the provision to one or more employees with adequate knowledge of the undertaking's risk profile in relation to money laundering and terrorist financing. Any delegation must involve one or more named persons or named positions. There can never be any doubt about which person or position the task is delegated to. The tasks to be performed under Section 7 (2) cannot be delegated to a unit in an undertaking, for example its compliance function.

Delegation to one or more persons will be particularly relevant in large undertakings with multiple departments working in areas covered by the AML Act. It is important to note that responsibility that follows from Section 7 (2), cannot be delegated, but is the responsibility of the person appointed in accordance with the provision.

Because responsibility always lies with the AML Officer, delegation of tasks to one or more other named persons or positions can, for example, be subject to a requirement for reporting or the like to the AML Officer, such that he/she continues to bear the ultimate responsibility.

6.3. Compliance Officer

Reference to the AML Act: Section 8 (3).

Reference to the 4th Money Laundering Directive: Article 8 (4), letter a.

Regarding the requirements for a Compliance Officer, refer to:
Executive Order no. 1026 of 30 June 2016 on the management and governance of banks, etc. and Executive Order no. 1723 of 16 December 2015 on the management and governance of insurance companies, etc.

If an undertaking is compelled to have a compliance function by other legislation, it shall appoint a Compliance Officer at management level.

The purpose of the requirement for a Compliance Officer is solely to determine that for financial undertakings already subject to a requirement to have a Compliance Officer from other legislation, that person's function will also include requirements under anti-money laundering legislation.

The requirement applies to the following undertakings, which according to other legislation must have a compliance function:

a) Banks.
b) Mortgage credit institutions.
c) Stockbroker companies.
d) Life insurance companies and multi-employer occupational pension funds.
e) Savings banks.
f) Providers of payment services and issuers of electronic money, cf. Annex 1, nos. 1-7, of the Payments Act.
g) Insurance brokers, when they provide life insurance or other investment-related insurance.

Subsidiaries of foreign undertakings are not covered by the requirement.

The Compliance Officer must work independently. The Compliance Officer shall check and determine that the undertaking complies with the AML Act and rules issued pursuant thereto. This means that the person must check and assess whether the undertaking's business procedures and methods for combatting money laundering and terrorist financing are appropriate and effective, and that the undertaking notifies the MLS, cf. Section 26 (1) of the Act. In addition, the Compliance Officer shall check and assess whether the measures taken to remedy any deficiencies are effective.

The Compliance Officer shall ensure that controls performed by the undertaking are sufficient as part of the undertaking's internal controls. See Section 4.3.3. on internal controls.

Due to independence from the general management, the Compliance Officer can also handle employee reports of violations or potential violations (whistleblower scheme) pursuant to Section 35 (1) and Section 36 a (1) and (2) of the Act. See Section 29 on whistleblower schemes.

6.4. Responsible Executive Board member

Reference to the AML Act: Section 8 (5). Reference to the 4th Money Laundering Directive: Article 46 (4).

When deemed relevant, undertakings must appoint a member of the Executive Board responsible for implementation of the requirements in the AML Act and rules issued pursuant thereto.

This means that undertakings with no Executive Board are not obliged to appoint a person in accordance with the provision. The provision is therefore not intended to introduce a requirement that undertakings must make organisational changes.

The organisation and operation of undertakings is performed by the Executive Board in undertakings that have one. The requirement to appoint a responsible member of the Executive Board must therefore ensure that the intention and purpose of the provision are anchored at management level.

There is not requirement that undertakings with no Executive Board (e.g. if personally-owned) have to appoint a person an Executive Board member.

The responsible member of the Executive Board has a special duty to ensure that the undertaking complies with the rules of the AML Act. Their job is to ensure anchoring at management level and management focus on preventive measures against money laundering and terrorist financing. This does not relieve the rest of the general management of responsibility.

The responsible member of the Executive Board can fulfil the duty by e.g. regularly holding meetings with the AML and Compliance Officers, to ascertain the status of the undertaking's compliance with the rules of the AML Act and the implementation of new rules within the area of money laundering. If the undertaking is deficient in relation complying with money laundering legislation, the responsible member of the Executive Board must ensure that such deficiencies are corrected.

In smaller undertakings, the person appointed according to this provision can be the same as the AML Officer, cf. Section 7 (2), or the Compliance Officer in Section 8 (3).

Subsidiaries of foreign undertakings in Denmark
Subsidiaries of foreign undertakings in Denmark do not need to appoint a person in pursuance of Section 8 (5) of the AML Act.

Subsidiaries of Danish undertakings abroad
If a Danish undertaking has subsidiaries abroad, it must be aware that the responsible member of the Executive Board is also responsible for those subsidiaries.

6.5. Internal audits

Reference to the AML Act: Section 8 (4).

Reference to the 4th Money Laundering Directive: Article 8 (4), letter b.

Regarding the requirements to internal audit, refer to:
Executive Order no. 1912 of 22 December 2015 on the implementation of audits in financial undertakings, etc. and financial groups.

If an undertaking has an internal auditor, the Board of Directors must ensure that the audit assesses whether the undertaking's policies, business procedures and controls in the area of money laundering are organised and function satisfactorily.

The purpose of the requirement for an internal auditor is solely to determine that financial undertakings already compelled to have an independent auditor also perform audits in compliance with the requirements of the AML Act and rules issued pursuant thereto. This means that the job description for the internal auditor must contain provisions that an internal audit must ensure the undertaking's compliance with written policies, business procedures and controls in the field of money laundering and terrorist financing.

The requirement applies to the following undertakings if they have an internal auditor:

1) Banks.
2) Mortgage credit institutions.
3) Stockbroker companies.
4) Life insurance companies and multi-employer occupational pension funds.
5) Savings banks.
6) Providers of payment services and issuers of electronic money, cf. Annex 1, nos. 1-7, of the Payments Act.
7) Insurance brokers, when they provide life insurance or other investment-related insurance.

7. Education

Reference to the AML Act: Section 8 (6).

Reference to the 4th Money Laundering Directive: Article 46 (1).

Regarding the requirements for a basic course for board members, refer to:
Executive Order no. 1424 of 29 November 2016 on a basic course for members of the Board of Directors in banks, mortgage credit institutions and insurance companies.

Pursuant to the provision in Section 8 (6), undertakings shall ensure that employees, including management, have received adequate training in the requirements of the AML Act. To fulfil the requirement, the

person appointed must be actually involved in the undertaking's work with prevention of money laundering and terrorist financing. The requirement applies to the undertaking's Executive Board and senior management.

According to other legislation, board members of a bank, mortgage-credit institution or insurance company shall undertake a basic course on prevention of money laundering amongst other things, see the Executive Order on a basic course for members of the Board of Directors in banks, mortgage credit institutions and insurance companies.

The undertaking is not obliged to train employees who perform functions not related to money laundering or terrorist financing.

The undertaking is required to have a adequate training programme. The undertaking's business procedures and controls must also ensure that training is given to employees who deal with customers.

Providing and reviewing the undertaking's written policies and business procedures with the employees is not sufficient. Neither will training that solely focuses on the requirements of the law be sufficient, but is not related to, e.g. the undertaking's business model, including its product range, customer types etc.

The undertaking can opt to only give individual employees training within their relevant areas of work. Such training must ensure that the employees have satisfactory understanding of the requirements there are within the area of money laundering and terrorist financing, and what significance the requirements have for the job of the individual employee. The employee must be able to perform his/her job fully satisfactorily and ensure that the undertaking complies with the requirements of the Act.

The undertaking must ensure that the employees take part in the training.

Training in certain special business areas must be adapted to the special functions of the employees, including highlighting the indicators of money laundering and terrorist financing that can be expected to occur in the various areas. Such special areas can include securities trading, import/export financing and cross-border correspondent relationships.

The undertaking's employees must also receive training in relevant provisions and data protection, to ensure that personal data is processed in accordance with data protection legislation. This will help ensure that according to the provisions of the AML Act, personal data can only be obtained with a view to complying with the requirements of the Act.

The requirement on sufficient training implies that the undertaking must train its employees and management at appropriate intervals. When updating its business procedures, the undertaking shall train its personnel when relevant to their work.

Part 3 – KYC procedures

It is a basic principle of anti-money laundering legislation that the undertaking must know its customers. The rules on KYC procedures are found in Chapter 3, Sections 10-21 of the AML Act.

The purpose of KYC procedures is to prevent money laundering and terrorist financing by undertakings knowing who their customers are, and what their purpose is with the business relationship or a single transaction.

KYC procedures are mandatory and apply continuously throughout the customer relationship. That means that details on the customer have to be updated at appropriate intervals based on risk assessment. See Section 8.3 on KYC procedures at appropriate intervals. The undertaking must be able to document the details it obtains in pursuance of Chapter 3 of the AML Act.

When transferring a customer portfolio, the buyer has a duty to ensure that the risk assessment, risk management and KYC procedures, etc. meet the requirements of the AML Act. It is not a requirement that the buyer carries out renewed KYC procedures on the entire customer portfolio at the time of the transfer, but the buyer is responsible from the time of transfer to fulfil the requirements of the AML Act, including updating information on the transferred customer portfolio. In the event of a merger of one or more undertakings, it will also be the new or continuing company that is responsible for complying with the requirements of the AML Act. When a business transfer takes place, in the form of a transfer of the shares in an undertaking subject to the AML Act, the undertaking transferred will continue to be subject to the AML Act, while the transferee of the shares will not have a direct responsibility for the undertaking fulfilling the Act's requirements for KYC procedures.

What is a customer?
A "customer" includes natural and legal persons (including companies, associations and public authorities).

A customer relationship arises when the undertaking either establishes a business connection with a customer or performs a single transaction for a customer. This can include, for example, the undertaking entering into an agreement with the natural or legal person, e.g. the opening of an account (lending, borrowing, leasing etc.), depositing, transfer of funds, currency exchange, purchase or sales of securities, advisory services, brokerage, e.g. sale of property etc., or an agreement to draw up accounts or perform auditing.

The customer is a natural or legal person the undertaking enters into a contractual relationship with, or on whose behalf the undertaking performs a transaction or activity.

The AML Act's customer concept only includes the undertaking's own customers and thus not the customer's customers. Similarly, the Act's business relationship concept only covers the undertaking's own business relationships, and not the business relationships of its own business relationships. KYC procedures do not therefore have to be carried out in relation to customers' customers or business associates' business associates, and transaction monitoring need only include the funds that are transferred/received via the customer's account.

Examples of customer relationships

1) In the case of guardianship and joint custody, the guardian is the person who acts on behalf of the customer. The customer is the minor or the person under guardianship or joint custody.

2) The child is the customer for child's savings accounts. The person opening the child's savings account acts on behalf of the customer.

3) A lessee is the leasing company's customer. The dealer from whom a leasing company buys equipment and/or sells the equipment to at the end of the leasing agreement, is not classed as a customer according to the AML Act.

4) A guarantor for a liability, e.g. a loan taken out with a bank or mortgage credit institution, will be regarded as a customers when the loan is taken out, as the guarantor is party to an agreement with the bank/mortgage credit institution, establishing a business relationship. In such a situation, the debtor and the guarantor are both regarded as customers.

5) In the event of third party collateral, specific assessment of each aspect has to be considered if a business relationship is established. If an account is opened in connection with third party collateral, a business relationship will always have been established.

6) The customer for life insurance and pensions is always the natural or legal person the company has contracted with (the policyholder), and who owns the insurance policy. For job market and company pensions, when independent policies are issued, it is the employee who has to be identified and checked as the customer. For group insurance schemes, when independent policies are not issued, it is the employer/association who has to be identified and checked as the customer. When life insurance companies make or sell an investment, a customer relationship is not established. This is due to the fact that life insurance companies only establish customer relationships as defined by the AML Act with the natural and legal persons with whom the company enters into an agreement, and who are the holders of an insurance policy.

7) An auditor can obtain help from a third party (e.g. another auditor or a tax advisor) to undertake work for a customer. In principle, the third party will be regarded as a subcontractor to the auditor. However, the specific circumstances can mean that the third party enters into a contractual relationship with the auditor's customer. For example: this will be the case when an auditor gives declarations. Who is the third party's customer therefore depends on specific evaluation of with whom the customer relationship has been entered into, the scope and duration of the work, with whom contact was made and to whom the service will be invoiced.

8) A real estate agent (sales broker) who sells a property will regard both buyer and seller as customers. If the buyer is represented by another real estate agent, an auditor, lawyer or other persons providing the same services, cf. Section 1 (1), no. 17 of the AML Act, the buyer will not be regarded as a customer for a sales broker.

9) A buyer broker, regardless of whether registered as a real estate agent, who buys a property will regard both buyer and seller as customers. If the seller is represented by a real estate agent, auditor, lawyer or other persons offering the same services, cf. Section 1 (1), no. 17, the seller alone will be considered to have entered into a business relationship with the seller.

10) A lawyer's customers/business associations are its clients, and a client relationship must be regarded as established when the lawyer undertakes to represent the client. In many instances, a client relationship is established during the first meeting with the client.

11) In securities trading,5 the customer is the natural or legal person with whom the undertaking enters into an agreement for the purchase or sale of securities.

12) The following examples of defining the customer concept can be used especially in securities trading:
    a) A counterpart, to whom a securities trader6 makes contact with regard to undertaking the customer's orders, is not a customer of the securities trader.
    b) A securities trader who contacts an undertaking is that undertaking's customer. The securities trader's customers are not the undertaking's customers.
    c) If a customer has a deposit and/or current account with an undertaking, the customer is still a customer of that undertaking due to the deposit and/or current account, even though the customer may have made contact through a securities trader, e.g. through a portfolio management agreement with the securities trader.
    d) Counterparties that an undertaking deals with via a marketplace as defined in Directive 2014/65/EU (MiFID II) or a marketplace located in a third country that is subject to a decision on equivalence taken by the European Commission or another relevant authority, are not customers.
    e) Counterparties with which an undertaking enters into bilateral securities trading are not customers, if it is an agreed condition that clearing takes place via one of the following entities:
        i. A central counterparty (CCP) which has been authorised as a CCP by a competent authority of a Member State in accordance with Chapter 1, Section III of Regulation (EU) no. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (as amended).
        ii. A central counterparty CCP located in a third country recognised by ESMA pursuant to Article 25 of Regulation (EU) no. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, CCPs and trade repositories (as amended).
    f) A person who owns securities issued by an undertaking is not that undertaking's customer.

13) In the case of payment initiation services, the contractual relationship between the provider of the payment initiation service and the individual internet business/webshop consists of the provider's delivery of and the internet business/webshop's integration of the payment solution for use in the online shopping of the internet business/webshop's customer. The payment initiation service's business relationship is thus the internet business/webshop, while the internet business/webshop's customer is not a business relationship in relation to the payment initiation service.

5 In this guide, the term "securities trading" covers trading in financial instruments as defined in the Capital Markets Act and in Annex 5 to the Financial Business Act.
6 In this guide, the concept of "securities trading" includes the definition pursuant to the Financial Business Act and undertakings with a similar license from an EU country or under similar supervision in a third country.

8. When should an undertaking conduct KYC procedures?

Section 10 of the AML Act describes when an undertaking must conduct KYC procedures:

1) When establishing a business relationship.
2) When the relevant circumstances of a customer change.
3) At appropriate times, including when the undertaking or person during the relevant calendar year is legally obliged to contact the customer, to investigate any relevant information regarding the beneficial owner or owners.
4) In the event of individual transactions over a certain value.
5) For the provision of games, when the stake or payout exceeds a certain amount.
6) In the event of a suspicion of money laundering or terrorist financing.
7) In the event of doubt concerning previously obtained details on the customer.

The following section describes the above situations in more detail.

8.1. Establishing a business relationship

Reference to the AML Act: Section 10 (1), no. 1. Reference to the 4th Money Laundering Directive: Article 11, letter a.

In principle, an undertaking establishes a business connection when it provides a service or sells a product to a customer. For customer relationships where no business relationship has been established. See Section 8.4 on individual transactions.

When an undertaking establishes a customer relationship, when it can be expected at that point that the customer relationship will be of a certain duration, a business relationship is established. Therefore, a business relationship will be established if the undertaking believes that the customer will make use of the undertaking's services repeatedly, and will thus be a regularly-returning customer.

A business relationship will always be established if a customer opens an account or the like with the undertaking, e.g. for depositing funds, lending, leasing or sales of property.

Accounts cannot be opened anonymously or under a false name, and therefor it is a requirement that KYC procedures are always performed when establishing a business relationship.

8.2. The relevant circumstances of a customer change

If the business relationship is established, and the customer's relevant circumstances, change, KYC procedures must be performed again.

The undertaking must react if it becomes aware of changes in the customer relationship, e.g. a considerable increase in the customer's commitments and/or changes in its business.

In such situations, the undertaking must use risk assessment to determine whether new information about the customer needs to be obtained, including, for example, obtaining and verifying new identification details.

If the customer is a legal person, the undertaking must use risk assessment to determine whether new information about the beneficial owners needs to be obtained. If the undertaking has new beneficial owners, the undertaking must identify and take reasonable measures to check the new beneficial owners. It will also often be necessary to identify the new owner and control structure for the customer in question.

Examples of when the relevant circumstances of a customer change:

1) If a customer's purpose or intended nature of the business relationship changes significantly, e.g. because the customer begins to make much larger transactions than previously. See Section 9.7 on the purpose and intended nature of the business relationship.
2) If a customer is classed as a PEP.
3) If a customer moves to/from Denmark, or relocates its place of business to/from Denmark, especially to/from a high risk country.
4) If a customer's owner and control structure change, e.g. due to a reconstruction or because the undertaking's authorisation to undertake certain activities is revoked.

The undertaking must conduct KYC procedures when it becomes aware that the customer's relevant circumstances have changed. These can be part of the undertaking's monitoring, regular KYC procedures or if the undertaking can otherwise obtain definite knowledge about the customer. See Section 9.8 on regular monitoring of the business relationship.

8.3. KYC procedures at appropriate times

When a business relationship is established, the undertaking must perform its KYC procedures at appropriate intervals during the customer relationship. The requirement to conduct KYC procedures also applies when the undertaking or person during the relevant calendar year is legally obliged to contact the customer, to investigate any relevant information regarding the beneficial owner or owners. The purpose is to ensure that the details the undertaking has on an existing customer are correct and sufficient. The undertaking must therefore, in addition to performing KYC procedures if the customer's relevant circumstances change, also ensure that they are performed at fixed intervals and when the undertaking is legally obliged to contact the customer.

"Legally required" is defined as an undertaking being required to contact a customer in order to investigate any relevant information regarding the beneficial owner(s). Such an obligation can exist for example, in accordance with the Directive on administrative cooperation in the field of taxation7, in particular the CRS rules and including the FATCA rules.

If an undertaking is obliged to contact the customer, it must also check whether any relevant details concerning the beneficial owner or owners is still correct.

7 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation, as amended by Council Directive 2014/107/EU.

An example could be when an undertaking is obliged to fulfil due diligence requirements under the CRS rules, and becomes aware of new relevant information regarding a person's status. In this instance, the undertaking will be obliged to contact the customer in order to obtain a new self-declaration or proof document, and will also be obliged to examine any relevant details concerning the beneficial owner or owners.

Another example may be when a trustee of a trust pursuant to the Section 46 a (5) of the AML Act, conducts its annual investigation of whether there have been changes in the registered details about the customer's (the trust's) beneficial owners, and finds that it is necessary to contact one or more members of the trust, including e.g. the founder of the trust or other trustees.

The requirement for performing KYC procedures at appropriate intervals must be based on risk assessment. That means that the undertaking must determine the interval based on risk assessment of the customer relationship. The undertaking can group customers into different categories, e.g. customers with limited risk, and customers with increased risk, and can set one interval for the former and another for the latter. However, the undertaking cannot decide that KYC procedures do not need to be performed.

As such, the intention is that the undertaking focuses on customer relationships with increased risks, while customer relationships with limited risk do not need the same extensive and frequent procedures.

There is no mandatory method determines as to how the undertaking must perform its KYC procedures at appropriate intervals. The KYC procedures can therefore be performed by an automated and/or manual process, for example. But this must be based on a risk-based approach.

If a customer relationship with a legal person is involved, it can e.g. be relevant to check whether the customer has beneficial owners at appropriate intervals, in the event of limited risks.

8.4. Individual transactions

Reference to the AML Act: Section 10 (1), no. 2.

Reference to the 4th Money Laundering Directive: Article 11 (1), letter b.

Other legislation: Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying funds transfer and repealing Regulation (EC) No 1781/2006.

The principle is that an undertaking establishes a business relationship when it performs transactions for a customer, and thereby has to conduct KYC procedures. However, the undertaking can perform individual transactions for customers that do not use the undertaking regularly.

In its KYC procedures, the undertaking must ensure that it is able to determine when a customer goes from being a customer for which the undertaking performs individual transactions, to become a business relationship. The undertaking can therefore lay down a series of criteria to determine whether a business relationship exists or not. Such criteria could include:

1) The number of times the customer uses the undertaking.

2) The periods between two transactions.
3) The number of transactions

When individual transactions are involved, the undertaking must conduct KYC procedures when it executes transactions for a customer of at least EUR 15,000.

Other limits apply to money transfers and currency exchange. KYC procedures must be conducted for money transfers when the undertaking executes an individual transaction of more than EUR 1,000, and the procedures must be conducted when a currency exchange transaction is EUR 500 or more.

If the size of the transaction is not known in advance, KYC procedures must be conducted as soon as the undertaking suspects that the transaction or transactions will amount to EUR 15,000 or EUR 1,000 or EUR 500 respectively.

The above limits apply regardless of whether the transaction is carried out as one or as several transactions which are or appear to be interrelated.

Examples of interrelated transactions:

1) A customer asks for EUR 800 and 900 respectively to be transferred, thus exceeding the limit of EUR 1,000.
2) A customer returns several times the same day or the day after, and performs the same type of transaction.
3) A customer person comes several days in a row and exchanges amounts corresponding in total to EUR 500 or more.

An individual transaction is involved when a business relationship has not been established. There is no individual transaction if a business relationship is established due to other services, e.g. opening an account, advisory services or the like.

Frequently returning customers of e.g. currency exchange companies and money transfer companies should be regarded as business relationships. When a customer that makes repeated individual transactions should be regarded as an established business relationship requires specific assessment, and KYC procedures therefore have to be conducted. It will depend on such factors as how often the customer makes a transaction, and the length of time between individual transactions. See Section 8.1. on establishing a business relationship.

If there is any suspicion of money laundering or terrorist financing, KYC procedures must always be conducted. See Section 8.6 on suspected money laundering and terrorist financing.

The undertaking must be aware that it must observe the requirements in the Money Transfer Regulation for money transfers concerning details on the payer and payee. This requirement applies even though the undertaking is not obliged to conduct KYC procedures according to the requirements in the AML Act.

See Section 8.8. on individual activities that are not transactions.

8.5. The provision of games, when the stake or payout exceeds a certain amount

Reference to the AML Act: Section 10 (1), no. 3. Reference to the 4th Money Laundering Directive: Article 11, letter d.

A provider of games is defined as a legal or natural person established in this country providing games commercially. All providers of games that are covered by the Gambling Act are considered to conduct commercial activities.

Only providers of games established in Denmark are covered by the AML Act. Providers of games with a Danish authorisation to provide games are regarded as established in this country and are thus also covered by the Act.8

Individual dealers of games in shops, kiosks, etc., who sell a game in the name of the provider of games are not covered by the scope of the Act. This implies that it is the provider of game's responsibility to ensure that a dealer conducts KYC procedures if not already done when establishing the business relationship. In such cases, the dealer must conduct KYC procedures if the player places a bet or is paid a win or both of at least EUR 2,000, whether the transaction is individual or several transactions that appear to be interrelated.

The undertaking can decide itself which part of the process triggers conducting KYC procedures.

If several transactions are interrelated, assessment can be made based on the individual dealer and within a period of 24 hours. As a general rule, several transactions in connection with an undertaking's sale of bets within one day by the same dealer will be regarded as interrelated. For example: a customer walking in and out of the same store several times in a day, making several transactions, will be regarded as interrelated transactions. The same is true if the customer splits a transaction up during the same visit.

Note that the definition of interrelated prohibited transactions in land-based betting cannot be applied to online gambling, as the amount of data available and general opportunities to follow the player are far greater.

The undertaking must always be aware of whether a business relationship is established, e.g. by setting up a loyalty card or schemes in which winnings are transferred to a bank account. For online games, a business relationship is entered into from the beginning of the customer relationship, as a gaming account is established before playing starts. See Section 8.1. on establishing a business relationship.

For further information about games, please refer to the Danish Gaming Authority's subject-specific money laundering instructions9.

8 This is stated in FT 2016-17 L41 Report on the Bill on Preventive Measures against Money Laundering and Terrorist Financing (AML Act) submitted by the Business, Growth and Export Committee on 30 May 2017, pages 9-10.

9 www.spillemyndigheden.dk/uploads/2020-01/Version%201.1%20Spillemyndighedens%20vejledning%20om%20forebyggende%20foranstaltninger%20mod%20hvidvask%20af%20udbytte%20og%20finansiering%20af%20terrorisme.pdf

8.6. Suspicion of money laundering or terrorist financing

Reference to the AML Act: Section 10 (1), no. 4.

Reference to the 4th Money Laundering Directive: Article 11 (1), letter e.

The undertaking must always conduct KYC procedures when it becomes aware of or suspects money laundering or terrorist financing. The requirement applies even if only an individual transaction is involved under a certain amount. See Section 8.4 on individual transactions, or provision of a game for which the stakes or payout are under EUR 2,000. See Section 8.5 on the provision of games when the stakes or payouts exceed a certain amount.

There can be situations involving suspicion when it is not possible to conduct KYC procedures, e.g. if the customer refuses to give such details, or leaves the premises when asked for them. In such instances, the undertaking must inform the MLS, providing the details it has.

8.7. Previously obtained details on the customer

Reference to the AML Act: Section 10 (1), no. 5.

Reference to the 4th Money Laundering Directive: Article 11 (1), letter f.

Executive Order no. 1376 of 12 December 2019 on reporting discrepancies in details on beneficial owners.

The DBA's guide on beneficial owners.

The undertaking must conduct KYC procedures if there is any doubt as to whether the details obtained about the customer's identity etc. are correct and/or sufficient.

This means that if the undertaking has grounds to believe that the details obtained are not correct and/or sufficient, new KYC procedures must be conducted. The requirement includes that full or partial KYC procedures must be conducted based on risk assessment. It is not therefore just an updating of the customer's identity details. The undertaking must make a specific assessment which details need to be obtained.

The undertaking should decide whether the details are insufficient or incorrect. The need for and scope of the additional KYC procedures to be performed in the same instance can be based on the specific conditions, for example:

1) If the undertaking is in doubt as to whether any specific details are insufficient, it can decide that only parts of the KYC procedures are necessary to repeat.
2) If the undertaking is in doubt as to whether the details obtained are correct, it can decide that the full KYC procedures must be repeated.

In the event of insufficient details, supplementary details on the customer in questions will often be missing. An example of when the details obtained are insufficient can be when the undertaking becomes

aware of details on the customer that cause the customer's risk profile to be increased, or that the purpose and intended nature change.

In instances when it transpires that some of the details are incorrect, it may often be necessary for the undertaking to verify all the details again to ensure that they are all correct. But this will depend on which type of details are incorrect. If, for example, the customer has given an incorrect house number by mistake, it will not necessary mean that the full KYC procedures have to be repeated. If, for example, the undertaking is in doubt as to whether the incorrect details were given deliberately by the customer, the full KYC procedures must be repeated. See Section 13, on risk assessment – KYC procedures.

If an undertaking in connection with its customer knowledge becomes aware that details on a customer's beneficial owners do not match those registered in the DBA's IT system, the undertaking must report this to the DBA as soon as possible. If the customer has the discrepancy corrected as soon as possible, the undertaking will not have to report the discrepancy to the DBA.

8.8. Individual activities that are not transactions (advisory services)

Reference to the AML Act: Section 13. Reference to the 4th Money Laundering Directive: Article 2 (3).

If an undertaking performs an individual activity that is not a transaction, the requirements in Section 11 of the AML Act on obtaining and verifying identification details on the customer can be waived on the background of a risk assessment.

An example of an individual activity is the provision of advice when there is no immediate or future prospect of the customer returning with further assignments, for example tax advice of a general nature or individual general advice pertaining to investments that does not take the customer's specific income and asset circumstances into consideration. In such cases, a business relationship will not be established. Assessment can therefore be performed on the basis of whether the activity is of a general nature, or whether the undertaking needs to relate to the customer's specific details to perform the activity, including the customer's earnings and assets. The important thing is that no business relationship is or will be established in that specific situation..

The undertaking should then be able to prove that this specific case involved an individual activity, and that a risk assessment of the specific customer led to the KYC procedures being omitted.

The formation of a company for a customer, or sale of a shelf company cannot be considered to be an individual activity, even if the customer relationship must be anticipated to be short-term. The execution of such activities for a customer will therefore be the establishment of a business relationship.

If there is any suspicion of money laundering or terrorist financing, KYC procedures must always be conducted. See Section 8.6 on suspected money laundering and terrorist financing.

9. Content of KYC procedures

Section 11 of the AML Act stipulates the general requirements for KYC procedures.

KYC procedures are mandatory throughout a business relationship with the customer and must be performed based on risk assessment of the customer relationship. Undertakings must therefore identify relevant risk factors and changes to the same in the individual customer relationship to assess the scope of the KYC procedures to be conducted.

The requirements in Section 11 stipulate that the undertaking shall

1) obtain identity details on the customer, and
2) verify the identity details obtained via an independent and reliable source.

9.1. Obtaining identity details

Reference to the AML Act: Section 11 (1) and (4) Reference to the 4th Money Laundering Directive: Article 13. Reference to the 5th Money Laundering Directive: Article 1 (1), no. 8.

Undertakings must always obtain identity details on the customer.

Identity details can be obtained, for example, through general customer contact, e.g. from personal meetings with the customer, written correspondence between the customer and the undertaking, telephone calls or via the undertaking's IT systems, including e.g. video contact via a sufficiently secure line, or via e.g. online banking.

Identity information, in the form of the customer's name, can also be obtained through NemID based on a specific assessment. In such instances, the undertaking will not also be able to use NemID as a control source, and the undertaking will therefore have to check the identity details via a source other than NemID. Refer to Section 9.2 below.

Natural persons
If the customer is a natural person, their name and CPR number must be obtained.

If the customer in question does not have a CPR number, similar identity details must be obtained, such as a national ID number for foreigners. When the customer does not have a CPR number or similar, identity details must include date of birth.

For persons who are not resident in Denmark, an alternative to the CPR number could be a similar national ID number or details on date of birth. If the undertaking uses a customer's national ID number, it is essential to ensure that it is a unique number, that the number is permanent (e.g. a permanent social security number), or at least the customer's active national ID number (e.g. a passport number), as in some countries it is possible to get a new national ID number.

It is important that the undertaking ensures that the ID number is actually active/valid, e.g. that the passport has not expired at the time of identification, which will be the time when the customer relationship is established.

Date of birth only can only be used in the relatively rare cases when there is otherwise no unique ID number.

The identity details obtained, including the date of birth, must give the undertaking assurance that the customer is who he or she claims to be.

In principle, it will be the customer who provides identity details. It is therefore insufficient in many cases for the customer to only provide their CPR number, and the undertaking then obtains a name from the Central Office of Civil Registration. In instances related to an extremely low risk, it can be sufficient if identity details on the customer can be obtained from the customer's employer, e.g. for job market pensions.

The undertaking must obtain the customer's full name to ensure that verification of the customer being who he or she claims to be is effective. But in some instances, the undertaking can perform risk assessment in relation to the procedure it used when obtaining identity details from the customer.

The principle is that the name and CPR number given by the customer must match the source of control, such as a driver's licence or passport. In the event of obvious typographic errors, the undertaking can, however, accept the details obtained from the customer. If parts of the customer's full name are missing, e.g. one of the customer's first names, the undertaking must obtain the identity details from the customer again. In practice, this could happen if the undertaking does not physically meet the customer when establishing the customer relationship, and the customer fills out a form with identity details, which are then verified by the undertaking in the CPR register. If, for example, the customer has given two out of four first names, the undertaking must obtain the full name from the customer.

If, for example, the undertaking obtains the identity details via a form, and uses two control sources provided together by the customer, it can determine whether the customer has provided his/her full name for the two control sources, and that there is no doubt that the customer is who he/she claims to be. An example of two control sources can, as mentioned, be driver's licence and passport.

When establishing a business relationship to a customer, the undertaking must register the customer's full name.

The undertaking must always be able to demonstrate to the authority which supervises its compliance with the AML Act that knowledge of the customer is sufficient.

Legal persons
If the customer is a legal person, their name and CVR number must be obtained.

If the customer in question does not have a CVR number, similar identity details must be obtained. For foreign undertakings, other forms of identification details can be a registration number, e.g. TIN number (Tax Identification Number), LEI code (Legal Entity Identifier) or another unique registration number.

If the customer has no CVR number or similar, it is a requirement that the undertaking at least has details of the customer's legal status (form of incorporation), e.g. if a limited liability company, a foundation, trust or other.

9.2. Verifying identity details

Reference to the AML Act: Section 11 (1), no. 2 and (4).

Reference to the 4th Money Laundering Directive: Article 13 (1), letter a.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 8, letter a.

For electronic identification and relevant trust services, refer to:
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).

The identity details the undertaking has obtained on a customer must be verified on the basis of documents, data or details obtained from a reliable and independent source. This means that verification of the customer's identity must be done through a source other than the customer.

The reliable source can be a public authority, but it can also be another reliable external source. It is also important that the source is current. This is especially relevant in relation to physical ID documents, when the undertaking must check that the document is still valid.

Electronic identification means can be used in connection with KYC procedures. A reliable and independent source can include electronic means of identification, relevant trust services or any other secure form of remote identification process or electronic identification process that is regulated, recognised, approved or accepted by the competent national authorities.

It is relevant to ensure that the document used for verification is valid, as the person's identity details can have changed, e.g. details of nationality, change of unique ID number, etc.

Using risk assessment, the undertaking must determine whether the identity details ought to be updated at a later date, including whether proof of identity should be obtained again, because previous proof of identity has expired in the meantime.

The undertaking must obtain a new identification document if there is any doubt about the document's authenticity.

The extent of documentation, data or information providing adequate verification of a customer's identity details is a specific evaluation. But there can be no reason to doubt that the customer is the person that they claim to be. In this connection, the undertaking must risk assess its customers, which can mean that enhanced KYC procedures must be conducted.

If the undertaking believes that there is increased risk concerning the business relationship, it should take further action, regardless of whether the customer's identity details have been verified. The undertaking can request additional documents from the customer, consult external sources or require that the first payment be made from a bank account in the customer's name, etc. The undertaking must thus determine which procedures it will use to ensure that there is no doubt that the customer is the person he/she claims to be. See Section 14 on enhanced KYC procedures.

9.3. Examples of verification of a reliable and independent source

Verification of a reliable and independent source can include a search of a reliable and independent register or database or document issued by a public authority.

The principle is that the undertaking must be presented with original, physical identification documents, when the customer is physically present. If the customer is physically present, he/she should, in principle, also be able to present identification documents, and not just copies of the same.

Natural persons

Verification for natural persons can consist of e.g. a search in the CPR (Central Office of Civil Registration), details from the Danish Tax Agency, identification documents issued by a public authority, such as passport, driver's licence, NemID, ID card, health insurance card or birth certificate.

It is not a requirement that the customer presents photographic identification. In situations when the customer physically comes to the undertaking, verification in the form of photo identification (e.g. passport or driver's licence) will provide increased assurance that the customer is the person he or she claims to be. This will be particularly relevant in instances of high risk.

Legal persons

Verification for legal persons can consist of e.g. a search in the CVR (Central Business Register), details from the Danish Tax Agency, or a copy of the certificate of incorporation and articles of association.

If the customer is established outside Denmark, similar details from corresponding public authorities or registers can be used to verify the legal person's identity details.

For legal persons without a CVR number, e.g. certain associations, verification can be performed by obtaining a copy of the deed of foundation and articles of association if available, supplemented by details on the persons who can act on behalf of the association. A deed of foundation can, for example, be a copy of the minutes from the founding general meeting. Details on who can act on behalf of the association will typically be provided in the articles of association, e.g. the Chair and Treasurer together, and their names will typically be stated in the minutes of the association's last general meeting.

There are many different types of associations, including stakeholder organisations and voluntary societies. Such associations cover a broad spectrum, including in relation to risk, and the undertaking should therefore take this into account in its KYC procedures. On the basis of a risk assessment, the undertaking must determine which details it needs. For example: the undertaking can assess individual associations based on a number of factors, such as the association's purposes, including its members, whether the association is a member of a recognised umbrella association, whether the association is an approved public information association, and obtain publicly available information on the association, and how the association is financed.

When the customer is a legal person, the undertaking should be aware of the requirement for verification of the identity of the beneficial owners. See Section 9.6 on beneficial owners.

Practical examples:
Notwithstanding the examples below, specific assessment in each customer relationship is required as to what details must be obtained from the customer, and when they have been sufficiently verified from independent and reliable sources. However, the undertaking must always obtain a name and, in principle, a CPR number or similar if the person in question does not have a CPR number. See Section 9.6.2 for more details.

An example of a process for how details can be obtained, and how verification of a physical person can be performed based on risk assessment, and when verification is performed using two sources:

1) The customer states his/her name and CPR number to the undertaking.
2) The customer presents a driver's licence to the undertaking.
3) The undertaking verifies the name and CPR number by searching the CPR register.
4) The undertaking verifies that the details on the driver's licence match the name and CPR number given by the customer. The undertaking also verifies that the photo on the driver's licence matches the customer's appearance.
5) The undertaking retains documentation of verification of identity details, i.e. in this instance, copies of the driver's licence and audit trail for CPR search.

For some customers, it can be difficult to obtain standard identification documents, such as national insurance cards, passports and driving licences. Examples of this type of customer include foreign workers, foreign students, asylum-seekers, refugees, homeless and minors.

In such instances, the undertaking should adopt an approach to the customer that compensates for the problems the customer has in producing documentation of his/her identity.

In some instances, it can therefore be necessary for an undertaking to use other control sources than the usual. These can be in the form of other sources the customer has, but that the undertaking would not usually use. For example: presentation of a letter from a public authority to the customer, related to a residence permit.

In some instances, it can also be necessary to contact a public authority to ask it to confirm the person's identity.

Foreign workers and students will not always have a CPR number at the start of their stay in Denmark, and persons allocated an administrative ID number, e.g. by the Danish Tax Agency or the Danish Agency for International Recruitment and Integration (SIRI), will not always be registered with an address in the CPR register at the time the bank makes its enquiries. However, some customers may need to set up a Danish bank account to fulfil the conditions for their residence permit, even though they have not yet been registered in the CPR register. This will be the case, for instance, for workers from non-EU countries, when the Aliens Act in some circumstances requires that their wages are paid into an account in Denmark as a condition of their residence permit. In such instances, the undertaking could use the customer's provisional work permit or residence permit containing, for third-country nationals, their assigned administrative identification number as the source of verification of the customer's identity details together with

other sources, such as passport. In the event of doubt about the validity of a residence permit for workers from non-EU countries for example, the undertaking can contact SIRI for confirmation.

9.4. Remote customers

An undertaking has a better chance of ensuring that the customer is who he or she claims to be when physically meeting the customer. When the customer is not physically present (remote relationship), the undertaking must consider the potentially increased risk. Photo identification will not provide the same assurance as a physical meeting, unless the undertaking uses digital systems, for example, that allow the customer to provide photo identification at the same time as the undertaking being able to see the customer via digital systems, e.g. a live video link. This will help provide greater assurance that the customer is the person that they claim to be.

The scope of identity verification for customers who are not physically present also depends on the properties and characteristics of the product or service the business relationship concerns, in relation to the risk of money laundering or terrorist financing. As such, the undertaking must always use risk assessment to determine whether control sources are necessary to ensure that knowledge of the customer is sufficient, including whether more than one source should be used to verify identity details, or risk-mitigating measures. An example of a risk-mitigating measure can be that the undertaking sends a physical letter with a unique code to the customer's registered address, which the customer must then quote to the undertaking, e.g. by phone, or by logging on to the undertaking's website. See Section 9.5 below on use of NemID for further examples of risk-mitigating measures.

9.5. Use of NemID or other form of electronic ID

NemID can be used to verify the customer's identity details when using PID CPR match to verify CPR numbers and public digital signatures (OCES) to verify a name.

NemID is a reliable and independent source, but when more than limited risk is involved, it will be necessary for the undertaking to use other control sources, or risk-mitigating measures along with NemID, to be able to obtain sufficient knowledge of the customer when conducting KYC procedures. In this connection, the undertaking should be aware of the potentially increased risk inherent in customer relationships when not meeting the customer physically. See Section 9.4 above on remote customers.

Undertakings covered by the AML Act can use information obtained, for example, through electronic identification means, relevant trust services under the eIDAS Regulation, or any other secure form of remote identification process or electronic identification process regulated, recognised, approved or accepted by the competent authorities. It follows from the eIDAS Regulation that undertakings and persons are obliged to recognise electronic identification means (eID) from other EU or EEA countries. The types of eID that are to be recognised must be notified to the Commission. They will then be included in the Commission's list of notified eIDs in accordance with Article 9 of the eIDAS Regulation.

The undertaking can only use NemID or other form of electronic ID as the only source of control when it has made a risk assessment of the specific customer relationship, and determined that simplified KYC procedures can be conducted and that sufficient knowledge of the customer can be obtained using NemID or other form of electronic ID. However, the undertaking must be aware that in some specific customer relationships, it may be necessary to obtain other details, e.g. on the business relationship's purpose and intended nature.

If the business relationship with the customer contains products or services where the national risk assessment for money laundering and terrorist financing indicate that high risk products or services are involved, the customer relationship will not represent a limited risk in principle. This means that in such customer relationships, NemID or other form of electronic ID will not be sufficient to ensure the necessary knowledge of the customers.

NemID or other form of electronic ID as a source of control can be supplemented with other sources of control or risk mitigation measures. Such measures could include:

1) The first transaction takes place via the customer's Nemkonto or another bank account registered in the customer's name.
2) The undertaking sends a unique code to a mobile phone number that it has checked belongs to the customer, or by physical letter to the customer's registered address.
3) The undertaking verifies the customer's IP address in relation to geolocation.
4) The undertaking asks the customer questions, which can be subsequently verified by a reliable and independent source, e.g. information from the customer's personal tax folder.

The above examples should not be seen as exhaustive, as there can be several ways an undertaking can use risk-mitigating measures. The undertaking must also be aware that it can make a specific assessment itself of which risk-mitigating measures are sufficient in relation to knowledge of the customer.

The undertaking must be able to demonstrate to the authority which supervises compliance with the AML Act that the undertaking's knowledge of the customer is sufficient in regard to the risk of money laundering and terrorist financing. The undertaking's KYC procedures (and its verification of identity details) must therefore be designed to ensure the undertaking has sufficient knowledge of the customer.

9.6. Beneficial owners

Reference to the AML Act: Section 11 (1), no. 3, Section 2 (1), nos. 1 and 9 and Section 15 a.

Reference to the 4th Money Laundering Directive: Article 13 (1), letter b.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 8, letter b.

Reference to the DBA's guide: Beneficial owners, the guide concerns beneficial owners, including who, what and where must be registered.

The term "beneficial owners" is used in previous anti-money laundering legislation, and is now used in anti-money laundering legislation, and in the rules on registration of beneficial owners. The term has the same basis in the 4th Money Laundering Directive in both legislation versions, and is therefore a common term. The rules on registration of beneficial owners include a requirement that different legal persons etc. must register their beneficial owners in a register. The anti-money laundering legislation has a requirement that undertakings covered by the AML Act must identify and verify the customer's beneficial owners.

Some legal persons etc. are not covered by the requirement on registration of beneficial owners in the rules on registration of beneficial owners, but the exemption does not apply for the requirements of the

AML Act that undertakings must identify and verify the beneficial owners of their customers, as part of their KYC procedures. Undertakings must therefore also identify beneficial owners if, for example, their customer is a voluntary association or cooperative housing association, even if they are not subject to the rules on registration of beneficial owners.

Because the rules on beneficial owners have a common background, an undertaking according to the AML Act that has to identify its customers' beneficial owners can use the DBA's guide on beneficial owners to help interpret the term, and to determine who has to be identified, and to determine the owner and control structure. However, undertakings should be aware that the requirements of the AML Act on what details have to be obtained according to KYC procedures differs from the details to be registered about beneficial owners in the CVR.

As part of its KYC procedures, the undertaking must identify the beneficial owners of its customers.

The undertaking must:

1) obtain identity details on the beneficial owner(s),
2) implement reasonable measures to verify the identity of the beneficial owner(s), and
3) if the customer is a legal person, identify its ownership and control structure.

9.6.1. Definition of beneficial owner

A customer's beneficial owner is the natural person(s) who ultimately own or control the customer, or the natural person(s) on whose behalf a transaction or activity is conducted.

Beneficial owners can be natural persons, and the undertaking must identify the full ownership and structure chain, and determine who ultimately owns or controls the customer.

For example: if a customer is company A, 100% owned by company B, the undertaking must identify the natural person or persons who own and control company B.

When the undertaking has to identify who the customer's beneficial owners are, the undertaking must assess which persons own a sufficient number of shares, voting rights or can control the undertaking in another way. An indicator of what is a sufficient number will, in principle, be that the person owns more than 25% of the shares and/or the control. But it is important to emphasise that the percentage limit is only an indicator for beneficial ownership or control.

The principle is that the customer has beneficial owners, and can identify them. There are however instances when there are no natural persons who own and/or control the customer to a sufficient degree to be defined as beneficial owners. In such instances, the customer's general management will be regarded as the beneficial owner(s) instead. This can be, for example, when a customer is an association that does not have beneficial owners, whereupon it is the general management that must be considered the beneficial owners of the association.

If the undertaking has identified one or more beneficial owners, but there is still doubt as to whether the person or persons identified are actually the beneficial owners, both those persons and the general management must be regarded as the beneficial owners of the customer.

The undertaking must note the measures it has initiated in an attempt to identify the beneficial owners. Notation must be made before the undertaking regards the general management as the customer's beneficial owners.

The undertaking must retain the details it has obtained and used to identify the customer's beneficial owners. For example: if the undertaking has developed a diagram of the "owner chain" from the undertaking's customer and to its beneficial owners, or if the undertaking has identified the customer's ownership and control structure from a printout of the DBA's register of beneficial owners.

In a customer relationship that implies limited risk, the undertaking can also obtain details and notes that the customer has used for the purpose of identifying its beneficial owners. However, the undertaking should evaluate the customer's details and notes before they can be used as part of the undertaking's investigation of the customer.

The requirement on identifying and verifying beneficial owners does not apply to undertakings whose shares are traded on a regulated or corresponding market, when subject to a duty to provide information in accordance with EU law or corresponding international standards that ensure transparency. In situations when the customer's shares are traded on such a regulated market within the EU/EEA or a corresponding market outside the EU/EEA with the same duty to inform as within the EU/EEA, the undertaking does not need to identify and verify the beneficial owners of the customer. When determining a corresponding duty to inform in markets outside the EU/EEA, the requirements for the duty to inform laid down by relevant articles in the Market Abuse Regulation (2014/596/EU), the Transparency Directive (2004/109/EC) and Prospect Directive (2003/71/EC), and any other EU regulations that follow from these relevant articles will be relevant in this connection.

9.6.2. Obtaining identity details

Undertakings must always obtain details on the identity of the beneficial owner(s) (with the exception of the owners of companies listed on the stock exchange).

The requirement to obtain details about the identity of the beneficial owner(s) applies, for example, when the customer is a legal person, such as an undertaking, a foundation, an association or another legal entity. It also applies in connection with a nominee scheme, in which the person on whose behalf the nominee is acting is the beneficial owner.

The undertaking must obtain details that allow it to know with certainty who the beneficial owners are. It depends on a specific assessment how and which details the undertaking must obtain on the customer's beneficial owners, but assessment can never lead to not obtaining any identity details. Regarding identity details of beneficial owners, refer to Section 9.1 of the guidelines on natural persons.

The undertaking must obtain the name and, in principle, CPR number, or other similar details of the beneficial owners, if the person does not have a CPR number.

Regardless of what details the undertaking obtains, date of birth should always be included.

In certain situations, it may be possible to refrain from obtaining the CPR number of the beneficial owners. However, this will only be the case if the undertaking will otherwise be able to obtain equally secure identification of the beneficial owners as it would be if it were informed of the CPR number.

This may be the case, for example, in the case of a publicly known person. "Publicly known" is defined as a person being generally known to the general public at home or abroad. Examples include mayors, owners, directors or board members of large, well-known undertakings, business people, department heads or board directors.

If the beneficial owner or owners are not resident in Denmark and do not have a Danish CPR number, the details must, in principle, contain a unique and permanent or unique and active ID number for the beneficial owner. If the beneficial owner(s) do not have a unique and permanent or unique and active ID number, their date of birth must be included in the details obtained by the undertaking.

In the case of foreign beneficial owners, it will be possible in some cases to refrain from obtaining an ID number, where the undertaking will be able to obtain equally secure identification of the beneficial owner as if the undertaking had requested an ID number. This will be the case, for example, with a publicly known person.

The publicly known beneficial owner in question must be identifiable – and the identity must be verifiable, cf. Section 9.6.3. – by reliable sources, e.g. on the Internet. A reliable source on the Internet can be the website of a public authority or a large undertaking, for example.

The undertaking must ensure it obtains sufficient details to ensure that the beneficial owner is the person the customer has stated. The undertaking must always be able to prove to the authority that supervises its compliance with the AML Act that it has sufficiently identified and verified the details on the beneficial owner, cf. Section 9.6.3. The AML Act's requirement for retaining documentation for KYC procedures performed applies in all cases, even when sources are downloaded from the Internet, for example.

If the undertaking becomes aware of significant changes in the customer relationship, it must decide whether to obtain new details on who the beneficial owners are. "Significant changes" can include the undertaking's business relationship with the customer, e.g. a major expansion of a customer's engagement, or changes in the customer's business, e.g. new management, new business associates or new beneficial owners. If the undertaking becomes aware that a beneficial owner is a politically exposed person, it must assess whether this could have an influence on risk assessment of the customer, including whether the undertaking in this connection must obtain further information about the customer and the beneficial owners. If the undertaking assesses that the customer's risk has been increased, it must always assess whether its information on the beneficial owners is sufficient.

9.6.3. Verifying the identity details of beneficial owners

Verification of identity details obtained must be based on a risk assessment of what reasonable measures are in relation to the particular customer.

The undertaking must thus always obtain identity details, and then perform risk assessment of whether and to what extent they have to be verified. See Section 9.6.2. on obtaining identity details. The undertaking must also obtain a registration certificate or extract of details held in the DBA's IT system when establishing a business relationship with an undertaking or other legal entity, or a trust or similar legal arrangement that are compelled to register details of their beneficial owners with the DBA. "An extract of

details from the DBA's IT system" is defined as the PDF overview that can be downloaded regarding the undertaking in question, on which its beneficial owners appear.

The fact that "reasonable measures" must be taken to verify a beneficial owner's identity details means that the undertaking can e.g. use a risk assessment to deem it sufficient to use details about the beneficial owners provided by the customer, and compare them with the details obtained from the DBA's IT system, a corresponding EU/EEA register of beneficial owners or a corresponding foreign register outside the EU/EEA, such as in the USA, the UK, Canada or Australia. It will be sufficient if the undertaking has determined that the customer relationship constitutes limited risk. In specific cases, the undertaking can also decide that verification can be omitted wholly, or only needs to be performed regarding some of the beneficial owners of a customer. An example is an association with limited risk, when the undertaking uses a risk assessment to specifically choose to only verify the identification information for the board members empowered to bind the association by signature.

The undertaking must always perform verification of the customer's own information. See Section 9.6.2. on verifying identity details.

If the beneficial owner(s) reside in this country, the undertaking's risk assessment may lead to it being deemed sufficient to compare the identity details received from the customer with details in the CPR register or in some other manner, such as via information from the Danish Tax Agency, e.g. annual tax returns.

If the undertaking believes that a customer relationship represents a limited risk, it can use the DBA's register of beneficial owners as a source to verify who the customer's beneficial owners are. It should, however, be noted that the publicly available part of the register of beneficial owners does not contain information on the beneficial owners' CPR numbers. Using the register as a source to verify is therefore only possible in instances with limited risk, when it is believed that this is sufficient as a reasonable measure to verify the beneficial owner. In principle, this will only be in instances when the customer and the product both represent limited risk.

If the undertaking believes that there is an increased risk in the customer relationship, it will not be sufficient to solely verify the identity details provided by the customer in relation to that obtained from the DBA's IT system. It may be necessary in such instances to verify the identity of the beneficial owners using one or more independent sources, e.g. a copy of a publicly-issued identification document. See Section 9.3 on examples of verification from a reliable and independent source.

9.6.4. Clarifying ownership and control structure

When the customer is a legal person (including an association), the undertaking must identify its ownership and control structure. This also applies to non-legal persons if the customer is e.g. a trust or similar legal arrangement. "Ownership and control structure" is defined as meaning that the undertaking obtains details on, e.g. the customer's owners, management, rules for binding the company by signature(s), ownership agreements, share classes or the like. The undertaking must determine itself which details are relevant to clarify a customer's ownership and control structure.

The undertaking's clarification of a customer's ownership and control structure will help determine who are the customer's beneficial owners. The undertaking can therefore often identify the ownership and

control structure first, to understand who it has to identify and perhaps verify as the customer's beneficial owners.

The undertaking must always clarify the customer's full ownership and structure chain, i.e. the undertaking must clarify the entire ownership chain of any legal persons (undertakings) to find the persons who ultimately own or control the customer. Clarifying the ownership and control structure therefore includes any foreign legal or natural owners.

Using risk assessment, the undertaking can decide which investigations it will have to implement to clarify the customer's ownership or control structure. In cases of limited risk therefore, e.g. when the ownership and control structure is transparent, and where no risk factors have been identified based on a specific risk assessment that directly or indirectly relates to the ownership and control structure, it is sufficient for the undertaking to clarify the structure by drawing up a group diagram showing shareholdings. Alternatively, the undertaking can use the information obtained via the CVR (Central Business Register), including about the undertaking's beneficial owners.

In instances of increased risk, it may be necessary for the undertaking to obtain documentation of shareholdings in the form of articles of association, shareholders' register or the like.

However, the undertaking must always clarify the customer's full ownership and structure chain for all business relationships with legal person, but it can then determine the extent of the precautions and controls it needs itself, based on its own risk assessment of the business relationship.

Specific examples of identification of beneficial owners
Below are examples of identification of beneficial owners. How the beneficial owners of a business relationship must be identified in accordance with the AML Act is always a specific assessment that the undertaking must perform when establishing a business relationship. The undertaking must always obtain a name and, in principle, a CPR number or similar at least if the customer's beneficial owners do not have a CPR number.

Publicly-owned
In business relationships when the customer is or is 100%-owned by a public authority (including a municipality, state-owned undertaking, etc.), there will be no natural persons owning or controlling the customer to the extent that can be defined as a beneficial owner. Therefore, the general management should be regarded as the beneficial owner.

If the customer is a government authority, an agency or independent, publicly-owned undertaking, the director will be regarded as the beneficial owner. If the customer is a government ministry, the Secretary of State will be regarded as the beneficial owner.

If, for example, the customer is a limited company that is 100%-owned by a government authority, the general management of the company (the Executive Board) will be regarded as the beneficial owners.

If the customer is a publicly/municipally owned daycare institution or the like, the undertaking should regard the institution's general management as the beneficial owner(s) in accordance with the AML Act.

If, for example, a daycare institution wants to lease a dishwasher, the person in charge and who makes decisions on behalf of the institution will be regarded as the beneficial owner.

If it is the actual municipality that is the customer, a specific assessment is needed to determine who is the general management. In a municipality, it can be the mayor or other natural person with similar authority over that part of the municipality entering into agreement with the undertaking, who will be the person deemed to exercise general management in that specific instance. Municipalities can have different administrative structures, e.g. with multiple mayors or councillors. If, for example, the Child and Youth Administration of the City of Copenhagen decides to build new Scout huts, and is therefore the developer, it can be determined that the Mayor of the Child and Youth Administration will be regarded as the beneficial owner in this specific example.

Voluntary associations, cooperative housing associations, public housing organisations, etc.
When the undertaking has to identify a customer's beneficial owners, it can start with which type of undertaking or other legal entity the customer appears to be. If, for example, the customer is a voluntary association or cooperative housing association, the undertaking can start with how it identifies the beneficial owners in other types of associations, e.g. those associations not covered by the rules on registration of beneficial owners.

In principle, the undertaking has to clarify whether one or more persons own or control the association, in accordance with the definition of beneficial owners. If no one can be identified as beneficial owners, the general management must be regarded as the beneficial owner(s).

In associations, it will often be the Board of Directors or Executive Board (if they have one) that will comprise their general management, and that will therefore be regarded as the beneficial owners. But it will depend on specific risk assessment of each association and their status.

To help identify the beneficial owners, the undertaking can obtain the deed of foundation, articles of association or minutes from the general meeting.

Verification of the details obtained must be based on a risk assessment of what reasonable measures are in relation to the particular customer. Undertakings must be aware here that there are many different types of associations in Denmark. Associations therefore cover a very wide range in relation to risk profile, which is important for the verification measures to be taken.

Based on a specific risk assessment it will not be necessary to verify the identity details provided in some cases with limited risk. Even after a specific assessment, verifying the identity details for the members of an association's board empowered to bind the association by signature may still be justified when the undertaking believes that the association poses a limited risk. Only the members empowered to bind the association by signature can act and sign on behalf of and thereby commit the association. Those members will typically be the Chair and Treasurer, or the Chair/Treasurer and another board member. However, this depends on the specific association's rules on the power to bind by signature. In other instances, when the association does not pose a limited risk, it will be necessary to verify all the identification details for all members of the Board of Directors or Executive Board.

Investment associations

When the customer is an investment association, or a department of an investment association, the undertaking must identify and implement reasonable measures to verify the natural persons who ultimately own and control the legal entity with which the undertaking is establishing a business relationship. In this example, it will be the investment association as the legal person, with a CVR number, even if, for example, a service is only to be provided to single department of the investment association.

If no one owns or controls the investment association to such an extent that they can be defined as the beneficial owners, the association's general management will be regarded as the beneficial owners. Reference can be made to Annex 2 of the DBA's Guide to beneficial owners.

Alternative investment funds (AIFs)
An AIF can be a private equity fund, a property fund or something else, for example. When the customer is an AIF, the undertaking must identify and implement reasonable measures to verify the natural persons who ultimately own and control the legal entity with which it is establishing a business relationship. In this example, it will be the AIF as a legal person with a CVR number.

If no one owns or controls the AIF to such an extent that they can be defined as the beneficial owners, the AIF's general management will be regarded as the beneficial owners.

Subsidiaries
If the customer is a subsidiary, the undertaking must clarify the ownership and control structure, and determine which natural persons own or control the subsidiary's principle/parent company.

The Church of Denmark's self-governing institutions
The churches and priesthoods under the Church of Denmark are usually self-governing and run by the parish council. It is therefore members of the parish council that will be regarded as beneficial owners.

Funds
If a customer is a fund, the undertaking must determine who ultimately directly or indirectly controls the fund.

Funds, including commercial and non-commercial funds, do not have owners. The beneficial owner of a fund is regarded as the natural persons who ultimately directly or indirectly control the fund or in some other manner have powers similar to ownership, including the Board of Directors, and in some instances, special beneficiaries. However, the latter shall, in principle, only be regarded as beneficial owners if named in person according to the fund's articles of association to have a legal right to receive a significant share of the fund's assets.

Under Danish law, the founder of a fund has no form of ownership rights over its assets, and is therefore not the beneficial owner in principle. However, a specific assessment is involved, and it cannot be excluded that there can be situations when the founder, because of special powers bestowed in the articles of association, can be deemed to be the beneficial owner. The founder can furthermore be considered a beneficial owner if a member of the fund's Board of Directors.

Trusts and similar legal arrangements

If, for example, a customer is owned by a foreign trust, the undertaking must identify and take reasonable measures to verify the customer's beneficial owners. The undertaking must therefore assess the trust to clarify who can be considered the beneficial owner(s). The beneficial owner(s) of trusts and similar legal arrangements can be the following:

i. the founder(s),
ii. the trustee or trustees,
iii. The patron or patrons, special 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, and
iv. any natural person who ultimately exercises control over the trust through direct or indirect ownership or by other means.

The undertaking must retain details about the measures implemented.

Estates, bankruptcy estates and undertakings in liquidation
In the case of estates, bankruptcy estates and for undertakings in liquidation, the executor, insolvency administrator or liquidator – typically a lawyer – is retained to ascertain and distribute assets.

For undertakings, e.g. banks that have the estate, bankruptcy estate or undertaking in liquidation as a customer, the executor, insolvency administrator or liquidator will be regarded as the customer's beneficial owner. This is due to the executor, insolvency administrator or liquidator being regarded as the general management of the estate.

In public administration of an estate, it is thus the lawyer who is regarded as the beneficial owner of the estate. In private administration of an estate, the heirs have been given the estate and have full power of disposal over it. When heirs contact a lawyer/executor to request assistance with administration, there will be a power of attorney relationship between the estate and the lawyer/executor, according to which the lawyer/executor must be identified as the beneficial owner. If the heirs retain full power of disposal over the estate, it will be the heirs who are regarded as the beneficial owners of the estate. It is sufficient to identify and verify the heir who may have been authorised by the others to dispose of the estate as the beneficial owner.

Note that in the case of estates, bankruptcy estates and undertakings in liquidation, the estate's or the undertaking's previous beneficial owners will continue to be registered as being the customer's beneficial owners in the DBA's register of beneficial owners.

With regard to identification by lawyers of the beneficial owners in estates, bankruptcy estates and undertakings in liquidation, reference is made in more detail to the Danish Bar and Law Society's guidelines on money laundering.

Beneficial owners in other types of legal persons, etc.
Customers traded on a regulated market
If a customer is a listed undertaking, i.e. its shares are traded on a regulated market, the customer has no beneficial owners and the general management of the customer cannot therefore be regarded as the beneficial owners.

Customers owned by an undertaking with shares traded on a regulated market

If a customer is owned by a listed undertaking, with its shares traded on a regulated market, it will be the customer's general management who are regarded as the beneficial owners, as there are no beneficial owners of the (listed) undertaking.

For identification of who is the beneficial owner of other types of legal persons etc., refer to the DBA's Guide on beneficial owners, which deals with the identification of beneficial owners in companies, funds, certain associations and in undertakings that are covered by financial legislation etc. In connection with KYC procedures, Annex 2 of the DBA's guide can help interpret who should be regarded as the beneficial owner in those situations when no natural persons can be identified who own or control the undertaking to such a degree that they are the beneficial owners, as defined by the AML Act.

9.6.5. Reporting beneficial owners

Undertakings covered by the AML Act are required to report discrepancies in relation to the details registered on beneficial owners.

This section deals with the duty to reporting to the DBA's IT system for such undertakings. With regard to the AML Act's requirements for undertakings to obtain identity details and verify them in relation to a customer's beneficial owners, see Section 9.6.2. concerning the obtaining of identity details and Section 9.6.3. concerning the verification of identity details of beneficial owners.

As part of the undertaking's KYC procedures, the undertaking must obtain a registration certificate or an extract of the details in the DBA's IT system. If there is a discrepancy between the details obtained by the undertaking about the customer's beneficial owners and those in the DBA's IT system, the discrepancy must be reported to the DBA. If the customer has the discrepancy corrected as soon as possible, the undertaking will not have to report the discrepancy to the DBA.

The duty to report includes discrepancies in relation to the details in the DBA's IT system, i.e. details on the beneficial owner and the rights of the beneficial owner, and the details available to undertakings covered by the AML Act's KYC requirements when they investigate who the beneficial owners of their customer are.

In the case of estates, bankruptcy estates and undertakings in liquidation, when the trustee, insolvency administrator or liquidator is regarded as the customer's beneficial owner, the customer's previous beneficial owners must continue to be registered in the DBA's register of beneficial owners, and where reporting is only required, cf. Section 15 a of the AML Act if there are discrepancies in the details on the customer's previous beneficial owners. Reference is also made to Section 9.6.4 on clarification of ownership and control structure regarding estates, bankruptcy estates and undertakings in liquidation.

For further guidance, refer to the Executive Order on reporting discrepancies in details on beneficial owners, and the DBA's guide regarding reporting on beneficial owners, see https://erhvervsstyrelsen.dk/vejledning-indberetning-om-reelle-ejere.

9.7. The purpose and intended nature of business relationships

Reference to the AML Act: Section 11 (1), no. 4.

Reference to the 4th Money Laundering Directive: Article 13 (1), no. c.

The undertaking must assess the purpose and intended nature of business relationships. If relevant, the undertaking must also obtain details of the purpose and intended nature from the customer.

The undertaking must make a specific assessment whether it is relevant to obtain details. That assessment can depend on product type.

Knowledge of the purpose and intended nature of the business relationship will help the undertaking to determine whether the relationship has a legitimate purpose, and to obtain deeper insight into the overall risk profile of the business relationship.

The requirement that the undertaking has to assess the purpose of the business relationship means that the undertaking must know why the customer wants the relationship, e.g. the customer wants to use a deposit account for paying salaries, or to invest in shares and other securities.

The purpose of the business relationship is relevant to the undertaking's assessment of the specific customer relationship, including its assessment of whether there is a risk of money laundering or terrorist financing. Furthermore, the details are relevant to the undertaking's monitoring of the customer relationship, and for deciding whether a specific transaction or the like is unusual for the customer, and for the customer's purpose with the business relationship.

The undertaking needs to understand why the customer wants the product or service. If the undertaking believes it is relevant to obtain details of the purpose, it may need details on the following for example:

1) Why the customer wants a given product or service.
2) What is the expected size, quantity or frequency of transactions the customer wants performed.

If the undertaking does not obtain details on the purpose after risk-based assessment, it can use its monitoring of the customer to determine whether the customer's purpose with the business relationship is in line with the undertaking's understanding of it. The undertaking can use monitoring to determine what is typical or usual for the customer relationship in questions, and whether the customer deviates from it.

The requirement that the undertaking must assess the intended nature of the business relationship means that the undertaking has to understand its nature, i.e. the characteristics and circumstances that give the business relationship its distinctive character.

The undertaking will more often need to obtain details on the intended nature than the purpose, because the latter can be determined by or result from the product type. The intended nature of the business relationship indicates something specific about the customer, and the customer's use of the product. Examples include understanding the origin of the customer's funds, or how a business customer generates its revenue.

If the undertaking believes it is relevant to obtain details of the intended nature, it may need details on:

1) The customer's specific business model if the customer is a legal person.
2) The customer's earnings and assets.
3) How the customer intends to use the funds.

9.8. Continuous monitoring of the business relationship

Reference to the AML Act: Section 11 (1), no. 5. Reference to the 4th Money Laundering Directive: Article 13 (1), letter d.

The undertaking must continuously monitor an established business relationship. The requirement applies to monitoring the transactions made by the customer and in relation to other customer activities, generally referred to as the customer's behaviour, which the undertaking gets to know, for example, through general contact with the customer.

The purpose of monitoring is to reveal whether the behaviour of the individual customer, including the customer's transactions and activities, is consistent with the undertaking's knowledge of the customer. The undertaking has to monitor the customer's behaviour to ensure that it complies with the customer's business and risk profile, and that the customer's transactions and activities are in line with those of other customers with the same business and risk profile.

The term "customer's business profile" is defined as information about the customer's profile based on details on, e.g. the purpose of the business relationship, extent of transactions, size of transactions, regularity and duration. "The customer's risk profile" means that monitoring of the business relationship must be based on the profile of the customer the undertaking has compiled based on its risk assessment of the business relationship with the customer. See Section 13 on risk assessment – KYC procedures.

Monitoring should be adapted to each customer's circumstances and be continuously adjusted based on knowledge of the customer and its history. However, undertakings with a simple business model can opt to monitor all or a group of their customers in the same way, e.g. a money transfer company with the same customer types, and that only transfers money to a single geographic territory.

The undertaking should use monitoring to ensure that the transactions and activities carried out by the customer are in accordance with the undertaking's knowledge of the customer, and its business and risk profile. If a customer's business and risk profile changes, the undertaking must adjust its monitoring. If the undertaking has investigated the customer based on suspicious circumstances, it can be relevant to expand the monitoring. See Section 24.1 on enhanced monitoring.

Based on risk assessment, the undertaking can search for details on the origin of the customer's funds, if a transaction is unusual given the undertaking's knowledge of the customer's earnings and assets, including liquidity. In such instances, the undertaking must know the origin of the funds that concern the business relationship. Typically, simply obtaining additional details from the customer about the origin of

its funds will not be sufficient to disprove a suspicion. The undertaking must obtain documentation, for example. in the form of a sales agreement, pay slips, estate inventory or similar.

The term "origin of the funds" applies where the following originate from:

1) Customer's wealth.
2) Funds used in a transaction.
3) Funds that are part of a business relationship.

For example: if a customer wants to deposit or has deposited a large amount the undertaking regards as unusual for the customer, the undertaking can obtain details and documentation of the origin of the funds the customer wants to deposit or has deposited.

In relation to customers with increased risk, it may be necessary to know the origin of the funds before the undertaking performs a transaction or other activity for the customer. It will be relevant, for instance, when the undertaking has determined from risk assessment of the business relationship that this is a customer relationship with increased risk of money laundering or terrorist financing. See Section 14 on enhanced KYC procedures.

In relation to business relationships that concern advisory services and brokerage, the undertaking must monitor whether the customer's requests are unusual in relation to the details the undertaking has on the customer and its business/risk profile.

Because the requirement on monitoring applies to transactions and activities, it can be relevant to have manual and system-based monitoring. Manual monitoring can, for example, involve the undertaking having determined how its employees report suspicious behaviour to the AML Officer. System-based monitoring can, for example, be an IT system that monitors the customer's transactions and activities, triggering an alarm in the event of unusual or suspicious behaviour.

There is no requirement that undertakings must have an IT system for monitoring, but in undertakings with a large number of customers and complex products and transactions, it can be necessary to ensure the necessary level of monitoring. It may, for example, be relevant in connection with the monitoring of its customers by a bank.

9.9. Continuous updating of details on the customer

Reference to the AML Act: Section 11 (1), no. 5. Reference to the 4th Money Laundering Directive: Article 13 (1), letter d.

Details, documents and data obtained about a customer must be continuously updated with regard to the undertaking being able to determine whether the risk related to a business relationship has changed. That means that details the undertaking obtained as part of its KYC procedures may need to be updated in the course of the customer relationship.

The undertaking can determine procedures for updating. For example: the undertaking can decide that updating details on a customer broken down into different risk classifications can be performed at different intervals, depending on whether the risk is limited, medium or high.

See Section 8.2 on changes to a customer's relevant circumstances, and 8.3 on KYC procedures at appropriate times.

10. When a person acts on behalf of the customer

Reference to the AML Act: Section 11 (2).

Reference to the 4th Money Laundering Directive: Article 13 (1).

When a person acts on behalf of a customer, or when there is any doubt whether a person is acting on its own behalf, the undertaking must:

1) identify the person, and
2) verify the person's identity using a reliable and independent source.

The requirement arises in instances when a person states themself that they are acting on someone else's behalf, or when the undertaking is in doubt whether the person is acting on its own behalf.

The natural or legal person on whose behalf another person is acting on is the customer, and is therefore the person whom the undertaking will conduct its KYC procedure on.

The undertaking is only compelled to identify and verify the person's identity of the person acting on behalf of the customer. This means that the undertaking does not have to conduct other KYC procedures on that person, including, for example, purpose and intended nature.

When natural or legal persons act on behalf of a customer, the undertaking must ensure that such natural or legal persons have authorisation to do so.

The scope of the provision relates to third parties, and in this context, the power of attorney is not covered by Section 11 (2) of the AML Act, because the holders of a power of attorney act as part of the undertaking and not as an independent third party on behalf of the undertaking. However, other legislation may imply that the undertaking should ensure that the person concerned acts on the basis of a power of attorney and within its limits.

If the undertaking is in doubt about whether a person is acting on behalf of a customer, it can be sufficient to ask the person in some instances. If the undertaking cannot thereby disprove the doubt, or if there is doubt as to whether the person's details are correct, the undertaking must check the person's identity.

In the event of a power of attorney relationship, it is the undertaking who must determine what documentation is necessary. There are some products for which power of attorney is naturally used, such as when setting up child savings accounts. This product is limited risk, and the child as a customer can e.g. be identified and verified by his/her birth certificate. The parents or grandparents must be identified and verified as proxies acting on behalf of the child.

There are other power of attorney relationships in which just one document can be sufficient documentation. These can include a municipal employee able to present an identity card issued by the municipality and documenting the employment relationship.

In situations when a power of attorney relationship is unclear, or when there is doubt concerning it, the undertaking must have details or documentation from the person that proves the person has the necessary authorisation to act on the customer's behalf.

The requirement that the undertaking ensures that natural or legal persons acting on behalf of a customer are authorised to do so, does not apply if the person in question is a lawyer appointed in this country or in another EU or EEA member state.

11. Beneficiaries of life insurance and pension funds

Reference to the AML Act: Section 12 (1) and (2).

Reference to the 4th Money Laundering Directive: Article 13 (5).

Identity details must be obtained for life and pension insurance on the beneficiary named in the policy. Life insurance and pension companies must obtain the name of the beneficiary as part of their KYC procedures.

If this is an unnamed person or a group of unnamed persons, the undertaking must have sufficient information to be able to identify the beneficiary or beneficiaries at the time of disbursement.

"Sufficient details" in this context means that the life or pension insurance company believes it will be able to identify the beneficiary at the time disbursement is made. The insertion of "next of kin" as the beneficiary will be sufficient, as the beneficiary can be identified at the time of disbursement according to the applicable for the next of kin.

As soon as the beneficiary is identified or designated, the undertaking must obtain identity details on that person. Obtaining identity details on the beneficiary can be performed, for example, by the customer (the policyholder) informing the undertaking of the name of the person.

The purpose of obtaining the name of the beneficiary is that this information must be established in the risk assessment of the customer relationship, including whether enhanced KYC procedures should be carried out.

If a beneficiary is a PEP, enhanced KYC procedures must be implemented. See Section 15 on politically exposed persons.

Verifying the identity details of beneficiaries
A beneficiary's identity details must be verified in the same way as customers, pursuant to Section 11 (2). For natural persons, the identity details will be name and CPR number.

Verification must be based on documents, data or details obtained from a reliable and independent source. See Section 9.2 on the verification of identity details.

Verification of identity details must be performed before disbursement to the beneficiary.

This means that verification of the identity details can wait to be performed at a point in time before disbursement to the beneficiary, but details on name cannot wait until that time.

12. Correspondent relationships

Reference to the AML Act: Section 2, no. 4 and Sections 19, 20.

Reference to the 4th Money Laundering Directive: Articles 19 and 24.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 12.
Reference to: European Banking Authority, Guidelines for risk factors, JC 2017 37, 04.01.2018.

The conclusion of a correspondent relationship with a respondent is covered by the AML Act. This applies both to correspondent relationships in EU and EEA member states, and to correspondent relationships outside the EU/EEA.

Correspondent relationships are defined in Section 2, no. 4 of the AML Act, as:

a) The provision of banking services from one bank (the correspondent) to another bank (the respondent), including the opening of a current account or debit account, as well as other services such as cash management, international funds transfer etc.
b) A relationship between an undertaking subject to Section 1 (1), nos. 1-13 or 19 (the correspondent) and another undertaking subject to Section 1 (1), nos. 1-13 or 19 (the respondent), when similar services are provided, including relationships entered into for the purpose of securities transactions or the transfer of funds.

A correspondent relationship not only covers business relationships between banks, but also between those undertakings listed in the provision in Section 2, no. 4, letter b, e.g. providers of payment services, if providing a banking or similar service. In a correspondent relationship, the correspondent provides (sells) the financial services, while the respondent receives (buys) the financial services.

There will generally be a correspondent relationship covered by the AML Act when two financial undertakings exchange financial services of an ongoing nature. In general therefore, no correspondent relationship will be established when carrying out an individual transaction.

When determining whether an individual transaction or a correspondent relationship is involved, the undertaking can take into account the risk in the transaction, including the size of the amount and the financial product. The undertaking should have clear procedures for this, including how to ensure that there is an individual transaction.

Exchange of SWIFT keys

International electronic money transfers are supported by a messaging system offered by SWIFT (Society for Worldwide Interbank Financial Telecommunication), via an RMA (Relationship Management Application), also known as an RMA key.

To be able to communicate money transfer notifications using the SWIFT system, undertakings have to have created and exchanged an RMA key (authorisation key) with each other.

The SWIFT system makes it possible to control which types of messages (MT types) can be exchanged through the RMA. Opening an RMA and/or exchanging SWIFT messages between two undertakings does not in itself establish a correspondent relationship. Sending messages via the SWIFT system is only a communication channel that allows two undertakings to send messages via a secure system. However, in such situations, the undertaking must determine when establishing a business relationship is involved that requires the implementation of KYC procedures.

12.1. KYC procedures

If a correspondent relationship is within the EU/EEA, the general rule is that the undertaking can conduct normal KYC procedures, including making a specific risk assessment of the specific business relationship with the respondent, etc. That risk assessment can mean that the undertaking concludes that it will conduct enhanced KYC procedures on the respondent. See Section 12.2.1. on correspondent relationships within the EU/EEA.

When a correspondent relationship is with a respondent outside the EU/EEA, which does not involve making payments, the principle is that the undertaking can conduct normal KYC procedures, including making a specific risk assessment of the specific business relationship with the respondent, etc.

As soon as the undertaking establishes a correspondent relationship involving making payments with a respondent institution located in a country outside the EU/EEA with which no agreement has been entered into in the financial area, the undertaking must implement enhanced customer KYC procedures on the respondent. See Section 12.2.2. on correspondent relationships outside the EU/EEA.

The obligation to conduct KYC procedures rests with the correspondent, as the correspondent is the undertaking that provides (sells) financial services to the other undertaking, while the respondent is the undertaking that receives (buys) financial services directly from the correspondent. Therefore, only the correspondent has to perform KYC procedures on the respondent. In the event of the financial services being reciprocal (going both ways), both undertakings will have to conduct KYC procedures. See Section 12.2.

The LYC procedures must be completed before an undertaking covered by Section 1 (1), nos. 1-13 and 19 of the AML Act can establish a correspondent relationship.

12.2. The correspondent's duties

If the undertakings mutually exchange (buy and sell) financial services with each other, each undertaking (the correspondent) must perform KYC procedures on its customer (the respondent). This means that both undertakings must conduct KYC procedures on the counterparty for mutual exchange of services.

If it is believed that the relationship between two undertakings is a correspondent relationship covered by the AML Act, the correspondent is obliged to conduct KYC procedures on the respondent before the relationship is established.

12.2.1. Correspondent relationships within the EU/EEA

When a correspondent relationship is with a respondent in a country within the EU/EEA, the undertaking/correspondent must conduct KYC procedures, including making a specific risk assessment of the specific business relationship with the respondent, etc. The specific risk assessment can lead the undertaking/correspondent to conclude that it must conduct enhanced KYC procedures on the respondent.

In such a situation, the correspondent will have to conduct ordinary KYC procedures pursuant to Section 11 of the AML Act, and possibly supplement them with enhanced KYC procedures pursuant to Section 17 on the basis of risk assessment of the respondent.

There are certain factors that can indicate increased risk, which the correspondent has to be aware of, including:

1) If the account can be used by other units within the respondent bank's group, i.e. other units that have not been subject to the correspondent bank's KYC procedures.
2) If the account can be used by other banks or customers with a direct relationship to the respondent, but that have no direct relationship with the correspondent. In such instances, it will mean that the correspondent provides services to other banks than the respondent with which a correspondent relationship exists.

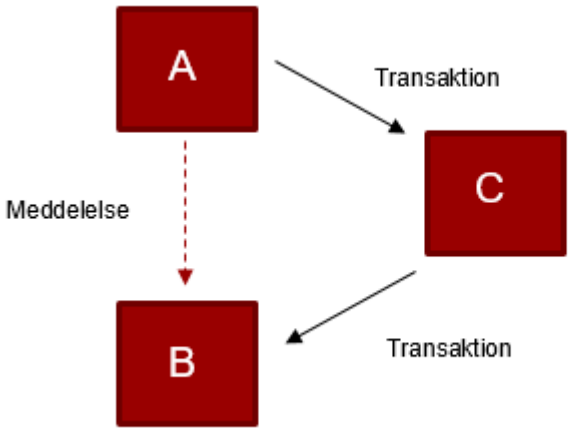
Conversely, there are also factors that can help reduce the risk, including:

1) When undertakings act on their own behalf, and therefore do not handle transactions on behalf of their customers, e.g. in connection with currency transactions between two banks, where the banks are the owners, and conducting the transactions does not involve a third party. I.e.: the transaction is executed at the expense of the respondent bank.
2) When the transaction concerns the sale, purchase or mortgaging of securities on regulated markets, e.g. when the respondent bank acts as or uses a deposit bank with direct access, normally through a local participant in a securities settlement system in the EU or a third country.

Undertakings entering into correspondent relationships can seek guidance on specific risk assessments and risk factors in the EBA's guidelines on risk factors.

The undertaking must be able to demonstrate to the authority which supervises compliance with the AML Act that the undertaking has sufficient knowledge of the respondent with regard to the risk of money laundering and terrorist financing.

The figure below illustrates an example when a customer at one bank (A) wants to send money to a customer at another bank (B). However, A does not have an account relationship with B. A can therefore not send money on behalf of its customer directly to an account with B. In the following cases, all three banks are established within the EU /EEA.



Bank A uses its correspondent relationship bank C (called the "intermediary bank"), which has a correspondent relationship with bank B. A can thus simply send a (SWIFT) message to B that there is an amount on the way to the customer at B, illustrated by the dotted line in the figure.

In this example, C is the correspondent and A is the respondent in the transaction between A and C. B is the correspondent in the transaction between C and B. C must thus conduct KYC procedures on A, while B must conduct KYC proceedings on C. There is no correspondent relationship or customer relationship between A and B, which is why A, in this scenario, does not have to conduct KYC procedures on B.

12.2.2. Correspondent relationships outside the EU/EEA

In instances when an undertaking/correspondent establishes a correspondent relationship with a respondent located in a country outside the EU/EEA with which the Union has not entered into an agreement in the financial field involving the execution of payments, the correspondent must always conduct enhanced KYC procedures on the respondent in accordance with the requirements that follow from Section 19 of the AML Act, in addition to the general KYC procedures.

The correspondent must therefore conduct standard KYC procedures in accordance with Section 11 of the AML Act, as well as enhanced KYC procedures in accordance with Section 19.

Reference is made at the end of the section regarding a more detailed review of Section 19 of the AML Act.

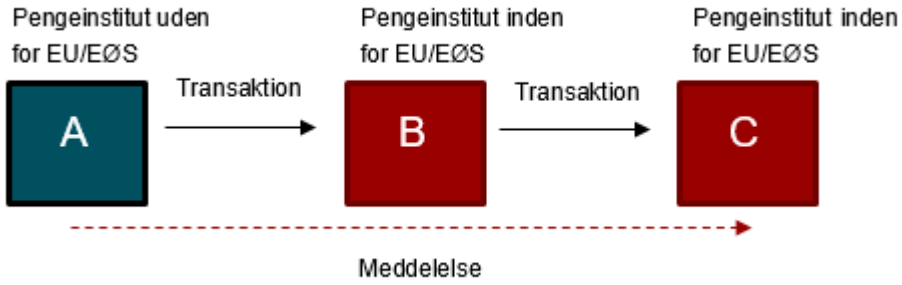
A correspondent relationship falls within Section 19 of the AML Act in the case of 1) a cross-border relationship with a respondent institution outside the EU/EEA with which the EU has not entered into an agreement in the financial area, and 2) a relationship involving the implementation of payments. Implementation of payments involves the transfer of funds for the respondent's customers to the correspondent.

"Payments" are defined as commercial payments for retail customers, business customers and/or financial institutions. Securities trading and the exchange of securities are thus not covered by the scope of the provision.

A number of financial services will thus fall outside the scope of Section 19 of the AML Act. For example, securities trading and/or confirmation or notification of letters of credit or guarantees.

If the correspondent relationship between the correspondent and the respondent outside the EU/EEA does not concern the implementation of payments, the requirements in Section 19 of the AML Act do not apply. However, the correspondent must continue to meet the requirements of Section 11 of the AML Act and possibly Section 17 vis-à-vis the respondent.

The figure below illustrates the situation when a customer at a bank (A) outside the EU/EEA wants to send money to a customer at a bank (C) within the EU/EEA.



Bank A does not have an account with bank C, which is why bank A uses bank B as an intermediary (called the "intermediary bank") to send the payment. Bank B is located within the EU/EEA. A has an account with B, and B has an account with C.

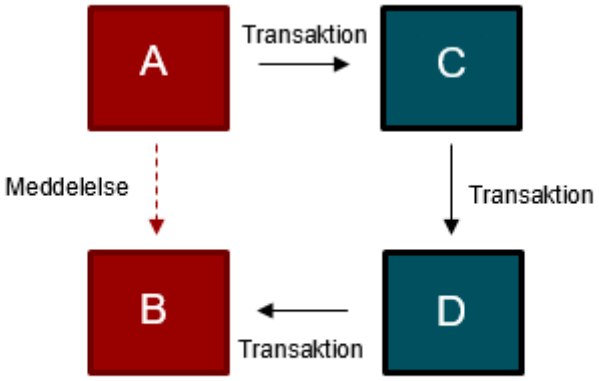
In this scenario:

C will conduct KYC procedures pursuant to Section 11 and possibly Section 17, based on a risk assessment, on B.

B in relation to A will conduct KYC procedures pursuant to Section 11, based on a risk assessment, and KYC procedures pursuant to Section 19, as A is located outside the EU/EEA.

The obligations to conduct KYC procedures only apply inter-partes. KYC procedures only have to be conducted on the direct counterpart, which is why bank C in this scenario does not have to do so on A, as A is not a respondent to C. A only sends a notification to C, which is illustrated by the dotted line.

The figure below illustrates payments through several intermediaries (called the "intermediary banks").



Banks A and B are located within the EU/EEA, while banks C and D are located outside the EU/EEA.

The funds are sent from bank A first via bank C to bank D and then to bank B. Bank A sends a SWIFT message to bank B, which is illustrated by the dotted line.

There is no correspondent relationship or customer relationship between bank A and bank B, which is why bank A does not have to conduct KYC procedures or risk assessment on bank B in this scenario. Bank B must conduct enhanced KYC procedures on bank D in accordance with the requirements of Section 19 of the AML Act. This is due to the fact that there is a cross-border correspondent relationship with a respondent institution located in a non-EU/EEA member state with which the EU has not concluded a financial agreement and a relationship involving the execution of payments.

The correspondent's obligations under Section 19 of the AML Act (supplement to the general obligations pursuant to Section 11)

If a correspondent relationship involving the execution of payments is established with a respondent from a country that is not an EU or EEA member state, the correspondent must:

1) obtain sufficient details on the respondent, so that the correspondent understands what the respondent's business consists of,
2) evaluate the respondent's reputation from publicly available information,
3) evaluate the quality of the supervision the respondent is subject to in the country in which the respondent is established, e.g. on the basis of evaluation reports from the FATF, IMF or others, or by contacting the respondent's supervisory authority on its supervisory activities.
4) obtain sufficient information to ensure that the respondent has effective control procedures in order to comply with the rules on combatting money laundering and terrorist financing,
5) obtain approval from the AML Officer,
6) document the correspondent’s and the respondent's responsibility for fulfilling the rules of the AML Act.

Re. 1-3: Sufficient details on the respondent's business, reputation and the supervision it is subject to:

It follows from nos. 1-3 that the correspondent should gather sufficient information on the respondent to understand what the respondent's business consists of and, based on publicly available information, assess the respondent's reputation and the quality of the supervision the respondent is subject to in the country in question,

In the opinion of the FSA, the requirement implies that the correspondent must obtain details of the respondent's business model, customer base, and assess (and where relevant, obtain) information on the undertaking's purpose and intended nature. To meet the requirement, available information about the respondent relationship can be used, e.g. via the Internet, from private providers of information on financial institutions worldwide and information provided by the respondent.

Re. 4: Sufficient information to ensure that the respondent has effective control procedures in order to comply with the rules on combatting money laundering and terrorist financing:
When the undertaking has to obtain sufficient information, it will have to perform assessment on the basis of the requirements that apply in accordance with international standards that correspond to the requirements in the Danish AML Act.

The correspondent must always make an assessment of the respondent, and in this connection assess the scope of investigation of the respondent.
As part of its investigation of the respondent, the correspond could:

1) use international AML questionnaires, e.g. Wolfsberg Group's Standard Anti-Money Laundering Questionnaire for the potential respondent relationship for answering,
2) obtain information on the respondent's policy within the money laundering area,
3) investigate whether the respondent has been found guilty of, involved in or suspected of money laundering or terrorist financing, and
4) obtain details of the respondent's business procedures for controls, compliance function or the like.

It is of major importance that the correspondent does not rely solely on information provided by the respondent itself, based on a risk assessment, e.g. via. Wolfsberg Group's Standard Anti-Money Laundering Questionnaire.

Re. 5: Approval from the AML Officer:
The AML Officer shall perform a genuine assessment of the respondent relationship on the basis of the details the correspondent has obtained from the respondent. There are no formal requirements for approval, but the undertaking must be able to document them.

Re. 6: Document its own and the respondent's responsibility for fulfilling the rules of the AML Act:
The correspondent must ensure documentation that there are clear agreements between the correspondent and the respondent pertaining to responsibility for compliance with the requirements in the AML Act, in cases in which funds belonging to the respondent's customers will be deposited in an account that has been set up by the correspondent in Denmark. This means that the correspondent and the respondent must have entered into a written agreement on who is responsible for the individual obligations, and that this agreement has been adopted by both the correspondent and the respondent.

12.3. Payable-through accounts

If the respondent relationship's customer has direct access to controlling funds held in an account with the correspondent relationship, the correspondent shall ensure that the respondent conducts KYC procedures and that the respondent is able to disclose information on the customer at the request of the correspondent.

If the respondent relationship's customer has direct access to funds held in an account with the correspondent (known as "Payable-through accounts"), the correspondent must ensure that the respondent in the country the respondent is established in is subject to requirements on conducting KYC procedures

The correspondent can, for example, ensure this by obtaining random samples of the respondent's established customer relationships. It will be insufficient to ensure that the respondent in the legislation is subject to KYC procedures. The correspondent must investigate and thus ensure that the respondent actually conducts them.

The correspondent must further ensure that the respondent can provide KYC information upon request to the correspondent. This can be done, for example, in accordance with the terms and conditions set out in a contract.

This requirement means that correspondents in Denmark are responsible for customer relationships of respondent relationships in the same manner as if those customers had direct customer relationships with the correspondent in Denmark.

12.4. The undertaking cannot have a correspondent relationship with a shell company

A shell company as defined by the AML Act is an undertaking that runs the same type of business as undertakings and persons referred to in Section 1 (1), nos. 1-13 and 19, but that is not present in the country where the company is domiciled, is not managed or administrated in the country in question and which is not part of a regulated financial group.

The undertaking cannot have direct or indirect relationships with a shell company, and cannot therefore set up or maintain such a relationship. Furthermore, the undertaking must take reasonable measures to avoid establishing correspondent relationships with undertakings when publicly available information reveals that the respondent allows shell banking companies to use the respondent's accounts.

"Reasonable measures" are defined as the undertaking performing an evaluation of potential respondent relationships before entering into a business relationship with them. Evaluation can include clarification of whether the potential respondent relationship has previously allowed that the respondent relationship allows shell companies to use its accounts.

The undertaking must therefore not set up a correspondent relationship, for example, before searching on the respondent relationship in publicly available sources.

13.Risk assessment – KYC procedures

Reference to the AML Act: Section 11 (3).

Reference to the 4th Money Laundering Directive: Article 13 (2).

The undertaking must conduct KYC procedures on all its business relationships. The requirements in Section 11 (1) and (2) can therefore never be omitted, even in instances of reduced risk.

This means that identity details must be obtained for all customers. Identity details must be verified, the customer's business and risk profiles clarified, and the customer relationship must be monitored. When customers are legal persons, the identity details of the beneficial owners must also be obtained. See Section 9.6 on beneficial owners.

The undertaking's KYC procedures can be conducted based on a risk assessment of the specific customer relationship.

The KYC procedure and risk assessment will determine the customer's risk profile at the time the customer relationship commences. The risk profile can change during the customer relationship, and therefore there is a requirement that the undertaking conducts KYC procedures regularly at certain intervals during the entire customer relationship, such that the details on the customer are kept updated. See Section 8.3 on KYC procedures at suitable times.

When entering into the business relationship, or in the event of later KYC procedures, the undertaking may also need to investigate the origin of the customer's funds to evaluate any possible risks related to money laundering or terrorist financing.

Risk assessment generally involves assessment of:

1) The risk of money laundering and/or terrorist financing.
2) Whether the customer is the person they claim to be.

The undertaking should determine the level of its KYC procedures based on the overall risk assessment it has performed on its business model. See Section 3 on risk assessment. The undertaking can also specifically assess each business relationship to a customer based on the same risk factors.

Risk assessment can address:

1) Who is the customer?
2) What products or services does the customer want?
3) Are there relevant geographical aspects to take into account regarding the business relationship to the customer?
4) Which delivery channels are there to the customer?

The factors listed are not exhaustive, and there is no requirement for the undertaking to take them all into consideration. The undertaking must therefore determine the relevant risk factors itself.

The risk assessment must include the business relationship's:

1) purpose
2) scope
3) regularity
4) permanence.

These four factors do not in themselves indicate a limited or high risk. For example: the purpose a customer has for the business relationship can specifically indicate high risk. Conversely, a business relationship to a customer can, for example, indicate a limited risk if it is regular and permanent. This depends on a specific assessment, and the undertaking must consider each factor and what they collectively indicate for the customer's risk profile.

Risk assessment must involve the factors stated in Annexes 2 and 3 of the AML Act, which list the factors that can be an indication of limited and high risk respectively.

When assessing the above four factors, the undertaking can, for example, assess the scope of the assets the customer wants to deposit, the size of the transactions or how long the customer expects the business relationship to last with the undertaking.

The undertaking can determine a model for its initial KYC procedures and risk assessments, e.g. putting the customers into categories of limited, medium or high risk. This is relevant for the undertaking to determine whether there is anything that can require simplified or enhanced KYC procedures with regard to a given customer, and how often regular updating of those procedures should be.

14. Enhanced KYC procedures

Reference to the AML Act: Section 17.

Reference to the 4th Money Laundering Directive: Article 18.
Reference to the 5th Money Laundering Directive: Article 1 (1), nos. 10 and 11.

Enhanced KYC procedures must be used in addition to the standard KYC procedures. This means that they will supplement the standard procedures in situations when a business relationship is deemed to have an increased risk or high risk of money laundering and/or terrorist financing. When assessing, the undertaking must take into consideration the high-risk factors presented in Annex 3 of the Act, as well as other high-risk factors deemed relevant.

It is not possible to provide an exhaustive list of which situations can require enhanced KYC procedures, nor what they should ultimately encompass. The undertaking has to determine from risk assessment what reassurance it can gain from knowledge of the business relationship, and limit the increased risk of money laundering and/or terrorist financing.

This does not mean that the undertaking cannot enter into business relationships with customers it deems to have an increased risk of money laundering and/or terrorist financing, but the undertaking is obliged to carry out enhanced KYC procedures. The undertaking must organise its enhanced KYC procedures on the basis of a risk assessment, cf. Section 17 (1) of the AML Act.

The measures to be initiated for increased or high risk can be determined on the basis of a risk assessment. The need for them can vary, according to what risk the undertaking has identified in its risk assessment of the business relationship. But there is no requirement that the undertaking has to customise the enhanced KYC procedures for all its business relationships. The objective is that in relation to its policies and business procedures, the undertaking safeguards and prevents increased risks that the business relationship may specifically imply.

Enhanced KYC procedures can include the undertaking:

1) Obtaining details on the customer's address or place of birth.
2) Obtaining details from other sources than the customer.
3) Obtaining additional details on the customer, such as the customer's purpose and the intended nature of the business relationship.
4) Obtaining details on the customer's wealth and origin of the funds.
5) Verifying the identity details obtained via several independent and reliable sources.
6) Conducting KYC procedures more often throughout the customer relationship.
7) Regularly checking the customer's transactions.
8) Obtaining details on the customer's business activities.
9) Obtaining additional information on the customer's beneficial owner(s).
10) Investigating the customer's previous business activities.
11) Investigating the customer or the customer's beneficial owners, for example by online searches.
12) Sending a contract or other document to the customer's address requesting that the customer return it signed (e.g. relevant for business relationships that have not involved physical contact).
13) Obtaining the approval upon establishment or continuation of the business relationship with the customer from the senior management.

The undertaking must assess whether there is a high risk at the start of the customer relationship with the customer. An example of a customer relationship with potentially higher risk is a new customer who does not reside or operate in the country (typically dealing in a foreign currency) but who still wants to open an account in this country.

Implementation of enhanced KYC procedures may also be necessary during the customer relationship, as part of the undertaking's monitoring of the customer. Such measures could include:

1) If the customer changes its transaction patterns, e.g. by making much bigger transactions than usual, or to geographical territories it has never previously had any relationship with.
2) If the customer shows an unusual pattern, or its use of transactions, products and/or services is much more complex than the "normal" behaviour of similar customers.
3) If there is any doubt as to whether the customer's details are correct, or if the undertaking becomes aware of a demonstrable purpose that is incompatible with the customer's details.

If the undertaking believes that the customer is high risk given the above or other instances, it must implement enhanced KYC procedures, regardless of whether the customer has never previously been in the high risk category.

Furthermore, enhanced KYC procedures must always be conducted:

1) if the customer is a politically exposed person (PEP). Approval of the business relationship is required in such instances from the undertaking's AML Officer (the Section 7 (2) person) upon

entering into the business relationship with the customer. See Section 15 on politically exposed persons, and

2) upon establishing a cross-border correspondent relationship with respondents from countries outside the European Union with which the Union has not entered into an agreement for the financial area.

In such situations, the undertaking must follow the procedures set out in Sections 18 and 19 of the AML Act. See Section 15 on politically exposed persons and Section 12 on correspondent relationships.

Irrespective of the undertaking's risk assessment of a customer relationship, the undertaking must, in accordance with Section 17 (2), implement enhanced KYC procedures if the customer is domiciled in a country on the European Commission's list of high-risk third countries. Undertakings must therefore continuously ensure that they are aware of the European Commission's list and whether their customers are, or could be, domiciled in a country that is, or will be, on the list.

If the customer is domiciled in a country listed on the European Commission's list of high-risk third countries, enhanced KYC procedures must include the following:

1. Obtaining additional details on the customer and its beneficial owners.
2. Obtaining additional details on the intended nature of the business relationship.
3. Obtaining details on the origin of the funds and the source of the wealth of the customer and the beneficial owner.
4. Obtaining details on the reasons for requested or executed transactions.
5. Obtaining approval upon establishment or continuation of business relationships with the person designated in accordance with Section 7 (2) (the AML Officer).
6. Enhanced monitoring of the business relationship by increasing the number of controls and by selecting transaction patterns that require closer investigation.

Re. no. 1: Obtaining additional details on the customer and its beneficial owners.
Additional details on the customer and the beneficial owner can include address or place of birth.

Re. no. 2: *Obtaining additional details on the intended nature of the business relationship.*
Additional details on the intended nature of the business relationship could be on the business relationship's transactions and expected scope. Details on the expected scope of the business relationship can be how many transactions the customer expects to have, how extensive the customer expects such transactions to be, and more generally what the customer expects to use the business relationship for. This information is particularly relevant when, in the context of enhanced monitoring of the business relationship, the undertaking needs to determine whether the customer's expected behaviour and transaction patterns are consistent with actual behaviour.

Re. no. 3: *Obtaining details on the origin of the funds and the source of the wealth of the customer and the beneficial owner.*
Obtaining details on the origin of the funds and the source of the customer's and the beneficial owner's wealth could be where the customer's or beneficial owner's wealth came from, where the funds included in the transaction come from, or where the funds included in the business relationship come from. In this connection, relevant details could include how the customer or beneficial owner generates revenue. If the customer or the beneficial owner owns considerable wealth, relevant details on the origin of the funds

could include whether the wealth came from a selling a business, insurance disbursement or from inheritance.

Re. no. 4: *Obtaining details on the reasons for requested or executed transactions.*
Obtaining details on the reasons for transactions requested or executed implies that undertakings covered by the Act must obtain details that further support the customer's purpose of specific transactions. Examples can include transactions to family members, or if the customer has partners or customers for whom transactions are requested or performed.

Re. no. 5: *Obtaining approval upon establishment or continuation of business relationships with the person designated in accordance with Section 7 (2).*
Obtaining approval upon establishing or continuing a business relationship with the person designated in accordance with Section 7 (2) (the AML Officer) implies that undertakings compelled to appoint a person according to Section 7 (2) must obtain the approval of that person before any establishment or continuation of a business relationship, if that business relationship is domiciled in a country listed on the European Commission's list of high-risk third countries.

Re. no. 6: *Enhanced monitoring of the business relationship by increasing the number of controls and by selecting transaction patterns that require closer investigation.*
The undertaking must carry out enhanced monitoring of the customer in question if the customer is domiciled in a country included on the European Commission's list of high-risk third countries. The undertaking can enhance its monitoring by increasing the number of controls and examining the customer's transaction patterns. The undertaking must thus carry out in-depth monitoring of the customer relationship and transactions, to determine whether the customer's intended nature of the business relationship is consistent with the undertaking's knowledge of the customer.

On the basis of a risk assessment, enhanced KYC procedures can be omitted in some instances for a branch or a majority-owned subsidiary of a legal person. Further reference is made to Section 17 (5) of the AML Act.

Pursuant to Section 17 (3) of the AML Act, the undertaking must implement one or more additional risk mitigation measures when natural persons or legal entities carry out transactions involving high-risk third countries.

"Transactions" are defined as one or more actions that transfer or assign one or more assets. Transactions involving high-risk third countries are defined as all types of transactions to and from a high-risk third country.

"Risk mitigation" measures are measures an undertaking takes to reduce the risks of money laundering or terrorist financing.
According to Section 17 (3) of the AML Act, risk mitigating measures consist of one or more of the following:

1. Applying supplementary elements of enhanced KYC procedures.
2. The introduction of relevant, enhanced, reporting mechanisms or systematic reporting of financial transactions.
3. Restriction of business relationships or transactions with natural persons or legal entities from third countries identified as high-risk countries.

After further assessment, the undertaking must choose to implement one or more of the above risk mitigation measures.

Re. no. 1: Applying supplementary elements of enhanced KYC procedures.
The undertaking must specifically assess which supplementary and enhanced elements are able to specifically limit risk in relation to its business model when conducting KYC procedures. For example, the undertaking will thus be able to use several of the measures listed as examples of enhanced KYC procedures, mentioned above for Section 17 (1).

Re. no. 2: The introduction of relevant, enhanced, reporting mechanisms or systematic reporting of financial transactions.
For example: the undertaking can choose to set up several parameters and reporting mechanisms for the customer's financial transactions in its control and monitoring system, thereby enhancing monitoring of the customer relationship and specific transaction patterns.

Re. no. 3: Restriction of business relationships or transactions with natural persons or legal entities from third countries identified as high-risk third countries.
Undertakings entering into business relationships or transactions with natural persons or legal entities from the third countries identified as high-risk third countries could choose to e.g. limit or restrict the supply of products or services to that customer when the customer enters into business relationships or transactions with natural persons or legal entities from high-risk third countries.

In the event of business relationships or transactions involving countries listed on the European Commission's list of high-risk third countries and in addition to the above risk mitigating measures, the undertaking must determine whether it is relevant to ensure that the first payment is made through an account in the customer's name at a credit institution subject to requirements on KYC procedures that are at least equivalent to those procedures set out according to the AML Act, cf. Section 17 (4) of the Act.

The undertaking must thus determine whether it will be relevant, cf. the following below, to make use of this additional risk mitigation measure when a business relationship or a transaction involves a high-risk third country, so that the undertaking can manage and limit the risks further.

If the undertaking believes that it will be relevant to ensure that the first payment must be made through an account in the customer's name at a credit institution subject to requirements for KYC procedures that are at least equivalent to those laid down by the AML Act, the first payment must thus be made from an account at a credit institution subject to the same legal requirements for KYC procedures as laid down by the AML Act. This can, for example, be a credit institution in another EU or EEA member state that has implemented the requirements in the Money Laundering Directives at the same level as in Denmark. It can also be a branch or a majority-owned subsidiary of a credit institution in Denmark, whereupon the credit institution pursuant to Section 31 (2) of the AML Act must ensure that its branch or majority-owned subsidiary also complies with the rules of the AML Act, even if it is established in a non-EU or EEA member state.

Examples of when it can be considered relevant to implement this additional risk mitigation measure.
A bank establishes a customer relationship with a high-risk customer who has business connections to a high-risk third country. Based on obtaining details on the purpose and intended nature of the business

relationship, the bank still feels insecure about the customer's business relationship with a high-risk third country, and therefore considers it relevant to prevent the risk of the bank being abused for money laundering or terrorist financing. The bank can therefore demand that the customer's first payment be made through an account in the customer's name in another bank, which is subject to requirements for KYC procedures that are at least equivalent to those laid down under the AML Act.

Another example might be that a bank has a customer with limited risk who has not previously made transactions to high-risk third countries. The customer now wants to make frequent and/or large transfers to a high-risk third country. In this case, the bank may consider it appropriate to ensure that the first payment is made through an account in the customer's name in another bank, which is subject to KYC procedures at least equivalent to those laid down in the AML Act to prevent the risk of the bank being used for money laundering or terrorist financing.

The undertaking's assessment of when it will be relevant to ensure that the customer's first payment is made through an account in the customer's name at a credit institution subject to KYC procedures at least equivalent to those laid down in the AML Act may depend on both the aspects of the circumstances relationship and those concerning the transaction, including the undertaking's own circumstances and control measures regarding the relevant transactions and customer relationship in general.

Some undertakings covered by the AML Act will thus have mechanisms built into their procedures and systems that take into account the risk inherent in business relationships or transactions involving high-risk third countries. In that situation, an undertaking's assessment of whether it is relevant to require the first payment to be made through an account in the customer's name at a credit institution subject to KYC procedures at least equivalent to those laid down in the AML Act can conclude that it is not relevant to make this requirement. For example, the bank could have a large group of customers with the same risk profile and with the same types of transactions involving high-risk third countries, when the bank has otherwise protected itself against being abused for money laundering and terrorist financing.

Conversely, other undertakings will not have such mechanisms embedded in their procedures and systems in relation to this type of customer or transactions. Such undertakings will therefore be able to conclude it relevant to demand that the customer's first payment be made through an account in the customer's name at a credit institute subject to requirements for KYC procedures that are at least equivalent to those laid down in the AML Act.

15.Politically exposed persons (PEPs)

Reference to the AML Act: Section 2, no. 8, Section 18.

Reference to the 4th Money Laundering Directive: Article 3, no. 9, Articles 21, 22 and 23.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 13.

A politically exposed person (PEP) is a person with a prominent public function, and can therefore be susceptible to bribery and corruption. It is in the interest of society to prevent this happening, and should it happen, it is in the interest of society for it to be identified in time and made subject to legal action.

Bribery and corruption are a major problem on a global level, and common international standards have been introduced to combat this. The definition of a PEP as well as the requirements for processing transactions by PEPs are laid down in international standards based on experiences collected over the years from authorities across the world.

The rules on identification of PEPs are of a preventive nature and should not be interpreted as stigmatising PEPs as being involved in criminal activity. Undertakings therefore have no grounds for refusing to enter into a business relationship or ending an existing business relationship purely because they have determined that an individual is a PEP or is a family member or known close associate of a PEP.

The AML does not impose any obligations on PEPs, their family members or close associates. However, PEPs should be aware that they, along with their family members and close associates, may be asked to clarify or document their finances or specific transactions.

To assist undertakings in their work, the FSA keeps a list of Danish PEPs on behalf of the Minister for Industry, Business and Financial Affairs, to contribute to uniform, unambiguous identification and delimitation of PEPs. This list is publicly available. The organisations, authorities and undertakings covered by the Executive Order on reporting and publication of information on domestic politically exposed persons are obliged to report to the FSA.

15.1. Who is a PEP?

15.1.1. Politically exposed persons

A politically exposed person (PEP) is a person who has been entrusted with one or more of the prominent public functions listed below. This definition is common to the whole of the EU, It takes into account the fact that individual member states have made individual adaptations.

The undertaking must have procedures to determine whether a customer, the customer's beneficial owner, the beneficiary of a life insurance policy or the beneficiary's beneficial owner is a PEP.

The definition of domestic (Danish) PEPs is as follows:

1) Head of State, Head of Government, Minister, Deputy Minister or Assistant Minister. In Denmark, this covers ministers and heads of departments.
2) Members of Parliament or a member of a corresponding legislative body. In Denmark, this covers members of the Danish Parliament and Danish members of the European Parliament.
3) Member of a political party's governing body. In Denmark, this covers the governing bodies or similar executive bodies according to the articles of political parties represented in the Danish Parliament.
4) Justices of the Supreme Court, members of the Constitutional Court and other senior courts whose decisions are only subject to appeal in exceptional circumstances. In Denmark, this covers Supreme Court Judges, and Danish judges in international courts.
5) Members of the Court of Auditors and the supreme governing body of central banks. In Denmark, this covers the Board of Governors of Danmarks Nationalbank, Danish members of the Public Accounts Committee and the Danish member of the European Court of Auditors.

6) Ambassadors, chargés d'affaires or high-ranking officers in the armed forces. In Denmark, this covers the senior chiefs of the armed forces, defined as the Chief of Defence, the Vice Chief of Defence, component commanders and ambassadors for Danish embassies.
7) Members of a state-owned undertaking's administrative, managerial or supervisory body. In Denmark, this covers the Board of Directors and the managing director of undertakings in which the state owns 50 percent or more or otherwise has effective control over the undertaking. Subsidiaries of such state-owned undertakings are not covered by the term. Self-governing institutions that are financed wholly or partly via the Finance Act are not covered by the term.
   The definition also covers the director of agencies and members of the Board of Directors in agencies where such persons have executive competence.
8) Directors, Deputy Directors and member of the board or a person with similar functions in an international organisation. In Denmark, this covers persons proposed, appointed or employed by the government, a ministry or a minister in an international organisation established by concluding a formal international political agreement.

The FSA's list contains details of the name, affiliation and date of birth of domestic PEPs and aims to ensure uniformity in the use of the definition for the persons covered above. The list indicates current PEPs. However, the list also includes an additional tab that lists former PEPs. The person will be listed for at least 12 months after their status as a PEP has ceased. The list does not contain details of family members, close associates or foreign PEPs, who have to be identified in some other manner.

The list is based on information reported to the FSA, when undertakings, agencies and organisations employing a PEP have reported details of their name and also report when changes occur within a period of three working days.

The list determines who is a PEP, and can be used by an undertaking. A person can be a PEP even if not on the list because of the reporting deadline. If an undertaking or person has certain knowledge that a customer is a PEP, that knowledge will take precedence over the list.

15.1.2. Family members and close associates

Reference to the AML Act: Section 2, nos. 6 and 7 and Section 18. Reference to the 4th Money Laundering Directive: Articles 20-23.

Family members and close associates to a PEP cannot be regarded as PEPs solely as a result of their connection to a PEP. Family members and close associates who are customers of the undertaking must be identified, because they can benefit from or be abused in connection with money laundering, etc.

Family members
The definition of a family member of a PEP is provided in Section 2, no. 6 of the AML.

The family members of a PEP comprise:
1) a spouse, civil partner or cohabiting partner
2) children and their spouses, civil partners or cohabiting partners
3) parents.

In other words, this term does not cover relatives such as siblings, stepchildren and step-parents.

Close associates
The definition of close associates of a PEP is provided in Section 2, no. 7 of the AML.

Close associates to a PEP comprise:

1) A natural person who is the beneficial owner of an undertaking or other form of legal person along with one or more PEPs.
2) A natural person who, in another way has a close business relationship with one or more PEPs. For example, a long-established trading partner.
3) A natural person who is the only beneficial owner of an undertaking or other form of legal person set up for the benefit of a PEP. This means that the natural person directly or indirectly controls all the shares, voting rights, etc. in the relevant undertaking or other legal person in question.

A person who participates in board work with a PEP, when the board is deemed to be the beneficial owner of a legal person, will not be considered to be a close associate for that reason. In such cases, the undertaking will have to determine whether there is a close business relationship with a PEP that falls under point 2 above. A specific assessment will be required in foundations and other similar legal arrangements to determine whether a person who participates in board work with a PEP (when the board is deemed to be the beneficial owner) should be considered a close associate.

An undertaking must deal with the family members and close associates of a PEP according to the same rules as for PEPs. Therefore, the specific risk assessment of a PEP will also be decisive for how an undertaking designs its KYC procedures for a PEP's family members or close associates. If a PEP is placed in a category with medium risk, his/her family members and close associates will be regarded in the same manner, unless the undertaking's individual assessment of the person concerned indicates otherwise.

15.2. Customer knowledge and risk assessment

15.2.1. Determining whether a customer is a PEP, family member or close associate

Reference to the AML Act: Section 18 (1). Reference to the 4th Money Laundering Directive: Articles 20-23.

Undertakings must obtain identity details on PEPs based on risk assessment. The PEP will usually be the primary source of such details, but it is possible (and sometimes necessary) to obtain them from other sources.

The undertaking must have business procedures and systems that ensure assessment takes place when a customer relationship is established or expanded. When making its decision, an undertaking must observe the following:

1) The undertaking must always determine whether a customer is a PEP. This can be done by consulting the list the FSA compiles on domestic PEPs. How an undertaking determines whether

the customer is a foreign PEP can be done by searching the internet, or using a commercial service provider offering such information. If the intended scope of business is significant, it can also be necessary to ask for details of what the PEP's position entails.

2) The undertaking must take reasonable steps to identify customers who are family members or close associates of PEPs. If the PEP is a customer of the undertaking, this can be done by asking the PEP if he/she knows whether family members or close associates are also customers. The undertaking can also identify family members or close associates by searching the internet, or using a commercial service provider that offers such information.
3) If the undertaking also has reason to believe that a customer is a family member or close associate to a PEP, it must take reasonable steps to establish whether that is the case. This also applies even if the PEP is not a customer of the undertaking.
4) An undertaking must take reasonable steps to determine whether a customer is a foreign PEP when establishing the business relationship. In instances when the undertaking only has a suspicion or indication that a customer is a foreign PEP, it should investigate in more detail for final clarification.

"Reasonable steps"

"Reasonable steps" are defined, for example, as the following measures, as it will be up to the undertaking in a given case to determine what is sufficient to meet the requirements of the AML Act:

14) The undertaking obtains details from the relevant PEP.
15) The undertaking uses the details on the customers it already has.
16) The undertaking uses the external sources it has access to, e.g. internet and news media.
17) The undertaking subscribes to one or more service providers offering information on who is a PEP, family members or close associates of PEPs.
18) The undertaking actively verifies the details it is unsure of, e.g. by asking the relevant customers.
19) With regard to foreign PEPs, the undertaking should consider whether it ought to cooperate with local resources, e.g. lawyers, banks, etc., in the country in question, to clarify whether the customer is a PEP.

If an undertaking only has a limited number of customers, obtaining information from each customer on whether they are a PEP, and/or routinely performing online searches on their name will be an adequate procedure after a risk assessment.

Commercial providers of PEP lists

As part of its business procedures for customer knowledge, the undertaking can subscribe to private commercial providers of solutions for PEP lists, and identifying the family members and close associates of PEPs. Use of such systems will normally be an appropriate means of obtaining details, but is not a requirement. But the undertaking ought to determine whether it needs to (also) use other sources for such information.

Beneficial owners

When an undertaking determines the beneficial owners of a customer (legal person), it shall establish whether there is a PEP amongst them. This must be done according to the same principles the undertaking has to follow when determining whether a customer is a PEP. If there is a PEP amongst a customer's beneficial owners, it does not imply in itself that the customer has to be handled in the same way as a PEP. The undertaking must perform a specific risk assessment based on the PEP's control over the customer, and must determine whether the customer is acting on behalf of the PEP.

An insurance company must, in relation to the beneficiary of an insurance policy, determine whether the beneficiary's beneficial owner in an insurance policy is a PEP. This must be determined before disbursement takes place, or in the event of full or partial transfer of the policy.

Time of establishment
The undertaking must conduct KYC procedures for all customers when establishing business relationships. The undertaking must also determine whether a customer is a PEP, a family member or close associate.

For pension companies, company pension funds and labour market pension funds, it is sufficient to determine whether a customer is a PEP at the time when the customer relationship is set up.

Specific to PEPs, their family members and close associates is the fact that their status may change during the customer relationship. For example, a customer who is not a PEP could become a PEP due to a new job or election to Parliament. The undertaking must therefore continuously monitor whether customers become PEPs. This can be done, for example, by:

1) checking available details on who are PEPs at sufficiently frequent intervals, including the FSA's list of PEPs, and comparing those details against the undertaking's customer register.
2) when a customer relationship is reviewed, e.g. for new loans, and
3) when a customer's transaction gives rise to closer investigation.

If a person ceases to be a PEP, the risk assessment and monitoring must continue for at least 12 months thereafter, see Section 15.2.6 on cessation of PEP status.

15.2.2. The origin of the funds and wealth

Reference to the AML Act: Section 18 (2). Reference to the 4th Money Laundering Directive: Articles 20-23.

The undertaking must take appropriate measures to determine the origin of the PEP's funds and wealth. The undertaking can only obtain details on funds and that part of wealth covered by the business relationship or transaction. For example, a mortgage credit institution is not obliged to enquire about the PEP's holdings of any securities. When a mortgage credit loan is taken out, the customary loans procedure will suffice in order to verify the PEP's financial circumstances. In the event of early redemption of the loan, the mortgage credit institution must determine the origin of the funds. The PEP's bank will often be able to identify more aspects concerning the origin of funds and wealth, because the customer relationship will typically involve multiple services that can be linked to the risk of money laundering.

The undertaking must determine the origin of the PEP's funds and wealth based on risk assessment. For example, the following details can be included:

1) in which country the person is resident,
2) the person's position, and
3) the customer's reputation.

Other appropriate measures can be running a risk assessment related to the product the customer has chosen. For products involving high risk and large transactions, the undertaking could carry out more thorough investigations than, for example, for a life assurance policy with a low annual premium. Conversely, the undertaking could carry out less thorough investigations for products with low risk.

Some pension companies have no direct customer contact, because they are mandatory company pension funds or job market pension funds, which the customer cannot personally pay into. In such instances, the customer's financial circumstances cannot be determined to the same degree as for other forms of insurance, for example.

Based on the risk assessment, the undertaking can ask the customer to provide the necessary details. It can be necessary to obtain the details from the person concerned if the undertaking does not have them already, or if the details it does have are no longer deemed to be up to date. The need for and scope of the details must be assessed based on the circumstances, including the customer's transactions. In certain situations, such as a business relationship extending over several years, when the undertaking already has a significant insight into the customer's financial circumstances, it will be possible based on a risk assessment to decide that the knowledge the undertaking has is sufficient to be able to verify the origin of the customer's funds and that element of their wealth covered by the business relationship. The undertaking can also obtain the details from external sources.

It is always the customer's funds and wealth that are to be investigated, since it is these funds that are covered by the business relationship or transaction. In cases when a PEP is the beneficial owner of the customer (a legal person), it is therefore still the customer's (the legal person's) funds and wealth that are covered by the provision, and not the wealth or funds of the beneficial owner.

The details the undertaking can use can include the following, or combinations of the same, for example:

- Annual statement from the Danish Tax Agency.
- Wage slips.
- Accounts.
- Any company annual reports.
- Print-outs from company accounts or from public registers paid for by the customer to document ownership
- Property details, including land tax and in the Construction and Property Register (BBR).
- Details on securities held on deposit, including overseas.
- Information about movements in accounts, etc.

Details of the PEP's financial circumstances in connection with the due diligence procedure, including on the origin of funds, can be omitted if the customer is not given access to a product that would enable transactions to be carried out.

15.2.3. Approval of the customer relationship

Reference to the AML Act: Section 18 (3). Reference to the 4th Money Laundering Directive: Articles 20-23.

The undertaking's AML Officer (Section 7 (2) person) must approve a customer relationship with a PEP and customer relationships with family members and close associates of PEPs. It is not a requirement for others among the undertaking's management to approve the business relationship, aside from those approvals that follow from other legislation, such as the Executive Order on management, and the undertaking's internal policies and business procedures.

With this approval, the AML Officer judges that with the intended business relationship the undertaking can continue to comply with the legislation, and can therefore enter into the customer relationship. In the event of approval, the AML Officer should take into account the extent to which the product carries an inherent risk of use for money laundering.

If the AML Officer finds that the risk of the undertaking being abused in connection with bribery and other forms of corruption is too high, the customer relationship should not be approved.

The requirement for approval does not presuppose that the AML Officer has to carry out an actual examination of all the details in an individual customer relationship. But approval must be based on sufficiently elucidated grounds. Neither does the requirement that the AML Officer has to credit-rate the customer, determine whether insurance cover is adequate, or in any other manner determine whether the services the undertaking provides to the customer are suitable for the customer. However, the AML Officer should determine whether the agreements envisaged with the customer will enable the customer to be able to conceal bribery, for example.

With regard to the continuation of customer relationships in particular, the undertaking should determine an appropriate interval in its procedures for reviewing and possibly approving customer relationships with PEPs or a family member or close associate of a PEP. Such an interval should be determined on the basis of the risk of money laundering or corruption that the undertaking believes the customer potentially represents. It will therefore often be relevant to set different intervals. For example: by differentiating between PEPs and family members or known close associates of a PEP who come from or do not come from countries known for high levels of corruption.

If an undertaking believes that it cannot approve or extend a customer relationship covered by the provision, it must decide whether to take steps to break off or wind up of the relationship. With regard to existing customer relationships that the undertaking cannot approve, see also Section 18.1 on the undertaking's obligation to break off or wind up a customer relationship.

When the undertaking is a pension company and has no direct customer contact, because of a mandatory company pension fund or job market pension fund, it is not a requirement that the AML Officer needs to approve the customer relationship.

15.2.4. Enhanced monitoring

Reference to the AML Act: Section 18 (4). Reference to the 4th Money Laundering Directive: Articles 20-23.

Risk assessment

When the undertaking has identified the customer, it must perform risk assessment of the customer relationship. Risk assessment must determine whether the PEP or family members or close associates could abuse the undertaking to cover money laundering, including bribery.

Risk assessment must also include the relevant risk factors for the customer relationship in question. This will be a specific assessment to a large degree.

When performing risk assessment, the undertaking should focus on the following:

1) The undertaking's own assessment of the risks of money laundering it is exposed to.
2) An assessment of to what extent the risk will be increased by a business relationship with the PEP in question and/or its family or close associates. This will be a case-by-case assessment, and not automatic assessment of whether a customer relationship causes the risk of money laundering.
3) Any information from public authorities. This includes national risk assessments in the countries concerned, and international risk assessments.

The PEP's function and risk exposure in relation to the products or services the PEP wants or has with the undertaking must comprise the overall basis for assessment of the risk category of the customer relationship.

Categorisation will depend, as mentioned, on individual assessment based on specific risk assessment of the customer relationship. For example, a customer can be placed in categories such as increased risk or normal risk.

It will also be possible to put customers into two categories, such as increased and normal/limited. The important thing here is that the undertaking identifies customers with high risk.

Whether the risk will be increased by a business relationship with the PEP in question and/or its family or close associates can depend on:

1) The PEP's position and opportunity for political and administrative influence, along with the nature of the customer relationship, including the products or services the undertaking will offer the customer. This will vary, depending on the nature of a person's function. Typically, considerable political and administrative influence will be involved if the PEP is empowered to make key political or administrative decisions, or can overturn or change such decisions. For example:
    - ministers
    - heads of department
    - directors of bodies able to make independent decisions in key areas.
2) The nature of the PEP's position and whether there is a risk of abusing that position. If a position is held in a country where there is a limited risk of widespread corruption, the PEP will be able to have a prominent public function without there being increased risk.
3) The chances of a service being used to cover up corruption, e.g. by placing an amount of money or channelling money to other legal persons, or to accounts abroad.
4) Other relevant risk factors.

The undertaking must seek to determine what function the PEP has, and what influence or potential influence that function entails, and whether the PEP is at special risk of being involved in bribery or some other form of corruption.

A minister with considerable political and administrative influence will be associated with greater risk purely by virtue of his or her function more than an ordinary member of the Danish Parliament. Similarly, the Chair of a Board of Directors with greater political and administrative influence than an ordinary board member will be associated with greater risk purely by virtue of his or her function.

The following products and services could normally involve a limited risk of money laundering and corruption in accordance with Annex 2 of the AML. This applies not only to PEPs, but to all customers:

a) Life insurance policies where the annual premium is low.
b) Pension insurance policies if there is no early surrender clause and the policy cannot be used as collateral.
c) Pension funds or the like, which pay out pensions to employees, and where contributions are made by way of deduction from wages and the rules of the fund in question do not permit the transfer of a member's rights.
d) Financial products or services which provide appropriately defined and limited services to certain types of customers with the aim of promoting financial inclusion.
e) Products where the risk of money laundering and terrorist financing are controlled by other factors, e.g. expenditure ceilings or transparency in relation to ownership (e.g. certain forms of electronic money).

The following products and services could normally in themselves involve an increased risk of money laundering and corruption in accordance with Annex 3, Subsection (2) of the AML. This applies not only to PEPs, but to all customers:

1) Private banking.
2) Products or transactions which might favour anonymity.
3) Business relationships or transactions with no physical contact and without security measures such as electronic signatures in place.
4) Payments from unknown or non-associated third parties.
5) New products and new business procedures, including new delivery mechanisms, and the use of new technologies or technologies in development of both new and existing products.

A PEP who, by virtue of his or her position, is deemed to hold a particularly high political or administrative position, cf. the above, would normally be classified as high risk if the PEP wants to undertake anything other than normal business, such as setting up current accounts, portfolio management agreements and other comparable normal transactions. The undertaking must be aware that the risk of bribery and other corruption does not usually depend on the size and composition of the customer's wealth.

The undertaking is not obliged to have any special categorisation for PEPs. The categorisation it uses for other customers can also be used for PEPs. For example: the high risk category can include PEPs with high risk, and other customers with high risk. Correspondingly, a PEP deemed to represent limited risk can be put in a category with normal risk, according to the circumstances.

Categorisation is relevant to how undertakings determine the need for monitoring a PEP and/or its family members or close associates. The undertaking must carry out enhanced monitoring until it believes that the person no longer poses an increased risk of money laundering and corruption. If the person's duties have been terminated, factors such as the person's continued relationship with his or her previous position, including former business partners and colleagues, must be included in the assessment.

The requirement for enhanced monitoring to continue until it is believed that the person no longer poses an increased risk does not apply to family members or close associates. However, the undertaking should assess whether these persons can also continue to be associated with a higher risk of money laundering. If so, the undertaking should design KYC procedures and monitoring according to the risk assessed.

Customer monitoring
Monitoring the transactions of PEPs can use the same systems the undertaking uses to monitor other customers with the same risk category. The undertaking does not need to have other systems for monitoring PEPs than the systems the undertaking uses to monitor other customers. But such systems should be designed to facilitate enhanced monitoring. The undertaking must regularly monitor all customer transactions with regard to detecting whether transactions are unusual for the customer itself, and for other similar customers. Transactions can be unusual with regard to:

1) size,
2) frequency,
3) sender and receiver of a payment to or from a PEP,
4) they go through complicated corporate constructions,
5) there are many links,
6) they go through links that do not seem natural for the transaction in question,
7) they are made in currencies not usual for the customer in question.

However, monitoring must be enhanced for PEPs and be based on risk assessment.

Depending on the undertaking's monitoring systems, enhanced monitoring will be able to include:

1) more frequent updating of customer knowledge (i.e. the purpose and scope of the business relationship) than for low-risk customers,
2) the transactions of PEPs are monitored more frequently than those of limited risk customers,
3) there is more focus on suspicious transactions through intensification of the maximum monitoring of the customer relationship,
4) that the criteria for when transactions are selected for individual assessment are enhanced than for the transactions of other customers,
5) that manual checking of transactions by PEPs is performed to a greater extent than those of limited risk customers,
6) that there are stricter criteria for when the undertaking asks about the transactions, and the less an explanation makes sense or is likely compared to normal, the more the undertaking should ask for documentation, and
7) that there are stricter criteria (for example, lower amount limits) for when the undertaking obtains documentation for transactions and movement of assets. For example: there can be documentation for employee shares allocated, house sale, inheritance, division of property etc., as the PEP will usually and easily be able to provide such documentation (e.g. a letter from an employer or lawyer).

The intensity of enhanced monitoring should be proportional to the undertaking's assessment of the risk. The greater the risk, the more monitoring needs to be intensified.

Foreign PEPs

The undertaking must always carry out enhanced KYC procedures when entering into a business relationship with a foreign PEP. Foreign PEPs will often represent a high risk, because the undertaking does not have the same first-hand knowledge as it does for domestic PEPs. As a rule, the undertaking will not have the same access and knowledge of details on the person's duties, the degree of the person's powers and control by virtue of salary level.

A PEP can represent a high risk if he or she holds a prominent public function in a country that is regarded as having a greater risk of corruption. The undertaking should take all reasonable steps to determine whether a country is or can be characterised on the basis of the information available by e.g.:

- Political instability.
- Weak public institutions.
- Weak protection against money laundering.
- Armed conflict.
- Non-democratic forms of government.
- Widespread organised crime.
- A political economy dominated by a minority of persons/entities with close links to the state.
- Absence of or a weak free press and legal or other measures that suppress journalistic investigation.
- A criminal justice system that is vulnerable to political interference.
- A lack of expertise and skills in connection with bookkeeping, accounts and auditing, especially in the public sector.
- Laws and culture that act against the interests of whistleblowers.
- Weaknesses in the transparency of ownership registers for undertakings, land and shares.
- Violation of human rights.

Conversely, PEPs can be categorised as general risk if they hold a position in a country where the risk of corruption is low. The undertaking must take all reasonable steps to determine whether a country is or can be characterised on the basis of the information available by e.g.:

1) Political stability and free, fair elections.
2) Strong and independent public institutions.
3) Credible anti-money laundering measures.
4) A free press.
5) An independent judicial service and criminal justice system without political interference.
6) A system in which political corruption and similar offences are effectively investigated and prosecuted.
7) Strong traditions for auditing within the public sector.
8) Legal protection for whistleblowers.
9) Well-developed ownership registers for undertakings, land and shares.

15.2.5. Beneficiaries according to insurance policies

Reference to the AML Act: Section 18 (5). Reference to the 4th Money Laundering Directive: Articles 20-23.

If a beneficiary or a beneficial owner of a beneficiary according to an insurance policy is a PEP, the undertaking must ensure on the basis of a risk assessment that the circumstances surrounding the insurance relationship are clarified. The AML Officer must also be informed when disbursement will be made according to the insurance policy, and in the event of full or partial transfer of the policy.

The requirements apply before disbursement begins and in connection the full or partial transfer of the policy, when the beneficiary is a PEP, or when the beneficiary's beneficial owner is a PEP. In cases when the beneficiary is a legal person, it is relevant to clarify whether the beneficial owner is a PEP. The requirement also applies when the beneficiary or its beneficial owner is a family member or close associate of a PEP.

A partial transfer applies, for example, if a life assurance policy is used to pledge security for a loan arrangement. It is completely normal in connection with taking out a loan or subsequently, for the lender to ensure security for a loan in the event of e.g. death. Pledging of security does not mean that the lender/pledgee becomes a beneficiary, but any beneficiary of the life assurance policy will typically have to give way to the pledgee's claim. Some insurance policies can be sold, which is classified as a transfer in accordance with Section 18 (5) of the AML. This practice typically only applies to the transfer of privately owned life insurance policies, since the terms and conditions of most company pension and labour market pension funds state that they cannot be pledged as security for a loan or transferred to a third party. The fact that the circumstances of the insurance relationship must be clarified means that the undertaking should perform a detailed investigation of the business relationship with the policyholder.

Such an investigation should focus on whether the beneficiary or the latter's beneficial owner is a PEP, in order to clarify whether corruption or other criminal behaviour could be involved in the insurance relationship. For example: the undertaking could consider whether it is natural for the relevant person to be the beneficiary in the insurance relationship. If, in connection with an investigation, the undertaking discovers conditions that appear suspicious, the undertaking must report to the MLS. See Section 25 on the duty to report.

It is a requirement that the undertaking informs the AML Officer before disbursement or full or partial transfer of an insurance policy is made to a beneficiary who is a PEP, or to a beneficiary whose beneficial owner is a PEP. It is not a question of the AML Officer having to approve the disbursement or transfer. However, the AML Officer should be informed sufficiently in advance to be able to react, if the disbursement or transfer is deemed to be associated with a risk of money laundering or corruption.

15.2.6. Termination of PEP status

Reference to the AML Act: Section 18 (6).

Reference to the 4th Money Laundering Directive: Articles 20-23.

When a person can no longer be regarded as a PEP due to their position, the undertaking shall assess whether there is increased risk linked to the person for at least 12 months after the end of their PEP status.

However, this does not apply to the PEP's family members or close associates. In principle, they will be regarded as other customers when the PEP is no longer a PEP. Family members or close associates will only be submitted to enhanced KYC procedures if the undertakings believes there are grounds to regard the customer as being in the high risk category.

The requirement for assessment for a minimum of 12 months was introduced in connection with the entry into force of the new AML. Undertakings are thus not obliged to comply with the requirement with regard to customers who ceased to be PEPs before the entry into force of the Act. This applies regardless of whether the customer's status as a PEP ended earlier than 12 months before the Act came into force.

16. Simplified KYC procedures

Reference to the AML Act: Section 21.

Reference to the 4th Money Laundering Directive: Articles 15 and 16.

Reference to: Executive Order no. 311 of 26 March 2020 on relaxed requirements for the KYC procedure pursuant to the Act on Preventive Measures against Money Laundering and Terrorist Financing (the AML Act).

Based on risk assessment, the undertaking can use simplified KYC procedures in relation to the business relationships deemed to have a limited risk of money laundering or terrorist financing.

Simplified KYC procedures are an option the undertaking can use after specific assessment. This not a requirement to the undertaking, such as the requirement to conduct enhanced KYC procedures in the event of high risk.

The simplified procedures are not an exemption to the KYC procedures in the AML Act. It is solely an option to adjust the ongoing KYC procedures and monitoring of the customer. This means that all the requirements in Section 11 must be met, but they can be met with a minimum of measures.

The undertaking can determine whether the customer or the transaction implies limited risk. This means that the undertaking must first specifically asses whether there are risk factors linked to the customer or transaction that can indicate that there is no limited risk, before the undertaking can conduct simplified KYC procedures.

The assessment must be an objective assessment of the customer's circumstances, including:

a) the product or services the customer wants
b) the purpose, scope, regularity and duration of the business relationship with the customer.

In its assessment, the undertaking must include the factors arising from Annex 2 of the AML Act.

Examples of simplified KYC procedures can include:

1) That the undertaking obtains limited identity details on the customer, although ensuring that the customer's identity is verified. "Limited identity details" are defined as fulfilling the minimum requirement of the Act, which is obtaining name and CPR number or the like, but that no additional identity details are obtained, for example.
2) That the undertaking conducts KYC procedures with a regard to updating the customer's identity details less often than for other customers, e.g. less often than for customers with medium or high risk.
3) That the undertaking does not obtain details on the customer's purpose with the business relationship, because it is given in the actual product type, and because the product type is not high risk.
4) That the undertaking monitors the customer to more limited extent than if it monitors a customer with a higher risk profile. But monitoring of the business relationship with the customer cannot be omitted.

Exemption for issuers of electronic money
Issuers of electronic money can be exempted in certain cases from the requirements for KYC procedures in Sections 11, 14 and 18 of the AML Act.

The following cumulative conditions must be met:
1) The payment instrument is not reloadable or has a maximum monthly payment transaction limit of EUR 150, which can only be used in Denmark,
2) The maximum electronic amount stored cannot exceed EUR 150.
3) The payment instrument can only be used for the purchase of goods or services.
4) The payment instrument cannot be financed by anonymous electronic money, and
5) The issuer must perform sufficient monitoring of transactions or business relationships to be able to detect unusual or suspicious transactions.

See also Section 1.4.2. on simplified requirements for the KYC procedure for issuers of electronic money.

17. When KYC procedures must be conducted

Reference to the AML Act's: Section 14 (1)-(4). Reference to the 4th Money Laundering Directive: Article 10 (1) and 14 (1)-(3).

The undertaking must always identify and verify the customer and any beneficial owners before establishing a business relationship with the customer or before any individual transaction is carried out.

However, the undertaking can establish a business relationship with the customer, or perform a transaction in connection with fulfilling the requirements on obtaining details of the customer's purpose and intended nature of the business relationship.

This does presume, however, that the initial KYC procedures intended to verify the identity of the customer or the transaction, have not shown that the customer or transaction have increased risk. If this is the case, the undertaking must perform enhanced KYC procedures before the business relationship is established or a transaction performed.

The undertaking can lay down the requirements for initial customer KYC procedures in relation to the risk of money laundering or terrorist financing associated with the individual business relationship or transaction.

If the business relationship or transaction involves high risk, the undertaking must implement additional measures. The undertaking must follow the requirements laid down by the AML Act for enhanced KYC procedures, e.g. in the event of a business relationship with a PEP. If the business relationship is not covered by the requirement for enhanced customer knowledge in Sections 18 or 19 of the AML Act, the undertaking must conduct the enhanced KYC procedures it deems necessary to counter the increased risk of money laundering and terrorist financing.

KYC procedures must be conducted throughout the customer relationship, i.e. from establishment to the end of the business relationship. KYC procedures can therefore never be terminated before the business relationship is wound up. In the event of customer relationships with limited risk, the undertaking can conduct parts of the KYC procedures, including obtaining details on the purpose and intended nature once establishment is complete.

The undertaking's KYC procedures must always be conducted based on a risk assessment.

17.1. Verifying identity details during establishment of a business relationship

The requirement that the undertaking must always identify and verify the customer before establishing a business relationship or before any individual transaction is carried out can be waived in certain circumstances.

Verifying identity details can be performed during establishment of a business relationship if:

1) it is necessary to avoid interrupting the normal course of business, and
2) there is limited risk of money laundering or terrorist financing.

The two conditions must both be fulfilled before the exemption can apply, and verification of identity details must be completed as soon as possible in such instances.

If it subsequently turns out that verification cannot be performed, the undertaking may be compelled to discontinue or wind up the business relationship. The exemption only allows the initial KYC procedures to be conducted during or after establishment of the business relationship, but they cannot be omitted.

Re.: It is necessary to avoid interrupting the normal business procedure

The term "normal business procedure" is defined as the procedure that, in normal circumstances, is carried out when the undertaking establishes a new business relationship. It is important to note that it requires an assessment of whether it is necessary in a specific situation to postpone verification of identity details.

The exemption allows the undertaking to begin establishing a business relationship for example, such as by opening an account or obtaining information to commence providing advice. However, the undertaking cannot proceed to e.g. perform a transaction or provide advisory services before the identity details of a business relationship have been obtained and verified.

Re.: There is no risk of money laundering or terrorist financing
This condition must be seen in the context of risk assessment the undertaking performs in connection with establishing a new business relationship and the initial KYC procedures. It is a mandatory condition that the process of establishing a business relationship can only be started before identity details have been verified if the business relationship implies limited risk.

17.2. Transactions in securities for a customer

A special exemption applies to the requirement that identity details have to be obtained and verified before establishing a business relationship, when opening an account, deposit account or the like that facilitates transactions in securities for a customer.

If the undertaking has introduced suitable security measures to ensure that the transactions cannot be made before the identity details are obtained and verified, the undertaking can e.g. open the account for transactions in securities.

18. Insufficient details, or details that cannot be updated

If the undertaking becomes aware that details obtained are insufficient and cannot be updated, it must take appropriate measures to counter the risk of money laundering and terrorist financing, including con-

> Reference to the AML Act: Section 14 (5) and (15).
>
> Reference to the 4th Money Laundering Directive: Article 14 (4).

sidering whether the business relationship should be discontinued.

This can, for example, be the case if the undertaking becomes aware during the course of its regular KYC procedures, that the details obtained on a customer are insufficient, or if it wants to update those details as part of its KYC procedures, and the customer refuses to provide them, or if the undertaking cannot contact the customer.

"Appropriate measures" are defined as the undertaking making a specific assessment of which measures should be implemented. The undertaking should always seek to conduct KYC procedures in another manner if there is no specific risk of money laundering or terrorist financing.

Appropriate measures can, for example, be that the undertaking:

b) refuses to offer the customer new products,
c) intensifies monitoring of the customer,
d) sets limits on the customer's transactions, or
e) revokes the customer's commitment or parts of it, e.g. some of the customer's products.

The measures the undertaking initiates must always be proportionate to the specific risk of money laundering or terrorist financing in relation to the customer relationship.

The AML Act does not contain rules for winding up a customer relationship or refusing to enter into new customer relationships. When the undertaking believes that KYC procedures cannot be conducted in

some other way, and that the risk of money laundering and terrorist financing is high, it can either break off or wind up the business relationship. See Section 18.1 below on the duties of undertakings to break off or wind up customer relationships.

18.1. The duties of undertakings to break off or wind up customer relationships

An undertaking only has a duty to break off or wind up a business relationship within the area of money laundering when all options for conducting KYC procedures have been exhausted, on which basis the undertaking has to conclude that it was not possible to conduct the procedures in relation to the business relationship in question.

This means that the undertaking must first seek to conduct the KYC procedures in another manner than its normal procedures.

For example, a customer that refuses to provide its details, or does not possess the type of identification details the undertaking normally gathers in accordance with its normal internal procedures are not sufficient grounds to wind up the customer relationship.

In such situations, the undertaking must determine whether the reason the customer refuses to provide the details can cause a risk of money laundering or terrorist financing. If this is not the case, the undertaking must seek to obtain the details in another manner. This could, for example, be in a situation in which the customer has no officially-issued identification document. In this instance, the undertaking can obtain the customer's birth certificate or equivalent instead.

The duty applied by the AML Act to break off or wind up a business relationship is therefore contingent on it being impossible to conduct KYC procedures, and it is believed there is a risk of money laundering and terrorist financing. The scope of the provision is very limited. In the vast majority of such cases, the undertaking will subsequently have to report to the MLS.

If the undertaking believes that a business relationship must be broken off or wound up, no further transactions or activities can be carried out for the customer. If a fixed loan is involved, it must be redeemed in relation to the redemption profile agreed with the customer. The credit allowance must be revoked, perhaps also in relation to the redemption profile.

Special considerations related to a lawyer's client relationship

The above section on options for breaking off or winding up a customer relationship do not apply to lawyers, when determining the legal position of a client in question, or defending or representing a client during or in connection with a lawsuit, including advising on the initiation of or avoiding a lawsuit.

The exemption will not apply in such instances, because the client's right to legal assistance and legal rights weigh heavier than the intention of gaining sufficient customer knowledge.

However, the purpose of this new provision is not to exempt lawyers from conducting KYC procedures. Lawyers have the same duty to seek to conduct the KYC procedures in another manner, and thus also exhaust all means of doing so.

19. Processing personal data

Reference to the AML Act: Section 16.

Reference to the 4th Money Laundering Directive: Article 43.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 26.

Reference to other legislation: Article 5 (1), letter b, (13) and (14) of the General Data Protection

Personal data obtained for the purpose of meeting the requirements of the AML Act must be processed in accordance with the data protection law rules that in principle apply to the processing of personal data carried out in whole or in part by means of automatic data processing. "Personal data" is defined as any form of data on an identified or identifiable natural person.

This means that the requirement in Article 5 (1) letter b of the General Data Protection Regulation must be complied with. The data collected must therefore not be further processed in a way that is incompatible with the explicitly stated and legitimate purposes for which it was collected.

Furthermore, the rules in e.g. Articles 13 and 14 of the GDPR on the right to be informed must be complied with. If personal data is collected about a data subject – for example a customer – the undertaking must provide the data subject with information on the purposes of the processing for which the personal data are to be used, the legal basis for the processing and details of any recipients or categories of recipients of the personal data.

If the customer is a natural person, the undertaking must inform the customer about the rules governing the processing of personal data with a view to preventing money laundering and terrorist financing before establishing a business relationship or executing a single transaction. The requirement does not apply if the customer is a legal person.

All personal data, including, for example, the customer's name and CPR number, or on the customer's beneficial owners, which the undertaking obtains according to the AML Act, can only be processed by the undertaking in accordance with the AML Act. Personal data cannot therefore also be used in other contexts by the undertaking.

The undertaking must thus inform the data subject about why it gathers data on the person in question when it conducts its KYC procedures.

Part 4 – Assistance from third parties and outsourcing

20. Assistance from third parties

Reference to the AML Act: Section 22 (also cf. Section 9 (2)). Reference to the 4th Money Laundering Directive: Articles 25-27. Reference to the 5th Money Laundering Directive: Article 1 (1), no. 14. Reference to other legislation: Article 28 (3) and Chapter 5 of the General Data Protection Regulation.

Undertakings can outsource the obtaining and verification of data to a third party in accordance with Section 11 (1), nos. 1-4. See section 23 on the distinction between Sections 22, 23 and 24. The possibility of third party assistance assumes that certain conditions are met, cf. below.

The undertaking can receive assistance from a third party if it:

1) is covered by Section 1 (1) of the AML Act, or
2) is a similar undertaking or person to those undertakings or persons listed in Section 1 (1) established in an EU or EEA member state or a similar undertaking or person in other countries subject to requirements to combat money laundering and terrorist financing equivalent to the requirements arising from the 4th Money Laundering Directive, and is subject to supervision by an authority, or
3) is a trade organisation or association of undertakings and persons mentioned in nos. 1 and 2, and is subject to requirements for combatting money laundering and terrorist financing which correspond to the requirements of the 4th Money Laundering Directive, and the trade organisation or association is subject to supervision by an authority.

Re. 1: Section 1 (1) of the AML Act:
An undertaking can receive assistance from a third party if that third party is covered by Section 1 (1) of the AML Act. This means that all undertakings and persons covered by the AML Act can enter into an agreement to provide assistance under Section 11 (1), nos. 1-4. This includes details derived from a risk assessment from/on the customer to implement KYC procedures.

This means that the information obtained by third parties to comply with Section 11 (1), nos. 1-4, is covered by the provision for assistance from third parties, and the details can therefore be used by the undertaking.

Re. 2: Assistance from a third party established in the EU/EEA:
The undertaking can also receive assistance from a third party if it is established in another EU/EEA member state or in other countries subject to anti-money laundering and terrorist financing. But this is contingent on the third party being an undertaking or person equivalent to those undertakings and persons covered by the AML Act, and that the undertaking is subject to requirements for combatting money laundering and terrorist financing which correspond to the requirements of the 4th Money Laundering Directive. In addition, third parties must be subject to supervision ensuring compliance with the rules.

If these requirements are fulfilled, the undertaking can use the details obtained on a customer's identity in the same manner as if the third party were established in Denmark. However, the undertaking must be aware that the undertaking itself is responsible for assessing whether the third party is subject to requirements that correspond to the 4th Money Laundering Directive. See Section 20.2 on responsibility. Furthermore, the undertaking must be able to justify such an assessment to the supervisory authority supervising the undertaking in Denmark, and should therefore also document the third party's assessment.

Re. 3: Assistance from a third party, a trade organisation/group of undertakings/persons:
The undertaking can also receive assistance from a third party that is a trade organisation or a group of undertakings or persons of the same type referred to under nos. 1 and 2. When the undertaking receives assistance from such a third party, it must ensure that it is subject to requirements on anti-money laundering and terrorist financing equivalent to those in the 4th Money Laundering Directive. The undertaking must ensure this before it uses the details obtained by the trade organisation or association.

When can the undertaking receive assistance from a third party?
The undertaking can receive assistance from third parties in situations when the customer is a customer of the third party and is, or will also be, a customer of the undertaking, and when the third party has already conducted KYC procedures in relation to the customer. This means that the information the third party has obtained on the customer can be reused by the undertaking.

It is not a requirement that the third party is the same undertaking type as the undertaking itself. This means, for example, that a bank can act on details of a customer's identity obtained from an accountant or provider of payment services. The decisive factor is that this third party is in compliance with the AML Act, and has the natural or legal person concerned as a customer.

The undertaking can receive assistance in obtaining details for its general KYC procedures in Section 11 (1), nos. 1-4. This means that the undertaking cannot receive assistance to obtain additional details to meet enhanced KYC procedures, including Sections 17, 18 and 19. Therefore, when an undertaking considers a customer high-risk, the undertaking itself must obtain details that supplement those provided by the third party, and implement other enhanced measures.

However, pursuant to Section 18, third parties can inform the undertaking that a customer is a PEP, family member or close associate to a PEP, whereupon the undertaking itself must conduct enhanced procedures in accordance with Section 18.

Note that if an undertaking uses commercial providers of PEP lists, it is not third party assistance according to Section 22. See Section 15 on politically exposed persons (PEPs).

The undertaking itself must perform risk assessment of the customer
The undertaking itself must perform risk assessment of the customer, and must therefore be aware that the same customer may have different risk profiles relative to the third party and in relation to the undertaking. This may be due to differences in business model, geographical location, etc., between the third party and the undertaking.

The undertaking may therefore need to obtain identity or verification details that complement those received from the third party.

The undertaking must also be aware that a third party's assessment of whether details need to be obtained on the customer's purpose and intended nature of the business relationship to the third party's undertaking are identical with the undertaking's own assessment and relationship to the customer.

The purpose of the business relationship and its intended nature can be assessed based on the service or product that the customer wants, for example. Assessment of whether the client's purpose and the intended nature needs to be known must be specific.

The undertaking may therefore need to obtain information about the purpose and the intended nature itself, if the third party has not obtained such information, or obtain information that complements that received from the third party.

20.1. Conditions

If the undertaking wishes to have a third party obtain details on the undertaking's customer or the customer's identity, the undertaking must do the following before entering into an agreement:

- Obtain sufficient details on third parties,
- Ensure that a third party undertakes to immediately forward a copy of identity and verification details upon request on the customer or customers, the beneficial owner (if any), along with other relevant documentation and data to the undertaking covered by the Act.

Re.: Obtain sufficient details on third parties:
The undertaking must obtain sufficient information to determine whether the third party meets the requirements for KYC procedures and record keeping. It is the undertaking's responsibility to determine what is sufficient.

"Sufficient information" is defined, for example, as the undertaking obtaining a statement from the third party describing the procedures the third party introduced to comply with the KYC procedures. The undertaking can, for example, also obtain the third party's policies and business procedures concerning customer knowledge in accordance with Section 11 (1)-(4), and record keeping of data according to Section 30.

In addition, it will be relevant to obtain information about whether third parties have received instructions from the supervisory authority in relation to customer knowledge requirements. If this is the case, the undertaking can investigate whether the instructions have been followed.

It can also be relevant for the undertaking to make random sample checks on the third party's business relationships.

Re.: Ensure that a third party undertakes to immediately forward a copy of identity and verification details upon request on the customer or customers, the beneficial owner (if any), along with other relevant documentation:
This condition is relevant because the undertaking that needs the information before establishing a customer relationship must conduct an independent risk assessment of the customer. The risk assessment must include taking into consideration the products or services offered by the customer.
Furthermore, the third party must undertake to immediately forward relevant verification documents and other relevant documentation and data on request to the undertaking or person subject to the Act, as well as proof that it complies with the requirements for record keeping in the 4th Money Laundering Directive.

This means that the undertaking must have the information obtained in accordance with Section 11 (1), nos. 1-4 available, when it has to perform a risk assessment of the customer. However, it is not necessary for the undertaking to also have the verification documents available at this time, as they can be forwarded by a third party at the request of the undertaking at any time.

The need for the aforementioned information to be provided immediately follows the purpose of the rules on KYC procedures. The KYC procedures will help ensure effective investigation, including by quickly allowing the undertaking or person to quickly be able to provide the necessary details on the customer or its beneficial owner's identity etc. to the investigative authorities.

It is therefore necessary that the obligations of third parties appear from the contract to which the undertaking subject to the Act enters into with third parties.

20.2. Responsibility

An undertaking using identity details obtained from third parties is responsible for compliance with the requirements of the AML Act. The undertaking cannot be exempted from responsibility when receiving assistance from third parties, and is therefore responsible for conducting KYC procedures itself, including obtaining details on the customer in accordance with the AML Act.

The undertaking is also responsible for conducting correct risk assessment of its customers, including determining what the risk assessment requires in terms of customer knowledge, customer monitoring, etc. in accordance with the AML Act.

If a customer or customer group is assessed to be high-risk, the undertaking must ensure that it conducts enhanced KYC procedures. In principle, it will be necessary to obtain sufficient additional details on that customer or customer group.

The undertaking's responsibility therefore means that it must ensure sufficient knowledge of the third party able to assure the undertaking that fulfilment of Section 11 (1), nos. 1-4 by the third party is effective. It is thus the undertaking that has to explain to the supervisory authority the adequacy of its customer knowledge.

If the undertaking concludes a long-term agreement with a third party to use the information the third party obtains pursuant to Section 11 (1), nos. 1-4, the undertaking should conduct regular checks to ensure that the third party obtains sufficient identity details on the customers. Furthermore, the undertaking must verify that the details are usable and easily accessible, and that the undertaking can receive a copy upon request without delay.

The undertaking, which assists as a third party, remains responsible for its own compliance with the AML Act.

Finally, the undertaking must pay particular attention to compliance with data protection rules in connection with the processing of personal data by third parties. If a third party is a data processor – which means a natural or legal person, a public authority, an institution or other body that processes personal data on behalf of the data controller – the undertaking must therefore be aware of the specific requirements contained in the data protection rules.

This implies, inter alia, that a data processing agreement with the data processor must be concluded. Data processing agreements must be concluded between the data controller and the data processor, and must comply with the requirements of the General Data Protection Regulation.

Refer to the Danish Data Protection Agency's guides on "Data Controllers and Data Processors", as well as "Data Processors and Subcontractor Data Processers", available on the Agency's website (www.datatilsynet.dk).

20.3. Third party established in a high-risk country

The undertaking cannot avail itself of the possibility of assistance from a third party if that third party is established in a country which is included on the European Commission's list of high-risk third countries.

However, this will not apply if the third party is a majority-owned subsidiary or branch established in such a high-risk third country, but when the entity that established the subsidiary/branch is established in an EU/EEA member state, and contingent on the subsidiary/branch fully complying with the group's policies and business procedures. See Part 2 – Risk assessment and management.

If the undertaking wants to use a subsidiary/branch it owns to assist in fulfilment of Section 11 (1), nos. 1-4, the undertaking must obtain information in addition to the conditions described in Section 20.1 that provide assurance that the subsidiary/branch fully complies with the group's policies and procedures.

21. Group relationships

Reference to the AML Act: Section 23. Reference to the 4th Money Laundering Directive: Article 28.

Undertakings that are part of a group can task another undertaking in the group to comply with the requirements of Section 11 (1), nos. 1-4. This includes obtaining details from/on the customer based on risk assessment to conduct KYC procedures. The term "group" is defined in accordance with the Companies Act's definition of group. It is a prerequisite that the group, in accordance with the 4th Money Laundering Directive:

1) uses KYC procedures,
2) has rules on the storage of data and programs to combat money laundering and terrorist financing, and
3) that an authority supervises compliance with the requirements of the 4th Money Laundering Directive at group level.

If an undertaking in a group uses another undertaking in the group as a third party, the group must comply with the three points listed above, whereupon the undertaking will be regarded as complying with the requirements for third party assistance in the AML Act. In addition to groups, the same options apply internally in undertakings consisting of a parent undertaking and one or more branches established in other countries, so that a unit outside Denmark is responsible for fulfilment.

"Programs for combatting money laundering and terrorist financing" are defined as the group's policies and business procedures in the money laundering area. See Section 4 on policies, business procedures and controls.

The requirement that group-level supervision be conducted should be understood as ensuring that one or more supervisory authorities supervise compliance with the requirements for KYC procedures, record keeping rules and programs for combatting money laundering and terrorist financing. To include that the supervisory authority in the parent undertaking's home country supervises the group's policies and business procedures to ensure effective compliance with these requirements.

The purpose of the provision is that repeated KYC procedures in a group do not entail unnecessary delays or administrative costs. The provision on assistance from another undertaking within a group therefore means that the conditions differ to some extent from the requirements of Section 22. See Section 20 on assistance from third parties.

The information that another undertaking in the group has obtained to comply with Section 11 (1), nos. 1-4, is covered by the provision, and can therefore also be used for the undertaking's fulfilment of the requirements for KYC procedures.

According to this provision, another undertaking in the group can assist in conducting enhanced KYC procedures pursuant to Sections 17-19. The other undertaking in the group can also assist in conducting a risk assessment of the customer. But it is important to note that risk assessment must always be performed in relation to the specific customer, including the inclusion of risk factors such as the product or service the customer is offered, geographical factors, scope and duration of the business relationship with the customer etc. See Section 13 on risk assessment – KYC procedures.

The undertaking that assists with conducting KYC procedures is part of the group, and because the undertaking that makes use of assistance from the group undertaking has ensured that the group fulfils the three conditions listed in this section, there is no requirement for the undertaking to obtain additional details on the group undertaking.

22.Outsourcing

Reference to the AML Act: Section 24.

Reference to the 4th Money Laundering Directive: Article 29.

Reference to other legislation: Executive Order no. 877 of 12 June 2020 on outsourcing for credit institutions, etc.

Reference to other legislation: Article 28 (3) and Chapter 5 of the General Data Protection Regulation.

An undertaking can opt to contractually outsource tasks to another undertaking (hereinafter referred to as the supplier), to comply with the requirements of the AML Act. See Section 23 on the differences between Sections 22, 23 and 24.

Such tasks can include:

1) Obtaining identity and verification information for use in the undertaking's KYC procedures.
2) Monitoring customer transactions.
3) Record keeping etc.
4) Reporting.

The supplier does not need to be covered by the AML Act.

All tasks arising from the AML Act can be outsourced as a rule. However, the undertaking can never outsource responsibility arising from the AML Act. See Section 20.2 on responsibility. The undertaking must be aware that the task in Section 7 (2) of the AML Act cannot be outsourced, i.e. the undertaking's responsibility to appoint an AML Officer can only be fulfilled by the undertaking itself. Similarly, the responsibility of the AML Officer cannot be outsourced. See Section 6.1 on AML Officers.

Undertakings subject to the Executive Order on outsourcing must be aware that in some instances, the Executive Order can lay down stricter requirements than those in the AML Act, which the undertaking must fulfil. Undertakings subject to the Executive Order on outsourcing must determine whether the activity is covered by the Executive Order.

22.1. Conditions

The option for an undertaking to outsource tasks to another undertaking to comply with the requirements of the AML Act is contingent on the fulfilment of certain requirements before a contract can be concluded with a supplier.

Before the undertaking concludes an outsourcing agreement with the supplier, it must ensure that:

1) the supplier has the required ability and capacity to perform the task satisfactorily
2) the supplier has the necessary authorities.

This means that the supplier must have relevant and professional knowledge of the task, and have sufficient resources to undertake it.

If the supplier is not established in Denmark, the undertaking must specifically focus on ensuring that the supplier has the necessary authorisations required for the relevant activity. In addition, it is relevant to ensure that the supplier has the necessary knowledge of national legislation to be able to fulfil the conditions in the same way as a supplier established in Denmark.

22.2. Who can an undertaking outsource to in accordance with the AML Act?

There is no requirement in the AML Act as to whom an undertaking can outsource tasks. This means that there is no requirement that the supplier be covered by the AML Act.

The supplier is therefore not a defined group of persons and undertakings, as is the case in Sections 22 and 23 of the AML Act.

For example, a supplier could deal in goods for which the customer/buyer is offered financing by the undertaking. In such instances, the undertaking can contract the dealer in connection with the sale for the dealer to obtain details of the customer's identity and control sources the undertaking needs for its risk assessment of the customer.

22.3. Checking the supplier

When the undertaking has entered into an agreement with a supplier regarding outsourcing of tasks, the undertaking must continuously check on the supplier.

Before the agreement is concluded, it is therefore important that the undertaking ensures it is possible to carry out the relevant checks on an ongoing basis.

Checks must ensure:

1) that the supplier lives up to the obligations arising from the agreement with the undertaking, and
2) that the outsourcing agreement with the supplier is still sound.

When the undertaking has to determine whether the outsourcing agreement is still sound, it must do so on the basis of the obligations incumbent on the undertaking. This means that by using the supplier, the undertaking must ensure that it fully meets the requirements of the AML Act in the same manner as if the undertaking itself performed the tasks, in accordance with the AML Act.

22.4. Responsibility

The undertaking can never outsource its responsibility. This means that the undertaking is always fully responsible for compliance with the obligations of the undertaking under the AML Act and other relevant legislation in the area. The undertaking will always be fully responsible for compliance.

"Other relevant legislation" can include EU regulations in the area of money laundering, data protection legislation, etc.

When an undertaking chooses to outsource a task for compliance with the AML Act, the supplier will be considered as part of the undertaking. Responsibility for the task to be carried out in accordance with the requirements of the AML Act is the responsibility of the undertaking.

Therefore, the undertaking is also responsible for ensuring that the supplier follows the necessary procedures for combatting money laundering and terrorist financing when working on behalf of the undertaking.

If outsourcing, the undertaking must be aware of the impact on its risks, and thus the residual risk the undertaking has after compiling its policies in the whitewashing area. For example: it can affect the risk profile if the undertaking outsources a task to an undertaking established outside Denmark, which has a lower regulation level than Denmark, and where there is insufficient supervision for combatting money laundering and terrorist financing, or, conversely, if the undertaking outsources a task to an undertaking that specialises in this kind of work and therefore can do so more effectively than the undertaking itself.

Finally, the undertaking must pay particular attention to compliance with data protection rules in connection with the processing of personal data by third parties. If a third party is a data processor – which means a natural or legal person, a public authority, an institution or other body that processes personal data on behalf of the data controller – the undertaking must therefore be aware of the specific requirements contained in the data protection rules.

This implies, inter alia, that a data processing agreement with the data processor must be concluded. Data processing agreements must be concluded between the data controller and the data processor, and must comply with the requirements of the General Data Protection Regulation.

Refer to the Danish Data Protection Agency's guides on "Data Controllers and Data Processors", as well as "Data Processors and Subcontractor Data Processers", available on the Agency's website (www.datatilsynet.dk).

23. Overview of the possibility of assistance from third parties, other undertakings and by outsourcing

Below is a diagram comparing the possibility of third party assistance for the standard KYC procedures and outsourcing to another undertaking (supplier) for tasks based on the requirements of the AML Act.

	″**Section 22.** Assistance from third parties for KYC procedures.	**Section 23:** Assistance from another group undertaking for KYC procedures.	″**Section 24.** Outsourcing of tasks for compliance with the AML Act.
When is the option relevant?	When the undertaking and third party have the same customer(s), and identity/verification details etc. can be reused.	When two or more undertakings in the same group have the same customer(s), and identity/verification details etc. can be reused.	When the undertaking sees the benefit of another undertaking performing specific tasks.
Contents	The undertaking can outsource obtaining and verifying details pursuant to Section 11 (1), nos. 1-4 to another undertaking (third party). The undertaking itself must conduct a risk assessment of the customer, including enhanced KYC procedures when necessary.	The undertaking can outsource obtaining and verifying details pursuant to Section 11 (1), nos. 1-4 to another group undertaking (third party). That group undertaking can also assist with risk assessment of the customer, and conducting enhanced KYC procedures if relevant.	The undertaking can outsource tasks to another undertaking (supplier) for compliance with the AML Act.

Purpose	The undertaking can reuse information obtained for use in KYC procedures.	KYC procedures do not need to be conducted twice within a group.	The undertaking can optimise its operations by outsourcing relevant tasks.
To whom and when	The third party must be an undertaking or person covered by Section 1 (1) of the AML Act. 1 or a similar undertaking/person in another country subject to similar requirements for combatting money laundering and terrorist financing.	The third party must be an undertaking within the group that has already obtained such details, and that complies with the group's business procedures and policies.	There is no requirement as to which undertaking or person the supplier is.
Responsibilities	The undertaking must obtain sufficient information about third parties and ensure that they can provide identity and verification details.	The undertaking must ensure that the group uses KYC procedures, has rules on record keeping and programs to combat money laundering and terrorist financing and is subject to supervision in the area.	The undertaking must check the supplier. The undertaking must ensure that the supplier has the necessary ability, capacity, authority and knowledge, both professionally and legally.
Responsibility	The undertaking is responsible.	The undertaking is responsible.	The undertaking is responsible.

Part 5 – Duty to investigate, register, report and keep records

24. Duty to investigate

Reference to the AML Act: Section 25 (1) and (2).

Reference to the 4th Money Laundering Directive: Article 18 (2).
Reference to the 5th Money Laundering Directive: Article 1 (10), letter b.

Section 25 (1) of the AML Act concerns the duty of undertakings to investigate the background and purpose of transactions, transaction patterns and activities when there may be a suspicion or reasonable cause to believe that they are, or have been, linked to money laundering or terrorist financing.

The purpose of investigation is to determine whether there is a suspicion or reasonable cause to suspect that a transaction or activity is, or has been, linked to money laundering or terrorist financing. This means that undertakings must have business procedures and systems in place that make it possible to identify such transactions and activities.

Undertakings must thus investigate the background and purpose of all transactions, transaction patterns and unusual activities that are complex, unusually large, carried out in an unusual pattern or do not have an obvious economic or legal purpose.

Criterion: "are complex"
When assessing whether a transaction is complex, the undertaking can e.g. focus on whether the transaction involves multiple parties or multiple jurisdictions, or whether the transaction allows the customer to receive payments from an unknown third party.

Criterion: "are unusually large"
The undertaking can assess whether a transaction is unusually large based on e.g. knowledge of the specific customer, including the customer's transaction patterns and product portfolio.

Criterion: "are carried out in an unusual pattern"
The undertaking can take the usual behavioural patterns of the customer and customer type as a starting point when assessing whether a transaction is made in an unusual pattern. Among other things, focus here can be placed on the size of the customer's usual transactions, how large the funds received are, etc.

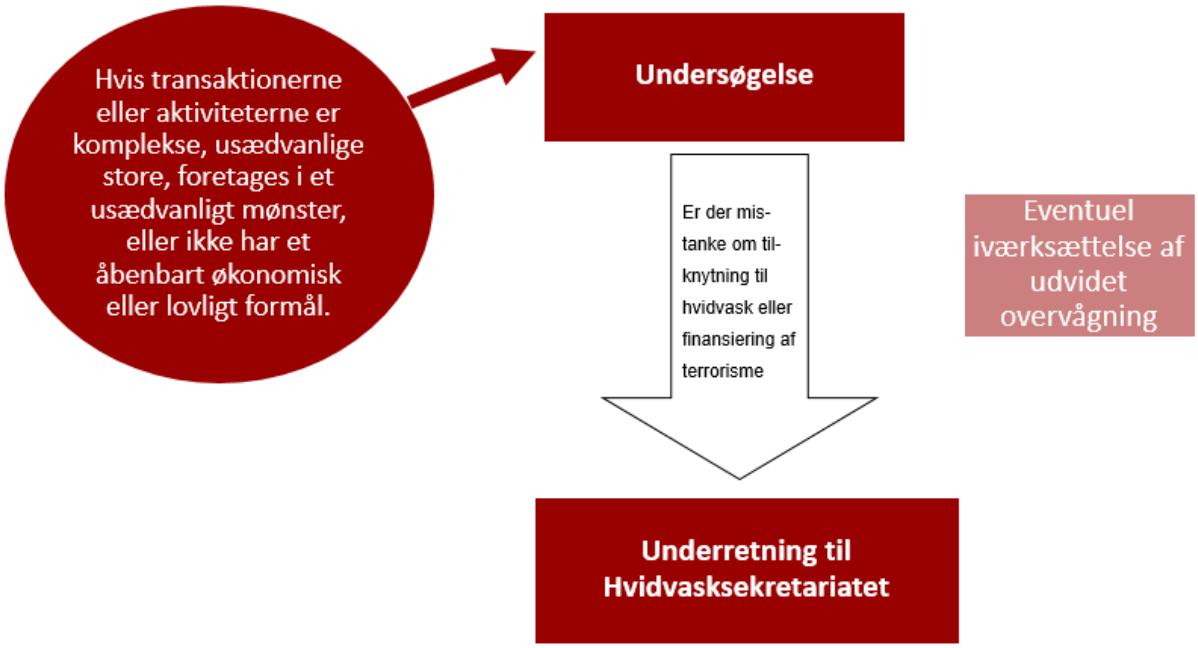
Criterion: "do not have an obvious economic or legal purpose"
If the transaction or activity does not have a clear economic or legal purpose, the undertaking must investigate the reason. Undertakings can, for example, focus on who the customer usually receives funds from, to whom the customer transfers money and the customer's transaction pattern. Forwarding or receiving a customer's funds when it is not clear what the economic purpose is can result in investigation of where the funds are going or where they come from.

For example: a customer who normally only receives funds from an employer who suddenly receives funds from an unknown third party, when it is not clear that the funds are part of a salary or the like.

Another example may be that a customer suddenly starts making a number of investments that clearly deviate from the previous investment pattern, e.g. because there are many more than usual, and the amounts are larger than the investments that the customer usually makes. A customer's unwillingness to provide information or an explanation of e.g. an increasing number of investments or a change in investment pattern can also be included in assessment of whether there are unusual activities.

The undertaking must have procedures and systems to make it possible to identify such transactions and activities.
If it is clear from the customer's behaviour that the undertaking is aware of money laundering or terrorist financing, a report can be made directly without having to conduct an actual investigation.

The following figure illustrates the process from the duty to investigate to duty to report and possible initiation of enhanced customer monitoring.



When assessing unusual conduct, the undertaking must use the details it has on the customer, including on the purpose and intended nature of the business relationship. Details on scope and expected cross-border activity can also be included. Such information should be compared with what seems suspicious. Banks and other undertakings that have customer managers may find it relevant to involve them with regard to knowledge of the customer.

The undertaking could also include information from publicly available sources, such as internet searches, if deemed to be a reliable and independent source.

It may be necessary for the undertaking to contact the customer to obtain additional information on the purpose of the transaction or activity. However, the customer's verbal explanation may not be sufficient to disprove a suspicion in many cases. It may therefore be necessary to ask the customer to substantiate an explanation, for example, with documentation in the form of:

1) A sales contract for the sale of a car.
2) A probate court or estate inventory certificate.
3) A purchase agreement from a property sale.
4) A sales contract from the sale of a business.
5) An annual statement for savings/net worth.
6) One or more pay slips from employment.

The undertaking's investigation should be designed to determine the following:

1) **Who** is the customer?
2) **What** does the customer look like?
3) **What** does the customer want?

4) **Where** will the transaction/activity be performed?
5) **When** should the undertaking perform transactions or activities for the customer?
6) **How** will the transaction/activity be performed?
7) **Why** is the customer doing this?

If the undertaking believes that an enquiry will inform the customer that the undertaking is suspicious and is in the process of conducting an investigation, or if the undertaking deems it inappropriate to contact the customer on the matter, the undertaking must report to the MLS. If the undertaking cannot completely disprove its suspicion, notification must also be made. The undertaking must be aware that the requirement implies that suspicion must be disproved if no notification is required. It is therefore not enough that suspicion has only been reduced. See Section 25 on the duty to report to the MLS.

The duty to investigate requirement must be seen in connection to the duty to report to the MLS. The undertaking must base its report to the MLS on assessments made concerning the specific situation in relation to:

1) the nature of the actions and deviation from normal customer actions
2) non-disclosure and other unusual and atypical behaviour by the customer.

If the undertaking's investigations (including questions about purpose, etc.), give the customer the opportunity to halt the transaction or activity, the suspicion has not been disproved. In fact, it could confirm the suspicion, and the undertaking should then report to the MLS.

24.1. Enhanced monitoring

When it is relevant, the undertaking must enhance monitoring of a business relationship in the event of a suspicion or reasonable grounds to suspect that a transaction or activity is, or has been, associated with money laundering or terrorist financing.
Consequently, the undertaking must, where appropriate, enhance customer monitoring with the aim of determining whether the transactions or activities appear suspicious. This means that the undertaking must assess whether enhanced monitoring of the customer is needed based on risk. This will be relevant, for example, when a report is given to the MLS.

Enhanced monitoring of a customer can involve:

1) That the undertaking adjusts automated monitoring of the customer so that the thresholds for when an alarm is triggered in the undertaking's monitoring system will be lowered.
2) That the undertaking focuses more on the customer's behaviour, including enquiries, activities, etc. For example: flagging the customer's profile internally to attract attention to a particular type of behaviour by the customer.
3) That the undertaking manually reviews the customer's relevant transactions on a regular basis.

In some specific customer relationships, regular monitoring can be part of a service provided, if that service provides insight into the customer's circumstances. This applies, for example, to an auditor's statement, including reviews of the customer's financial circumstances. Information obtained during execution of such tasks can be included in the undertaking's compliance with the AML Act's requirements for regular monitoring. In such instances, the undertaking must record and keep materials, documentation etc. in accordance with the requirements of the AML Act.

The undertaking must also be aware that it has to conduct KYC procedures when a customer's relevant circumstances change. See Section 8.2.

24.2. Duty to register

Reference to the AML Act: Section 25 (3).

Reference to the 4th Money Laundering Directive: Article 40.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 25.

The undertaking must register and keep the results of investigations conducted as part of a business relationship or an individual transaction, along with any other details received from the customer. See Section 26 on the record keeping.

The duty to register covers factual information on the customer and transaction, along with a conclusion to the investigation. The registration must be sufficient to refresh the memory and provide an understanding of the matter to others, including other employees and the police. As such, recording a individual words such as "business travel", or "casino" will be insufficient in connection with the investigation of a suspicious transaction or activity.

The information recorded can include:

1) The customer's explanation of the purpose of the transaction or activity.
2) Documentation for the customer's explanation.
3) An explanation from other relevant employees in the undertaking, such as the customer manager.

The duty to register the results of investigations applies to investigations in which the undertaking notifies the MLS, and those in which the undertaking fully disproves a suspicion, and therefore makes no notification.

24.3. Limitation of the right of access

Reference to the AML Act: Section 25 (4).

Reference to the 4th Money Laundering Directive: Article 40.

A data subject is not entitled to access into their own personal data that has been or will be processed in connection with an investigation on suspicion of money laundering and terrorist financing. That means that the subject has no right of access to the undertaking's investigations in progress and already completed. See Section 31 on duty of confidentiality.

25. Duty to report

Reference to the AML Act: Section 26 (1) and (5).

Reference to the 4th Money Laundering Directive: Article 33.

A report must be made to the MLS10 if the undertaking knows or suspects or has reasonable reason to suspect that a transaction or activity is or has been associated with money laundering or terrorist financing. The same applies if undertakings covered by Section 1, no 9 of the AML Act on the subsidiaries etc. of foreign undertakings. For example: a report concerning a customer of a subsidiary of a foreign undertaking in Denmark must be given to the MLS.

The MLS must be notified immediately. The undertaking must thus deal with suspicious transactions and activities in a manner that accelerates the process as much as possible. "The process" is defined as the stage from monitoring customer transactions and detecting something suspicious, to investigation and determining that the suspicion can be regarded as confirmed.

The duty to report also applies in connection with *attempts* to carry out a transaction or a request from a potential customer that wants to perform a transaction or activity. Refused requests must therefore also be reported if the undertaking considers that there is an attempt at money laundering or terrorist financing involved.

In instances involving a potential new customer, the undertaking should not conduct KYC procedures if there is a risk of the customer becoming aware that a report has been made to the MLS. However, it may still be possible to identify the person in some instances on different grounds, e.g. information or documents received from the potential customer.

It is not intended that anyone subject to the duty to report should make a detailed criminal assessment of the relationship. The undertakings and persons subject to the Act must, on the other hand, look into whether there are atypical conditions in relation to normal customer relationships, including whether the transaction concerns amounts or payment methods that appear to be atypical in the specific context.

Situations can occur when nothing appears atypical concerning a given transaction or activity, but that the undertaking or person is in possession of other information that specifically gives rise to suspicion.

A report is not an accusation, and the duty to report cannot be fulfilled by the undertaking making a report to the police. If an actual criminal offence is involved, a report can of course be made to the relevant police district.

The undertaking has a duty of confidentiality concerning a report given or considered. This means that a data subject has no right of access to reports made to the MLS concerning themselves. See Section 31 on duty of confidentiality.

10 The MLS is an operationally independent and autonomous unit, under the Danish State Prosecutor for Serious Economic and International Crime (SØIK). The MLS is tasked with receiving and analysing notifications of suspicious transactions and other information relevant to money laundering, related underlying crimes or terrorist financing.

The AML Act takes preference over Section 22 (1) of the Act on Approved Auditors and Audit Firms (the Auditor Act).
For approved auditors, the rules in Section 22 (1) of the Auditor Act. are not applicable to matters covered by the AML Act.

Note that the rules of the AML Act on the duty of confidentiality imply that in certain instances, auditors cannot notify the management or include details in their audit protocol as laid down in Section 22 (1), paragraphs 1 and 2 of the Auditor Act.

25.1. Violations of the ban on cash transactions

If an undertaking's customer violates the ban on cash transactions, it will be an unusual or suspicious activity in principle. In such instances, the undertaking must investigate the activity to determine whether to report to the MLS. If the undertaking cannot disprove that money laundering or terrorist financing is involved, it should be reported. See Section 2.3 on the ban on cash transactions.

25.2. Limitation of the right of access

A data subject is not entitled to access into their own personal data that has been or will be processed in connection with a report to the MLS on suspicion of money laundering and terrorist financing. This means that the data subject has no right of access into the undertaking's reports according to the AML Act with regard to reports given or considered. See Section 31 on duty of confidentiality.

25.3. Exemptions to the duty to report.

Reference to the AML Act: Section 27 (2)-(4). Reference to the 4th Money Laundering Directive: Article 33.

Certain undertakings, including auditors, are exempted from the duty to report in exceptional cases.

The exemption does not apply if the undertaking knows or ought to know that the customer is seeking assistance with regard to money laundering or terrorist financing.

Approved auditors
Audit companies and auditors approved in accordance with audit legislation are exempted from the duty to report in relation to information they receive from or obtain on a customer (client) when representing that customer at the National Tax Tribunal.

The exemption applies regardless of whether the information from the customer is obtained prior to, during or after proceedings.

Assistance to lawyers
The undertakings referred to Section 1 (1), nos. 14-17 of the AML Act (including approved auditors, tax advisors and bookkeepers) are exempted from the duty to report to the same extent as lawyers when they assist a lawyer before, during and after a court case, or when determining the legal position of a lawyer's client.

25.4. The undertaking's duty to refrain from conducting transactions.

Reference to the AML Act: Section 26 (3) and (4). Reference to the 4th Money Laundering Directive: Article 35.

Suspected money laundering
Until a report has been made, the undertaking must refrain from conducting transactions if is aware of, suspects or has reasonable grounds to suspect that a transaction or activity is related to money laundering. This requirement only applies if the transaction has not already been completed, for example, for faster payment transfers, when the transaction will often be completed before the undertaking becomes aware or suspects that the transaction is linked to money laundering.

The figure below illustrates the process for refraining from performing transactions in cases of suspected money laundering.

If it is not possible to refrain from completing the transaction, or if the undertaking believes that completing the transaction could harm the investigation, a report must be made it has been completed.

Suspected terrorist financing
If the undertaking is aware of, suspects or has reasonable grounds to assume that a transaction concerns terrorist financing, it must refrain from performing the transaction until it has received approval from the MLS.

The MLS will decide whether a transaction can be performed as soon as possible.

The figure below illustrates the process for refraining from performing transactions in cases of suspected terrorist financing.

25.5. Formal requirements for reporting to the MLS

Reference to the AML Act: Section 26 (6). Reference to other legislation: Executive Order no. 1403 of 1 December 2017 on the submission of reports, etc. to the State Prosecutor for Serious Economic and International Crime.

Undertakings must report a suspicion of money laundering or terrorist financing to the MLS digitally.

In principle, reports must be in Danish. If this is not possible, the report can be written in English.

Reports must be made in XML format via www.hvidvask.dk. The undertaking must check whether the report has been accepted or rejected before the end of the following banking day.

In the event of IT problems, such as breakdown or temporary reduction in capacity problems causing www.hvidvask.dk to be inaccessible for 8 successive hours between the hours of 08.00 and 16.00 on weekdays, reports must be submitted in XML format by email or other electronic media by agreement with the MLS. However, this does not apply to scheduled shutdowns for updating that have been announced in advance on the website, and when the announcement's instructions are followed.

For more details on reporting, including the requirements for XML format, refer to the MLS' user guides on www.hvidvask.dk11.

26. Record keeping

Reference to the AML Act: Section 30. Reference to the 4th Money Laundering Directive: Articles 40-43. Reference to the 5th Money Laundering Directive: Article 1 (1), nos. 25 and 26.

The undertaking is required to keep the following information:

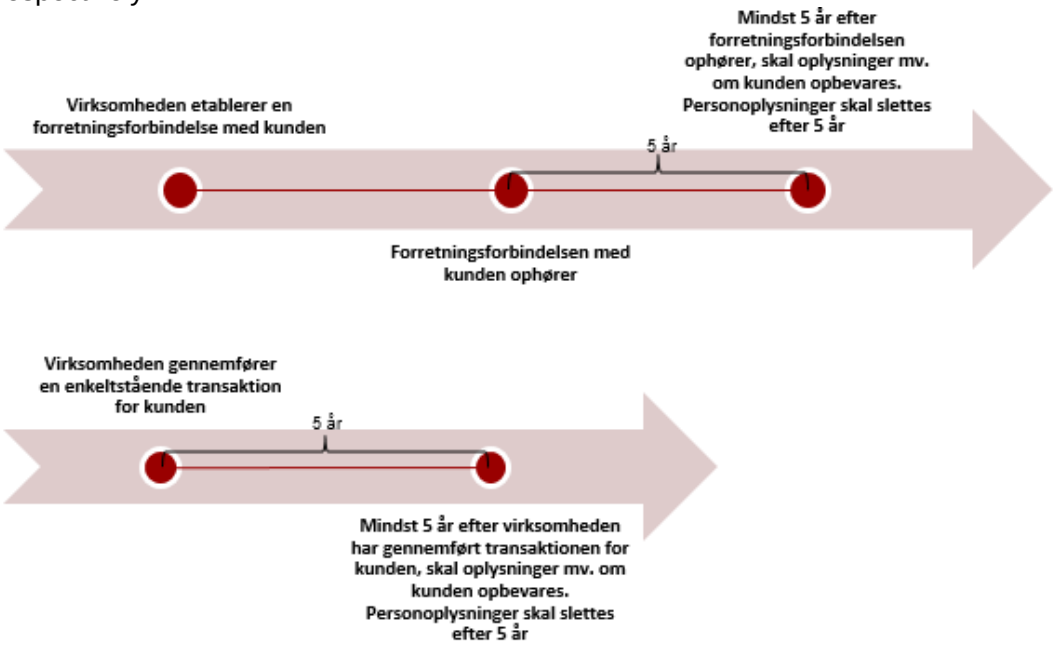
1) All information obtained in connection with KYC procedures, including the identity and verification details obtained and copies of identity details presented.
2) Documentation and records of transactions carried out as part of a business relationship or an individual transaction.

11 http://www.anklagemyndigheden.dk/da/brugervejledninger

3) Documents and registrations in connection with the duty to investigate and record.

The undertaking must keep such information for at least 5 years after the end of the business relationship, and for individual transactions, at least 5 years after the transaction has been completed.

The following figures illustrate the record keeping requirements for business and individual transactions respectively.



Re. 1)
"Identity details" refer to the actual details on a person or undertaking. If the customer is a natural person, their name and CPR number must be obtained. The same details must be kept for beneficial owners. When the customer is a legal person, name and CVR number will be kept, along with details of their ownership and control structure. Based on a risk assessment, the undertaking may also have obtained additional identity details, such as the customer's address.

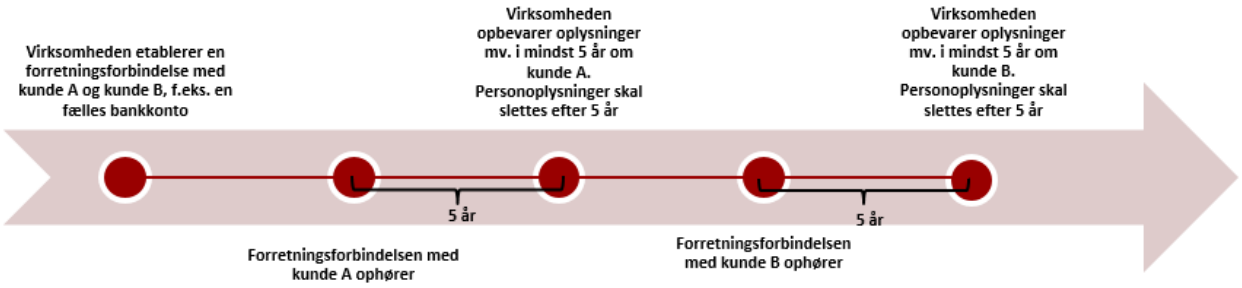
"Verification details" refer to the details the undertaking has used to verify that the identity details provided are correct. When NemID, electronic ID or other forms of OCES standard digital signatures or electronic databases are used, the undertaking must keep an audit trail to prove that verification of each customer's identity details have been verified. Details of verification of a legal person's ownership and control structure, including beneficial owners, must also be kept.

"Identification documents" include physical documents such as social security cards, passports and driving licenses. The undertaking must keep a copy of these documents. Only noting the details in the documentation provided is insufficient. The requirement for a copy of identification documents can be fulfilled, for example, by taking a photocopy or a scan of the document.

Because all the details obtained during the undertaking's KYC procedures have to be kept, all details on the purpose and intended nature of the business relationship, origin of funds etc., along with details the undertaking has obtained to risk assess the customer must be kept.

The undertaking must also keep other relevant details, such as approval of business relationships with politically exposed persons (PEPs) and correspondent relationships.

If a customer has shared products or services with another customer as part of its business relationship, e.g. a common bank account, and the business relationship with the customer ends, the undertaking shall keep the details for at least five years after the end of the business relationship. As such, the undertaking is not obliged to keep details of a business relationship for more than five years after the end of the business relationship with the other customer with whom the customer has shared products or services. See figure below.



Re. 2)
The undertaking must keep records of transactions and records thereof when executed as part of a business relationship or as an individual transaction.

Not all documents and records have to be kept. Only the details relevant to a specific transaction, i.e. on the nature and purpose of the transaction. These include documents, telephone notes etc. of a contractual nature, as well as account statements.

For example: if a loan offer does not turn into a loan to a customer, there is no requirement for the offer to be kept.

Re. 3)
The undertaking must keep documents and records relating to investigations made in accordance with the requirements of the AML Act, see Section 24 on the duty to investigate.

This requirement means that the undertaking must at least keep records of transactions and activities, including the results of investigations and the basis for the results.

It is not sufficient to state that an investigation has been conducted. The record must contain details of how and why an investigation was conducted and its conclusion.

Erasing personal data
The personal data held by the undertaking must be erased 5 years after the end of the business relationship, or 5 years from the completion of an individual transaction. The personal data in question must then be erased, unless other legislation, e.g. the Bookkeeping Act, requires retention for longer. The

undertaking can set an interval for deletion, but which cannot be longer than one month after the 5-year deadline unless there are compelling reasons for not doing so.

Data on legal persons is not subject to the same requirements. Such data must be kept by the undertaking for a minimum of 5 years. The data can be deleted after that period, but it is not mandatory. Data on natural persons, such as beneficial owners of a legal person, are personal data.

Part 6 – Cross-border activities and sanctions

27.Cross-border activities

Reference to the AML Act: Sections 31 – 31 b.

Reference to the 4th Money Laundering Directive: Article 45 (2)-(3) and (5).

27.1. Undertakings operating in other EU/EEA member states

Danish undertakings operating in another EU or EEA member state must ensure that the established undertaking complies with national regulations in the host country (the country in which the subsidiary or branch is established) regarding money laundering and terrorist financing.

An undertaking can operate in other countries, e.g. by establishing a subsidiary or branch.

The undertaking's responsibility for ensuring its subsidiary or branch complies with the host country's legislation only applies to those undertakings established covered by the 4th Money Laundering Directive.

For example: if the undertaking has established a subsidiary in another EU member state that solely undertakes HR work, IT operations or property management, the provision is not relevant.

It should be noted that cross-border activities with no subsidiary or branch established in the host country are not covered by the host country's rules on supervision within the money laundering area.

The undertaking must ensure that an established subsidiary or branch complies with the host country's policies, business procedures and controls for risk management, KYC procedures, the duty to investigate, record and report, duty to keep records, screening of employees and internal controls.

In addition, an undertaking that is the parent company must ensure that its subsidiary or branch complies with its own policies, business procedures and controls. Such checks must be carried out at appropriate intervals, and can, for example, include random checks of the subsidiary or branch's business relationships, documented customer knowledge details, reviewing the undertaking's reports and/or inspections of the undertaking.

27.2. If the host country's rules on money laundering and terrorist financing are less stringent

If the undertaking has established a business in a country that is not an EU or EEA member state with rules on money laundering and terrorist financing that are less stringent than the rules in the Danish AML Act, the obligated undertaking in Denmark must ensure that the established undertaking complies with the Danish AML Act and Danish data protection requirements. However, compliance only needs to be to the extent that will not violate national law in the host country.

27.3. If the host country's rules on money laundering and terrorist financing are less stringent than in Denmark

If the undertaking has established a business in a country that is not an EU or EEA member state with rules on money laundering and terrorist financing that are more stringent than the rules in the Danish AML Act, the obligated undertaking in Denmark must ensure that the established undertaking complies with the host country's rules. Because those rules are stricter in relation to the Danish AML Act law, the undertaking is not obliged to take further action.

The undertaking must still have policies and business procedures at group level adapted to the entire group. See Section 5 on groups.

27.4. If the host country's rules do not permit implementation of the requirements in the AML Act

If the undertaking has established a business in a country that is not an EU or EEA member state with rules that do not allow implementation and compliance with the requirements of the AML Act, the undertaking must take other measures to ensure that the risk of money laundering and financing of terrorism in the established undertaking is addressed in a different manner.

An undertaking subject to the Danish AML Act must notify the Danish supervisory authority that ensures compliance with the AML Act that the undertaking has established a subsidiary or branch in a country where it is not possible to implement and comply with requirements corresponding to the requirements in the AML Act.

The undertaking must provide notification irrespective of whether it has taken effective measures to meet the risk of money laundering and terrorist financing in the established undertaking.

The supervisory authority will determine whether those measures are sufficient to counter the risk, or whether additional supervisory measures are needed.

An undertaking can find guidance to mitigate the risk of money laundering and terrorist financing when it has established a business in a country that is not an EU or EEA member state with rules that do not allow implementation and compliance with the requirements of the AML Act in the EBA's technical standards for the field.12

27.5. Exchanging information on reports

Reference to the AML Act: Section 32 Reference to the 4th Money Laundering Directive: Article 45 (8).

12 Final Report on Draft Joint Regulatory Technical Standards on the measures credit institutions and financial institutions shall take to mitigate the risk of money laundering and terrorist financing where a third country's law does not permit the application of group-wide policies and procedures: https://esas-joint-committee.europa.eu/Publications/Reports/Final%20Report%20on%20Joint%20RTS%20on%203rd%20countries.pdf

Undertakings in a group covered by the AML Act have a duty to exchange information on reports to the MLS with other undertakings in the group.

That duty only covers reports relating to funds suspected of originating from a criminal act or associated with terrorist financing. The undertaking must therefore only disclose information when the report concerns a customer's funds, and not if the report relates to a customer's other activities.

However, undertakings can exchange information within a group when a customer's other activities are suspected of money laundering or terrorist financing. See Section 31.1 on exceptions to the duty of confidentiality.

The exchange of information is limited to the undertaking reporting suspicion of a customer's funds being profits from criminal activity or of being associated with terrorist financing in instances when the undertaking has informed the MLS. The exchange of information must only be made to relevant recipients. This means only with undertakings in the group who have the same customer(s) and personnel dealing with suspicious transactions in the group, for example.

Any undertakings receiving such reports must use them to determine and document whether they will subsequently implement enhanced KYC procedures.

27.6. Limitation of the right of access

A data subject is not entitled to access into their own personal data that has been or will be processed in connection with a report to the MLS on suspicion of money laundering and terrorist financing. This means that the data subject has no right of access into the undertaking's reports according to the AML Act with regard to reports given or considered. See Section 31 on duty of confidentiality.

27.7. Necessary information

When exchanging information, undertakings in a group cannot exchange personal data beyond what is necessary to fulfil the requirement.

This means that an undertaking sending the data must always consider each case separately. Consideration must be based on which information is necessary to exchange to fulfil the requirement. No additional information can be sent other than that included in a report to the MLS.

Information exchanged can contain the customer's name, address and CPR number if the undertaking considers it necessary. In principle, the duty to exchange information does not entitle the undertaking to exchange information about the customer's dealings with the undertaking or similar information.

28. Regulations on increased risk and financial sanctions

Reference to the AML Act: Sections 47, 51, 57, 60, 64, 65, 66 and Annex 3, Item 3 c.

Reference to the 4th Money Laundering Directive: Article 9.
Reference to the 5th Money Laundering Directive: Article 1 (1), no. 5.

Reference to other legislation: Regulation (EU) 2016/1675 of 14 July 2016 on identifying high-risk third countries with strategic deficiencies with subsequent amendments.

The DBA's guide on freezing assets published on May 1, 2008, with subsequent amendments. https://eksportkontrol.erhvervsstyrelsen.dk/vejledning-om-indefrysning.

The following chapter on regulations on increased risk and financial sanctions provides a general description of how undertakings must comply. For further guidance, refer to the DBA's website, www.eksportkontrol.erhvervsstyrelsen.dk/, and see below for reference to the DBA's guides on the area.

28.1. Regulation on high-risk third countries

On 14 July 2016, the EU Commission issued Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing the 4th Money Laundering Directive by Delegated Regulation EU 2018/212. The regulation lists countries deemed to have strategic deficiencies in their international schemes for combatting money laundering and terrorist financing, hereinafter referred to as "high-risk third countries".

The EU Commission can propose changes to the list, including adding and removing countries.

The regulation has been drafted to ensure effective protective mechanisms for the entire internal market, with the aim of increasing legal certainty for economic operators and stakeholders in general in their relationships with third countries.

The 4th Money Laundering Directive gives the EU Commission the power to identify high-risk third countries, and the regulation's list of high-risk third countries is determined on the basis of an evaluation of criteria under Article 9 of the 4th Money Laundering Directive.

The criteria include third countries' legal and institutional framework for combatting money laundering and terrorist financing, including measures regarding customer knowledge requirements, requirements for record keeping, etc.

Undertakings covered by the 4th Money Laundering Directive should apply enhanced KYC procedures to natural or legal persons established in one of the high-risk third countries listed in the regulation. See Section 14 on enhanced KYC procedures.

The annex to the regulation lists the countries that are considered to be high-risk.

The countries listed have committed to remedying the identified deficiencies, and have drawn up a joint action plan with the FATF.

28.2. Financial sanctions in the UN and EU systems

The UN Security Council adopts security resolutions, also known as UNSCRs, in areas such as terrorism, including restrictions on the financing of terrorism. Such resolutions can contain restrictions on countries as well as people, groups, legal entities and bodies.

Security resolutions have legal effect in Denmark through EU regulations implementing the resolutions. The EU regulations are directly applicable in Denmark.

In addition to the security resolutions, the EU can also choose to impose sanctions against a country (also called autonomous sanctions) on its own initiative, including financial sanctions against countries, individuals, groups, legal entities and bodies. This is, for example, the case with the sanctions against Russia, including against Russian legal entities, where the EU has adopted a regulation on restrictive measures against Russia.

All EU regulations containing sanctions can be found on the EU website, at www.sanctionsmap.eu. The relevant regulations on the website will be marked with a "frost sign" which means that the regulation concerns freezing and funds must not be made available to the persons, groups, legal entities and bodies subject to the freezing order.

There are regular changes to UN Security Resolutions and EU Regulations, especially changes to the freezing lists. It is therefore important that the undertaking ensures that it always uses the updated lists.

If an undertaking wants to receive information directly whenever the EU updates its sanctions, including freezing lists, it can sign up for the DBA's news email, https://eksportkontrol.erhvervsstyrelsen.dk/abonner.

The EU has created a database that contains a summary of the names of all the persons, groups, legal entities and bodies subject to freezing under EU sanctions. The EU constantly updates the database. There is a guide to using the database on the DBA's website https://eksportkontrol.erhvervsstyrelsen.dk/vejledning-om-indefrysning.

28.3. Screening customers and transactions

In the former AML Act, the undertaking was required to have procedures for screening EU regulations that contained financial sanctions. This is no longer a requirement under the current AML Act. However, undertakings must still comply with EU regulations and ensure that funds are not made available either directly or indirectly to the individuals, groups, legal entities and bodies listed in the freezing annexes to the regulations.

To ensure that the undertaking does not make funds directly or indirectly available to individuals, etc. subject to freezing, the undertaking must screen their customers and transactions. "Screening" means that the undertaking must ensure that neither the customer nor the transferee is listed in one of the EU regulations.

The undertaking can keep itself updated via the EU database, see the description in Section 28.2 on financial sanctions in the UN and EU systems. There are also several private operators that offer a screening service against various lists that ensures that all the lists being screened are updated.

28.4. Name and identity match

If the undertaking finds a match when screening a customer or transaction, for example, when the name of the customer or the transaction recipient matches an individual, group, legal entity or body that is subject to freezing, the undertaking must investigate whether this is just a name match or also an identity match. An identity match means that the customer or the transaction recipient is listed in one of the regulations, and therefore no funds must be made available to that individual, group, legal entity or body.

In the case of an identity match, the undertaking must therefore not open accounts, invest, transfer or otherwise give the individual access to the financial market. See the DBA's guide to freezing, https://eksportkontrol.erhvervsstyrelsen.dk/sites/default/files/media/2016-01-16_vejledning_om_indefrysning_da.pdf.

The undertaking is obliged to investigate whether there is just a name match or also an identity match. When the undertaking has conducted an investigation and found that the customer is listed in one of the EU regulations on sanctions against ISIL and Al Qaeda, terrorism in general, Afghanistan, Iran, North Korea and Syria, the undertaking must immediately report to the MLS. A report must only be made when an identity match has been found.

28.5. Indirect provision

Many of the EU's regulations on financial sanctions contain a provision that no funds or financial resources are to be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies subject to freezing.

The EU has published a guide on ownership and control for the purpose of investigating indirect provision. The guide can be found on the DBA's website.

Part 7 – Employees and whistleblower schemes

29. Whistleblower schemes

Reference to the AML Act: Section 35. Reference to the 4th Money Laundering Directive: Article 61 (3). Reference to the 5th Money Laundering Directive: Article 1 (1), no. 39, letter b. Reference to other legislation: Section 75 a of the Financial Business Act.

Undertakings must have a scheme under which their employees can use a specific, independent and autonomous channel to report violations or potential violations of the anti-money laundering legislation committed by the undertaking, including by employees or members of the Board of Directors of the undertaking. Anonymous reporting must be possible. In addition, undertakings must follow up on reports to the scheme, and be able to document in writing the process.

Under the general rules of the Financial Business Act, undertakings subject to financial legislation must have a whistleblower scheme.

The undertakings subject to the requirement for a whistleblower scheme in the AML Act are those subject to Section 1 (1), nos. 5, 8 and 11, of the AML Act, and for alternative investment funds nos. 13-20 and 22-24.

However, the requirement for the undertaking to have a whistleblower scheme only covers undertakings employing more than five employees. See Section 29.1 below for exemptions.

The fact that the undertaking must have a special channel means that the channel must be set up for employees to report violations or potential violations of the anti-money laundering legislation to the scheme. .

If the undertaking has a whistleblower scheme under other legislation, this scheme may also include reports under the anti-money laundering legislation. It is not a requirement for the undertaking to establish a separate whistleblower scheme for reporting violations of the anti-money laundering legislation as long as it ensures that employees can report violations or potential violations of the anti-money laundering legislation through a whistleblower scheme.

Violations of other legislation, such as the Marketing Act or Criminal Code (for example embezzlement, fraud, etc.) are not subject to the scope of the provision in the AML Act.

The undertaking's employees must be able to report serious, minor and potential violations. For example: cases that could only cause the undertaking to receive an order or a reprimand from the supervisory authority. .

That the channel must be independent and autonomous means that an autonomous function must be established that is independent of the general management, via which reports can be made outside the

normal procedures, for example directly to the department or employee that processes the reports. This could be the Compliance Officer for example.

Anonymity
The fact that it must be possible for reports to be made anonymously means that the person who reports a violation or potential violation can do so completely anonymously. This could, for example, be through a solution on the undertaking's intranet where reports can be submitted without specifying names and without the ability to track the computer's IP address and the like.

As a rule, reports should only be available to the department or employee dealing with such reports, such as the Compliance Officer.

It is important to ensure that employees who use the scheme can be completely anonymous, as it may be difficult for an employee to decide to report a violation to the undertaking if it cannot be done anonymously. For example, an employee may be afraid of losing their job while other employees may feel that they have acted disloyally to a colleague or the undertaking.

A violation or potential violation committed by the undertaking, including by employees or members of the Board of Directors, includes any violation or potential violation of the undertaking's obligations. This also applies even if a violation or potential violation is caused not only by a single person but, for example, due to a basic system error in the undertaking.
Therefore, violations due to omissions may also be reported, i.e. duties that undertakings do not meet.

If an undertaking or person has chosen to outsource some of their tasks, the employees of the undertaking will also be able to report the external undertaking's failure to comply with obligations to the undertaking's whistleblower scheme. Employees of the external undertaking will also be able to report violations to the relevant supervisory authority. See Section 22 on outsourcing.

Outsourcing
A whistleblower scheme can be outsourced to an external supplier, but the undertaking cannot waive its obligations under the legislation, and undertakings that use outsourcing are thus still responsible to ensure that the schemes comply with statutory requirements. See Section 22 on outsourcing.

An undertaking that manages, administers or otherwise handles a scheme on behalf of an undertaking must be aware of other special legislation that may hinder this. Such an external business must also be aware of any statutory disclosure obligations that undertakings may be subject to.

Employees, including the Executive Board, reporting to the whistleblower scheme will not violate the duty of confidentiality in Section 132 of the Companies Act, nor the confidentiality rules in special legislation, including the duty of confidentiality in the Financial Business Act. This also applies in cases when the scheme is outsourced to an external supplier.

Collective agreements
A whistleblower scheme can be established through a collective agreement.

In practice, this means that the labour market parties, in agreement with undertakings, can establish a scheme in a trade union, for example, to which employees of the undertaking can report violations. A

whistleblower scheme which is based on an agreement between the negotiating parties must comply with the requirements of Section 35 (1), as described above.

29.1. Exemptions to a whistleblower scheme

Undertakings with no more than five employees are not obliged by the AML Act to have a whistleblower scheme.

However, in such cases, undertakings must be aware that as soon as they hire a sixth employee, they are covered by the requirement.

Undertakings must establish a whistleblower scheme within three months after recruiting the sixth employee. This is to ensure that undertakings have the necessary time to establish the scheme when the undertaking exceeds the limit of five employees.

When calculating the number of employees in the undertaking, no distinction must be drawn between categories of employees in the undertaking. This means that all employees who have an employment contract with the undertaking, including, for example, employees without direct customer contact, internal administrative staff, etc., must be included in the overall calculation of the undertaking's employees. All employees must be able to use an undertaking's whistleblower scheme, and all employees must be included in the overall statement of undertaking employees.

Board members are not employees of an undertaking and are therefore not covered. Cleaning staff who are not employed not by the undertaking, but by a separate cleaning company are also excluded.

Employees in undertakings with five employees or less can report violations or potential violations to the relevant supervisory authority's whistleblower scheme.

29.2. Employees reporting an undertaking

Reference to the AML Act: Section 36. Reference to the 4th Money Laundering Directive: Articles 38 and 61 (2), letter b. Reference to the 5th Money Laundering Directive: Article 1 (1), no. 23.

An employee's report includes any notification or message to the supervisory authorities or to an undertaking's whistleblower scheme that can concern a violation or potential violation of the AML Act and its rules by the undertaking, including an employee or a board member. Reporting also includes reporting violation or potential violation of the 2nd Funds Transfer Regulation and regulations containing rules on financial sanctions against countries, persons, groups, legal entities and bodies.

An undertaking cannot expose employees to unfair treatment or unfair consequences because they have reported the undertaking's violation or potential violation of the AML Act to a supervisory authority or to a whistleblower scheme in the undertaking.

The undertaking cannot expose employees to unfair treatment or unfair consequences as a result of the employee having reported the undertaking to the MLS, even if it is an internal report based on an employee's suspicion of money laundering or terrorist financing.

Apart from dismissal, unfair treatment can include demotion, relocation, harassment or the like. In principle, all forms of unfair treatment are included.

Reporting to whistleblower schemes established through a collective agreement is also included in the provision.

Requirement for causal link
It is a prerequisite for the scope of the provision that:

1) the employee or former employee has reported a violation or potential violation to the supervisory authority, and
2) there is a causal link between the unfair treatment/consequence and the fact that the employee or former employee has reported a violation.

The provision is therefore applicable only in respect of unfair treatment or unfair consequences which are decided after the employee has reported an undertaking's violation or potential violation.

An "internal report" is defined as an employee of the undertaking making an internal report of a suspicion to the AML Officer. Protection of the employee or former employee applies regardless of whether the AML Officer refutes the suspicion after investigation. See section 24 on duty to investigate.

Compensation for the employee
If an employee has submitted a report and then experienced unfair treatment or consequences, the employee can receive compensation in accordance with the principles of the Act on Equal Treatment between Men and Women Compensation will be determined taking account of the employee's term of employment and the circumstances of the case, including compliance with the principle of effectiveness under EU law.

The employee or former employee cannot be entitled to compensation under several different sets of rules for the same incident. The same applies if the employee or former employee is entitled to compensation under collective agreements and other labour law agreements.
An employee who believes that they have been subjected to unfair treatment or consequences after having submitted a report of a violation or potential violation must claim compensation from the undertaking in the ordinary courts.

Protection of the employee laid down in Section 36 of the AML Act cannot be waived
The requirement for the undertaking not to treat an employee unfairly on the basis of the employee's report cannot be waived by agreement in advance or after the fact to the detriment of the employee.

It is possible to make agreements that put the employee in a better position than in the provisions of the bill.

29.3. Duty to report to the undertaking's Board of Directors on warnings about money laundering and terrorist financing

Reference to the AML Act: Section 36 a.

With regard to the definition of key persons, reference is made to Section 64 c (2) of the Financial Business Act

The general management of undertakings covered by the AML Act must report warnings of money laundering or terrorist financing received from others, including from foreign authorities, external auditors and consultants, and whistleblowers. Reports must be made to the undertaking's top management body without undue delay.

The duty to report also applies to foreign branches of Danish undertakings, cf. Section 1 (5) of the AML Act. This means that foreign branches of Danish undertakings have a duty to report warnings about money laundering or terrorist financing to the undertaking's top management body at the undertaking's Danish head office. The scope of application of Section 36 a is thus not limited to the persons and undertakings stated in Section 1 (1) of the AML Act.

The duty to report also applies to the Danish branches of foreign undertakings, which are covered by the scope of the AML Act. The general management of the Danish branches of foreign undertakings must report warnings about money laundering or terrorist financing to the undertaking's top management body at the undertaking's head office in the branch's home country.

The general management

The general management refers to personnel responsible for the daily management of a legal person or branch, including operations, sales and other results. The general management of a legal person or branch is typically handled by the Executive Board of the legal person or branch.

Without undue delay

"Without undue delay" is defined as warnings about money laundering or terrorist financing must be reported to the Board of Directors as soon as possible after being received in the undertaking.

Reporting
"Reporting" is defined as making the undertaking's top management body aware of all relevant information concerning a warning about money laundering or terrorist financing, including the content of the warning, the sender of the warning, and the circumstances in which the warning was received.

Warnings about money laundering or terrorist financing

"Warnings about money laundering or terrorist financing" are defined as any message that relates to knowledge or suspicion of a previous, current or possible future violation of the rules on money laundering and terrorist financing in connection with the undertaking, customers, employees, group undertakings, etc.

From others

Depending on the circumstances, "others" are defined as persons other than those explicitly mentioned who send a warning about money laundering or terrorist financing, the content of which is of such a nature and seriousness that the Board of Directors must be informed.

Foreign authorities

A "foreign authority" is regarded as any institution that is part of the public administration in a country other than Denmark. This can include the supervisory, tax, police and prosecution authorities of other countries, but the concept is not limited to these types of authorities. Warnings from the central banks of other countries will also be covered by the duty to report. Warnings received from institutions that are part of the public administration in Denmark are equated with warnings received from foreign authorities.

External auditors

"External auditors" are persons or undertakings approved in accordance with Sections 3, 10 or 11 of the Auditor Act13, who provide audit services or similar services for an undertaking, and that are not employed by the undertaking.

Consultants
"Consultants" are defined as any undertaking or person who provides services to an undertaking in the form of advice or the like (including lawyers) and who are not employed by the undertaking. It is not a precondition that an agreement has been entered into for the provision of services with the consultant.

Warnings from whistleblowers

"Warnings from whistleblowers" are warnings about money laundering or terrorist financing received through the scheme that follows from Chapter 7 of the AML Act. However, there may also be warnings from whistleblowers received in other ways.

Connection with and relevance to the undertaking

Undertakings must assess whether a given warning about money laundering or terrorist financing has such a connection with and relevance to the undertaking, customers, employees, group undertakings, etc., that it entails reporting to the undertaking's top management body. In this connection, the undertaking should keep in mind that reporting to the top management body must be done without undue delay.

The reporting requirement also applies to key personnel in the undertaking. "Key personnel" are defined in accordance with the concept in the Financial Business Act. They can be employees who are part of the actual general management, or employees responsible for a key function in the undertaking, cf. Section 64 x (2) of the Financial Business Act. For example, the provision lists that the person responsible for the compliance function, the AML Officer and the person responsible for internal audits will always be considered as key personnel. If the general management receives a report about a warning received from employees, it must report the warning to the undertaking's top management body.

13 Executive Order no. 1287 of 20 November 2018.

Part 8 – Duty of confidentiality and responsibility

30. Freedom from liability

Reference to the AML Act: Section 37. Reference to the 4th Money Laundering Directive: Article 37.

Reporting to the MLS
The notifications and information that undertakings have disclosed to the MLS in good faith in a report cannot mean that a duty of confidentiality will be violated, and do not therefore impose any liability on the undertaking's employees or management as a result.

The same freedom from liability applies to the suspension of transactions in connection with reports, see Section 25.4 regarding the undertaking's duty to refrain from conducting transactions.
In this connection, it is a requirement that the undertaking acts in good faith. The undertaking can thus not use the provision to e.g. suspend transactions, if it is aware that there are no circumstances subject to the duty to report.

31. Duty of confidentiality

Reference to the AML Act: Section 38 (1) and (8). Reference to the 4th Money Laundering Directive: Article 39.

The undertaking, including its management and employees, is obliged to keep secret:

1) that a report has been submitted to the MLS,
2) that the submission of a report is being considered,
3) that an investigation has been initiated, or
4) that an investigation will be initiated.

The duty of confidentiality only covers the above information. If an undertaking suspects that an employee of another undertaking is laundering the proceeds of, for example, embezzlement or breach of trust in relation to the undertaking, the duty of confidentiality cannot prevent the former undertaking from informing the latter undertaking of the suspicion of embezzlement or breach of trust.

Auditors or others who perform or have performed a special task for the undertaking have the same duty to keep the above information secret.

The duty of confidentiality is indefinite. This means that even if a report does not lead to the customer being charged with a criminal offence, the undertaking must not inform the customer that a report has been previously submitted about the customer.

The duty of confidentiality does not prevent lawyers, auditors, external accountants and tax advisors from advising their clients against carrying out illegal activities.

With regard to other undertakings, they may advise their customers against committing crimes if the undertaking believes it can be done without the customer becoming aware that a report has been submitted or will be filed.

31.1. Exemptions to the duty of confidentiality

Reference to the AML Act: Section 38 (2)-(7). Reference to the 4th Money Laundering Directive: Article 39. Reference to the 5th Money Laundering Directive: Article 1 (1), no. 24.

Disclosure to supervisory authorities and organisations
Upon request, the undertaking can disclose information that a report has been submitted or that it is being considered to the authorities or organisations that supervise compliance with the AML Act. These are the Danish Bar and Law Society, the DBA, the Gambling Authority and the FSA.

There is no general obligation to inform the supervisory authority or organisation, only the opportunity to disclose information on reports when requested to so.

Disclosure for law enforcement purposes
Information on reports can also be disclosed for law enforcement purposes. Law enforcement purposes include prevention, investigation, discovery and prosecution
of criminal offences, protection against and prevention of threats to public
safety.

Disclosure of information between undertakings in the same group
Undertakings in the same group can disclose information about the following:

1) That a report has been submitted or submission is being considered.
2) That an investigation has been or will be initiated.

The exemption from the duty of confidentiality applies to undertakings in the same group which are subject to supervision by the FSA or similar undertakings in the group with their registered office or domiciled in an EU or EEA member state.

See section 27.5 on the duty of undertakings to exchange information.

Disclosure of information to branches and majority-owned subsidiaries in third countries
Undertakings can disclose information to branches and majority-owned subsidiaries located in third countries as follows:

a) That a report has been submitted or submission is being considered.
b) That an investigation has been or will be initiated.

Exchanging information with such undertakings is only permitted if they fully comply with the group's policies and business procedures in the area of money laundering, including business procedures for the exchange of information in the group. It is a requirement that the group's policies and business procedures in the area of money laundering meet the requirements of the 4th Money Laundering Directive. See Section 5.2 on group risk assessment, policies and business procedures.

See section 27.5 on the duty of undertakings to exchange information.

Disclosure of information between undertakings with the same legal or organisational structure
Lawyers, auditors and audit undertakings approved in accordance with the Audit Act, as well as undertakings that otherwise provide the same commercial services as the previously mentioned groups of undertakings, including auditors that are not approved under the Audit Act, tax advisors and external bookkeepers can disclose information between each other on the following:

1) That a report has been submitted or submission is being considered.
2) That an investigation has been or will be initiated.

For information to be exchanged, undertakings must provide their services within
the same legal entity or organisational structure. This means that both the person who discloses the information and the person to whom the information is disclosed must have joint ownership, joint management or joint control of compliance with rules on the prevention of money laundering and terrorist financing.

Therefore, there can be no exchange between, for example, two lawyers if they do not belong to the same legal entity or organisational structure. The requirement that persons carry out their activities within the same legal entity or organisational structure does not mean that they must be employees of the same legal entity or organisational structure.

There can only be exchanges of information between the above undertakings if they have their registered office or are domiciled in an EU or EEA member state and in third countries that meet the requirements of the 4th Money Laundering Directive.

Disclosure of information between undertakings that are not part of the same group
Disclosure of information between undertakings that are not part of the same group is possible on the following conditions:

1) That a report has been submitted or submission is being considered.
2) That an investigation has been or will be initiated.

Three conditions must be met before disclosure can take place:

1) the information must concern the same customer and the same transaction,
2) the recipient of the information is subject to anti-money laundering and terrorist financing measures that are in line with the requirements of the 4th Money Laundering Directive, and
3) the recipient is subject to obligations with regard to confidentiality and protection of personal data.

Re. 1)
It is a requirement that the customer is a customer of both the recipient and the sender of the information and that the information relates to a transaction involving both the recipient and the sender. The customer must therefore be a common customer at the time of the disclosure of the information.

Re. 2)
The recipient of the information must be subject to anti-money laundering and terrorist financing measures that are in line with the requirements of the 4th Money Laundering Directive. The sender must verify that this is fulfilled before the information is disclosed.

If the recipient is established in an EU or EEA member state where the 4th Money Laundering Directive is implemented, this requirement will be met. If the recipient is not established in an EU or EEA member state, information on whether the requirements are met can be found in, for example, FATF's evaluation reports.

Re. 3)
The recipient and the sender must be subject to obligations with regard to confidentiality and protection of personal data.

There can only be exchanges of information between the above undertakings if they have their registered office or are domiciled in an EU or EEA member state and in third countries that meet the requirements of the 4th Money Laundering Directive.

The following undertakings cannot use the exemption from the duty of confidentiality and disclose information between undertakings that are not part of the same group, etc.:

1) providers of services to undertakings,
2) providers of games,
3) estate agents, estate agencies and undertakings providing the same services as estate agents or estate agencies.

Part 9 – Money transfers

32. The Funds Transfer Regulation

Reference to EU legislation: Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying funds transfer and repealing Regulation (EC) No 1781/2006.

Reference to other legislation: Directive 2015/2366 on payment services in the internal market and amending Directives 2002/65/EC and 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC of 25 November 2015, Article 3.

Reference to other relevant guides: The EBA's final guidelines of 16 January 2018:
"Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a funds transfer lacking the required information".

32.1. Background

The purpose of the Funds Transfer Regulation is to prevent, detect and investigate money laundering and terrorist financing. The regulation includes funds transfer when at least one of the providers of payment services involved, – i.e. the undertakings that carry out the funds transfer for a customer – is established in the EU.

The Funds Transfer Regulation lays down rules on the information about the payer and payee that is to accompany funds transfer, regardless of currency.

The information must accompany the funds transfer to make it possible to trace the transaction back to the payer or to the payee.

The Funds Transfer Regulation basically concerns all funds transfer that are fully or partly carried out electronically, regardless of the notification, payment or settlement system used. Funds transfers in which a payment is sent or received outside the EU are also covered by the regulation.

32.2. Definitions

Reference to the Funds Transfer Regulation: Article 3.

The regulation defines relevant concepts. Below are selected definitions.

"Payer" is defined as a natural or legal person who holds a payment account and allows a funds transfer from this payment account or, if there is no payment account, issues a payment order.

"Payee" is defined as a person who is the intended recipient of the funds transfer.

"Payment service provider" is defined as the categories of providers of payment services covered by Article 1 (1) of Directive 2015/2366 on payment services in the internal market, natural and legal persons benefiting from exemptions under Article 32 of the Directive and legal persons benefiting from exemptions pursuant to Article 9 of Directive 2009/110/EC (19) of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, and which provide funds transfer services.

"Intermediary payment service provider" is defined as a payment service provider which is the payment service provider of neither the payer nor the payee and receives and forwards a funds transfer on behalf of the payer's or payee's payment service provider or on behalf of another intermediary payment service provider.

"Payment account" is defined as a payment account as defined in Article 4, no. 12 of Directive 2015/2366 on payment services in the internal market.

"Funds" are defined as funds as defined in Article 4, no. 25, of Directive 2015/2366 on payment services in the internal market.

"Funds transfers" is defined as a transaction that is wholly or partly carried out electronically on behalf of a payer through a payment service provider to make funds available to a payee through a payment service provider, regardless of whether the payer and payee are the same person and regardless of whether the payer's and the payee's payment provider is the same, including:

a) A credit transfer as defined in Article 2, no. 1 of Regulation (EU) No 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro business requirements for credit transfers and direct debits in euro.

b) A direct debit as defined in Article 2, no. 2 of Regulation (EU) No 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro business requirements for credit transfers and direct debits in euro.

c) Funds transfers as defined in Article 4, no. 22, of Directive 2015/2366 on payment services in the internal market, whether they are domestic or cross-border.

d) A transfer effected by means of a payment card, electronic money instrument or mobile phone or other digital equipment or IT equipment using prepay or postpay technology and having similar characteristics to payment cards, etc.

The Funds Transfer Regulation distinguishes between: the payer's payment service provider, the payee's payment service provider and intermediary providers of payment services. In addition, a distinction is made between transfers within and outside the EU.

32.3. Initial overview of the Funds Transfer Regulation

General principle

The general principle is that complete information about the payer and payee must be provided with a funds transfer. There are, however, certain exemptions from the duty to disclose.

Exemptions for providers of payment services within the EU

If all providers of payment services involved in a funds transfer are established within the EU, limited information about the payer and payee may be provided.

However, the payee's payment service provider or intermediary payment service provider may require more information in the following situations:

1) If the funds transfer is over EUR 1,000, the payee's payment service provider or intermediary payment service provider may require complete details.
2) If the funds transfer is below EUR 1,000, the payee's payment service provider or intermediary payment service provider may require details of the payer's and payee's names and payment account numbers/transaction identifiers at least.

Exemptions for providers of payment services outside the EU

If one or more providers of payment services involved in a funds transfer are established outside the EU, only one exemption applies if

1) The money transfer is less than EUR 1,000, in which case limited details can be sent.

However, if the funds transfer is above EUR 1,000, the general principle is that full details must be provided.

What is full information?

1) the payer's name,
2) the payer's payment account number (or transaction identifier),
3) the payer's address, official personal document number, customer ID number or date and place of birth,
4) the payee's name, and
5) the payee's payment account number (or transaction identifier).

What is limited information?

1) the payer's and the payee's payment account number, or
2) a unique transaction identifier if they do not have a payment account number.

Who should send the information?

The payer's payment service provider is required to check and provide the necessary information in connection with a funds transfer for its customer.

Who should check if the information is sufficient?

The payer's payment service provider must ensure that there is nothing missing from the information sent with a funds transfer.

The payee's payment service provider and intermediary payment service provider must ensure that the necessary information has been provided with a funds transfer before a funds transfer can be approved.

32.4. Exemptions in the regulation

Reference to the Funds Transfer Regulation: Article 2.

According to Article 2 of the Funds Transfer Regulation, which concerns the scope of the regulation, certain services are not covered. For an exhaustive list of exemptions, see the Funds Transfer Regulation.

Directive 2015/2366 states in Article 3, letters a - m and o, the services to which the Funds Transfer Regulation does not apply, including:

1) Payment transactions made exclusively in cash directly from the payer to the payee without any intermediary.
2) Payment transactions from the payer to the payee through a commercial agent who, by agreement, is authorised to negotiate or conclude the sale or purchase of goods or services on behalf of either only the payer or only the payee, etc.

Similarly, the Funds Transfer Regulation does not apply to funds transfer made using a payment card, electronic money instrument, mobile phone or similar if:

1) this card, instrument or equipment is used solely to pay for goods or services,
2) the number of this card, instrument or equipment is provided with all transfers in connection with the transaction.

Conversely, this means that if such a card, instrument or similar can be used for transfers that can be made "person to person", such transactions with cards, instruments and similar are covered by the Funds Transfer Regulation.

If the undertaking makes use of the exemptions in a) and b), the undertaking should therefore have procedures to establish that a funds transfer is not a person-to-person transfer, but is instead a funds transfer in payment for goods or services.

Domestic funds transfer to a payee's payment account in connection with purchases of goods and services are not covered by the Funds Transfer Regulation if:

1) the payee's payment service provider is subject to the AML Act,
2) the payee can use a unique reference number to identify the legal or natural per-son who supplies goods or services, and
3) the amount does not exceed an amount corresponding to the value of EUR 1,000.

32.5. Obligations of the payer's payment service provider

Reference to the Funds Transfer Regulation: Articles 4 and 10.

The payer's payment service provider must always ensure that information about the payer and the payee is provided with a funds transfer.

The payer's payment service provider should therefore have policies and business procedures that can effectively ensure that the payment service provider complies with the requirements of the Funds Transfer Regulation in relation to the payment service provider's business model.

The payer's payment service provider must ensure that the following information about the payer is provided:

1) The payer's name.
2) The payer's payment account number.
3) The payer's address, official personal document number, customer ID number or date and place of birth.

The payer's payment service provider must ensure that the following information about the payee is provided:

1) The payee's name.
2) The payee's payment account number.

If the payer or payee does not have a payment account, the payer's payment service provider must instead provide a unique transaction identifier that allows the funds transfer to be tracked.

A "unique transaction identifier" is defined as a combination of letters, numbers or symbols determined by the payment service provider in accordance with the protocols for payment, settlement and notification systems used to make the funds transfer.

Verification of the payer's details
The payer's payment service provider must verify the information about the payer to be provided before the funds transfer can be executed. The information must be verified using documents, data or information from a reliable and independent source.

The payer's identity can be verified in the same way as verifications are carried out in accordance with Sections 10 and 11 of the AML Act, which describe the KYC procedures that undertakings must implement for new customers and established customers. See Part 3 on KYC procedures. See Part 3 – KYC procedures.

This means that the payer's providers of payment services' procedures must ensure that the required information about the payer is verified and accompanies the funds transfer from payer to payee.

If an intermediary payment service provider is included in the funds transfer, it must ensure that the information received about the payer and the payee is kept in conjunction with the transfer.

32.5.1. Funds transfers within the EU

Reference to the Funds Transfer Regulation: Article 5.

If all providers of payment services involved in a payment chain are established within the EU, a funds transfer can be accompanied by limited information about the payer and the payee.

Such a transfer shall at least be accompanied by:

1) the payer's and the payee's payment account number, or
2) a unique transaction identifier if they do not have a payment account.

In spite of the possibility that a funds transfer can be accompanied by limited information, the payee's payment service provider can request additional information. The additional information that the payee's payment service provider can request is determined on the basis of whether the funds transfer exceeds EUR 1,000.

Payment service providers and intermediary providers of payment services should have policies and procedures to assess whether a funds transfer of below EUR 1,000 is linked to other funds transfer, i.e. whether they are interconnected and together exceed the limit of EUR 1,000.

Funds transfers can be linked for example, if they are from and to the same payment accounts, or if they are sent within a short period of time.

Funds transfers over EUR 1,000
The payee's payment service provider can require complete information about the payer or payee to be made available within 3 working days if the funds transfer exceeds EUR 1,000. See Section 32.5 on the obligations of the payer's payment service provider.

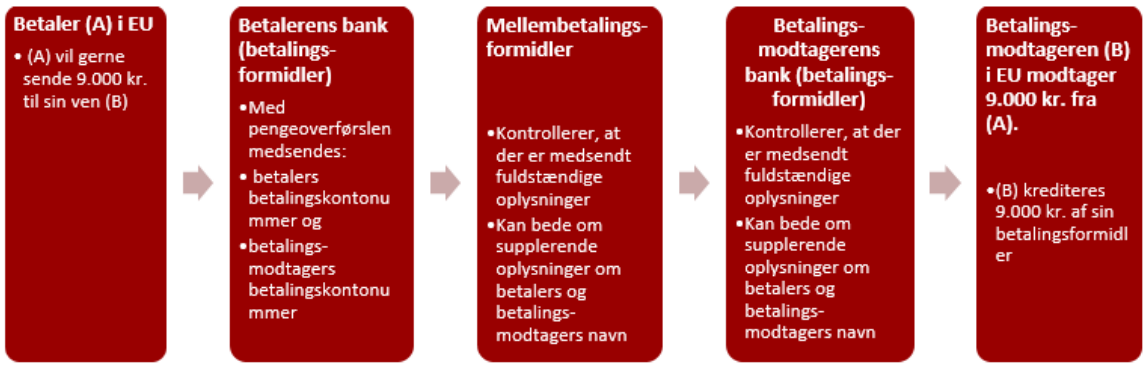
Funds transfers under EUR 1,000
If the funds transfer is below EUR 1,000, the payee's payment service provider can require that the payer's and payee's names and payment account numbers/transaction identifiers are made available as a minimum within a period of 3 working days.

In cases when the funds transfer is below EUR 1,000, the payer's payment service provider is generally not obliged to verify the information about the payer.

The payer's payment service provider must, however, always verify the information if

1) the payer's payment service provider has received the funds to be transferred in cash or in anonymous electronic money, or
2) the payer's payment service provider has a reasonably founded suspicion of money laundering and/or terrorist financing.

Eksempel: *processen for en pengeoverførsel, hvor betalingsformidlerne er banker, og hvor betalingsmodtagers betalingsformidler er etableret i EU.*



32.5.2. Funds transfers outside the EU

Reference to the Funds Transfer Regulation: Article 6.

For funds transfer to providers of payment services established outside the EU, the payer's payment service provider must always provide complete information about the payer and the payee.

Funds transfers under EUR 1,000
However, the requirement that complete information should be provided does not apply if the funds transfer does not exceed EUR 1,000.

Such a funds transfer must instead, as a minimum, be accompanied by limited information:

1) The names of the payer and the payee.
2) The payer's and the payee's payment account numbers or a unique transaction identifier if they do not have a payment account.

In cases when the funds transfer is below EUR 1,000, the payer's payment service provider is generally not obliged to verify the information about the payer.

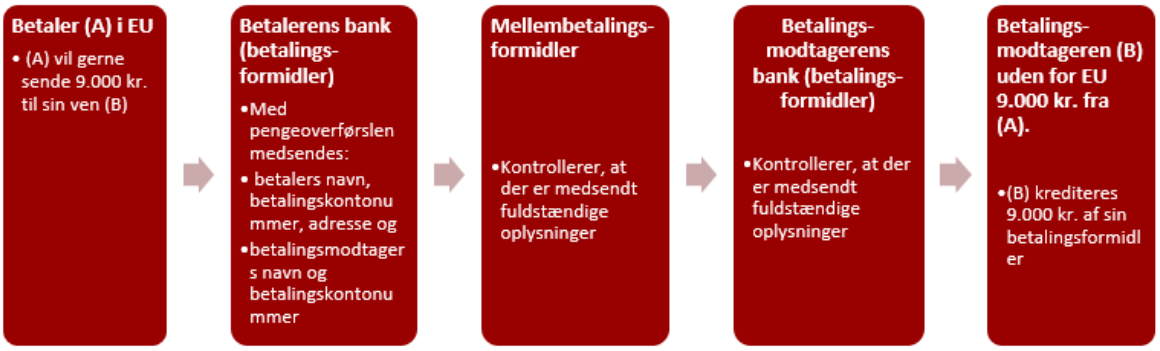
However, the payer's payment service provider must always verify the information if

- the payer's payment service provider has received the funds to be transferred in cash or in anonymous electronic money, or
- the payer's payment service provider has a reasonably founded suspicion of money laundering and/or terrorist financing.

Batch file transfer
If a single payer completes a batch file transfer to a payee outside the EU, the requirement to send complete information about the payer and the payee does not apply to each transfer in the batch transfer.

Instead, it is crucial that the batch file collectively contains the complete information and that the information about the payer has been verified

Eksempel: *processen for en pengeoverførsel, hvor betalingsformidlerne er banker, og hvor betalingsmodtagers betalingsformidler er etableret uden for EU.*



32.6. Obligations of the payee's payment service provider

Reference to the Funds Transfer Regulation: Articles 7, 8, 9 and 10.

The payee's payment service provider must determine whether any information about the payer or payee is missing.

The payee's payment service provider is therefore required to have effective procedures that can be used to ascertain whether the information transmitted in the system used contains characters or inputs in accordance with the system used. The payment service provider's procedures should therefore also be able to prevent or stop the execution of a funds transfer if no characters or inputs have been used in accordance with the system in connection with a funds transfer or if the information is meaningless, for example. If the characters are random characters like 'ABCDEFG', or if the name is not specified, for example "customer" only.

Effective procedures do not require a manual review. For example, the payment service provider may have a system with a list of characters or words that are meaningless and which, consequently, should result in a transfer not being completed or being stopped if such information is included.

In addition, the payee's payment service provider should have procedures to ensure that post-monitoring or real-time monitoring is carried out that can be used to determine whether any information about the payer or payee is missing, for example whether the payer's and the payee's payment account numbers or a clear transaction identifier have been specified.

Monitoring procedures must be proportionate to the payment service provider's business model and the risks of money laundering and terrorist financing to which the business model is exposed.

The payment service provider can also carry out regular random sample checks on funds transfer that have been completed to assess whether the procedures are effective.

Direct debit demand
The general principle is that the payer's payee has to provide the necessary information with a funds transfer, but if the funds transfer is a direct debit, the payee's payment service provider should send the necessary information about the payer and the payee to the payer's payment service provider as part of the direct debit demand.

Funds transfers above EUR 1,000
For funds transfers above 1,000 euros, the payee's payment service provider must always verify whether the information provided about the payee is correct before the payee is credited with the funds or the funds are made available to the payee regardless of whether the funds transfer is received as one or more linked transfers. The information must be verified on the basis of independent and reliable documents. Please note that the payee's information should already be verified in connection with the payment service provider's implementation of KYC procedures on the payee. See Part 3 – KYC procedures.

Funds transfers not above EUR 1,000
The payee's payment service provider is generally not obliged to verify the information about the payee under the Funds Transfer Regulation if the funds transfer or several linked funds transfers do not exceed EUR 1,000. See section 32.5.1 for a description of when funds transfers are linked.

However, the payee's payment service provider always has a duty to verify the information if:

1) the payer's payment service provider has received the funds to be transferred in cash or in anonymous electronic money, or
2) the payer's payment service provider has a reasonably founded suspicion of money laundering and/or terrorist financing.

Missing or incomplete information
The payee's payment service provider must have risk-based procedures to determine whether a funds transfer for which information is missing or incomplete information is provided must be rejected, suspended or other measures must be taken.

In cases in which the payee's payment service provider becomes aware that a funds transfer is missing information or the information is incomplete, the payment service provider must reject the transfer or request the missing information.

If a payer's payment service provider repeatedly does not provide the necessary information or sends incomplete information with a funds transfer, the payee's payment service provider must take measures in the form of warnings and deadlines for receiving information and then decide whether future funds transfer from this payment service provider must be restricted or rejected.

The payee's payment service provider reports the omission and the measures taken to the relevant supervisory authority which supervises the relevant undertaking's compliance with the AML Act.

32.7. Obligations of intermediary providers of payment services

Reference to the Funds Transfer Regulation: Articles 10, 11, 12 and 13.

Intermediary providers of payment services must ensure that all information provided with a funds transfer is kept with the transfer.

In common with the payee's payment service provider, intermediary payment service providers must have effective procedures for:

1) determining whether the information communicated in the system used contains characters or inputs in accordance with the system used,
2) ensuring that the information received is kept with the transfer and
3) ensuring that post-monitoring or real-time monitoring is carried out that can be used to determine whether any information about the payer or the payee is missing.

See Section 32.6 on payee's payment service provider.

The same rules apply to intermediary providers of payment services for funds transfers in which the payer or the payee's payment service provider is established outside the EU and to batch file transfers. See section 32.5.2.

Annex 1

Example of a process for the preparation of a risk assessment

The example is non-binding. Consequently, undertakings and persons that are subject to the AML Act are free to decide how they prepare a risk assessment.

The example below shows steps that an undertaking or individual (called an *undertaking* below) can follow in the preparation of the undertaking's risk assessment. However, it is important for each undertaking to document how it has assessed its risk, and each undertaking decides on the measures to be implemented as a consequence of the risk assessment.

1) Collection of internal and external data for the assessment of the different risk factor areas
   a) An undertaking must document/justify its assessments in internal information and in relevant external risk assessments, reports, guidelines, etc.
2) Identification of inherent risks in an undertaking's business model
   a) The risks of the undertaking being abused for money laundering or financing of terrorism in relation to risk factors including the following:
      i. customers
      ii. products, services and transactions
      iii. delivery channels
      iv. countries and geographical territories
3) Assessment of the scope and nature of the inherent risks, for example by weighting them using a fixed scale
   a) For example: by assessing the probability of abuse and the consequence of abuse on a scale with weightings for limited, medium or high risk for both probability and consequences.
   b) Each risk factor can be weighted individually so that the undertaking can see where the risks are highest.
4) Results of the risks in the undertaking's risk factors
   a) The undertaking could conclude the risk level for each of the risk factors listed under point 2, for example by calculating a score for each risk factor