Project AML/TEK

Contents

Acronyms

AMLD	The EU Anti-Money Laundering Directives – when a number is added subsequently it refers to the version. For example AMLD4 is the fourth AMLD.
CVR	The Danish business register, which is a register under the auspicious of the DBA that holds information on all registered Danish companies.
CVR number	Danish business registration number.
CPR	Register under the auspicious of the Ministry of Interior and Housing in Denmark that holds general personal information on any Danish citizens with a CPR number.
CPR number	Danish social security number.
DBA	Danish Business Authority, which holds the responsibility for various tasks in relation to business development and regulation, including CVR, and is a public authority under the Ministry of Industry, Business and Financial Affairs.
Danish FIU	The Danish Financial Intelligence Unit also known as the Money Laundering Secretariat.
Danmarks Nationalbank	The Central Bank of Denmark
DFSA	The Danish Financial Supervisory Authority.
GDPR	The General Data Protection Regulation.
KYC procedures	General term for the Know Your Customer procedures applied by the obliged entities. For the purpose of this report it refers to the customer due diligence procedures, both during onboarding and when performed ongoing. Furthermore, KYC-procedures can be characterized as enhanced or simplified, depending on the risk classification of the customer as further described in the MLA.
MLA	The Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism.
ML/TF	Money laundering and terrorist financing.
PEP	Politically Exposed Person as defined in the MLA.

RCA	Relative or Close Associate of a PEP as defined in the MLA.
Reports to the Danish FIU	Suspicious Activity Reports (SARs), Suspicious Transaction Reports (STRs) and Terrorism Financing Reports (TFRs) that are reported to the Danish FIU.

Summary

On 27 March 2019, the Danish government then in power and a broad majority in the Parliament entered into a political agreement on strengthening efforts to combat financial crime[1]. The sixth initiative in the agreement stipulates that the Danish Financial Supervisory Authority (the DFSA) must support the financial sector's work on building a common infrastructure that can support companies' Know Your Customer (KYC) procedures.

The KYC procedure is an important element in the fight against money laundering and terrorist financing (ML/TF). Knowing customers and the purpose of the customer relationship puts companies and persons that are subject to the Money Laundering Act (MLA) in a better position to assess whether customers' activities are unusual. Customer knowledge is built up continuously during a customer relationship through:

1. Obtaining and continuously updating relevant information (master data) about current customer relationships.

2. Ongoing monitoring of activities and transactions (transaction monitoring) relating to current customer relationships.

The obliged entities carry out ongoing monitoring in order to assess whether there are discrepancies in transactions and activities relative to customer knowledge, for example in the purpose and intended nature of the business relationship. Questionable matters (suspicious behaviour) must be examined, and if the examination supports a suspicion of ML/TF, the Money Laundering Secretariat (Danish FIU) must be notified.

The Danish FIU is Denmark's financial intelligence unit, which is responsible for receiving, analysing and disseminating information about possible ML/TF to the relevant authorities.

Companies and persons subject to the MLA thus act as the first line of defence in the preventive efforts to counter ML/TF, and customer knowledge is crucial to effective efforts. KYC procedures are therefore important, but can sometimes also be cumbersome for customers and the obliged entities.

Among other things, the process is cumbersome for customers because they typically have to submit and hand over material containing information, such as identifying data like a copy of a passport. Customers, particularly customers in long-term customer relationships, often do not understand why, for example, banks need such information on an ongoing basis, and feel it is unacceptable to have to provide this.

For the obliged entities, the process is cumbersome for other reasons, including:

1. Obtaining and specifically verifying customer master data is in many cases a resource-intensive process. This is partly due to the risk-based approach to the content of the KYC procedure, which means that it is not straightforward to set fixed criteria

[1] Included in the agreement were the government in power at the time (Venstre, Liberal Alliance and the Conservative People's Party), the Social Democratic Party, the Danish People's Party, the Danish Social Liberal Party and the Socialist People's Party.

as to when the KYC procedure that has been performed is adequate. In addition, these procedures are often manual.

2. The opportunities to quickly and effectively obtain adequate customer knowledge, including effective organisation of transaction monitoring, may be limited by lack of access to relevant data sources under the auspices of public authorities and limited knowledge-sharing across obliged entities and with the authorities regarding indications of suspicious behaviour.

3. The provisions of the MLA and the duty of confidentiality largely limit the opportunity for companies and persons subject to the MLA to share information about customers and their suspicious behaviour. This means that the opportunity to substantiate customer knowledge based on observations made by others is limited.

It is in the interest of the authorities to support effective KYC procedures, as any subsequent investigation into ML/TF cases builds on the information the obliged entities hold about their customers and their customers' behaviour. This emphasises the importance of continuously considering whether cooperation can be improved and whether the obliged entities have the right tools available for undertaking their task.

The Danish Financial Supervisory Authority (DFSA) is of the opinion that it is possible to optimise the infrastructure available so that KYC procedures can be carried out more effectively and in a way that better supports the fight against ML/TF, while at the same time making it less cumbersome for customers and the obliged entities.

The possibilities are however conditional on other necessary considerations, primarily in regards of personal data protection and customers' basic legal rights. The authorities must therefore strike a balance with these two considerations when determining whether anything further should be done to support those subject to the reporting obligation.

On this basis, the DFSA has analysed a number of different initiatives that are considered suitable for addressing the raised issues[2]. Among other things, the focus has been on the extent to which better use can be made of Denmark's existing digital infrastructure. In addition, the DFSA has analysed options for expanding the infrastructure. In connection with this, the focus has been on the legal issues. As one of the most digitised societies in the world with a strong history of establishing a common infrastructure, Denmark should be able to be a pioneer in this area.

In many ways, it is difficult to quantify the value of a specific initiatives before testing them in practice. The starting point for the analysis is therefore as follows:

> *Better customer knowledge and improved insight into criminal behaviour can help to detect suspicious behaviour more quickly and to a greater extent. Customer knowledge can be improved through more efficient use of resources and increased data sharing, and the potential for improvement will increase in line with the credibility*

[2] This analysis was named Project AML/TEK.

and scope of data. Improved insight into criminal behaviour requires better cooperation between relevant authorities and the sector.

Table 1 summarises the initiatives presented in the report. The initiatives are divided into two categories: better use of existing infrastructure, and expansion of existing infrastructure.

Table 1 – Summary of recommendations

Measure	Recommendation	Value	Complexity			Section
			Legal	Technical	Time frame	
Better use of existing infrastructure						
KYC-utilities	Support the sectors work in order to ensure effective implementation.	Medium	Medium/High	Low	Medium	4
The Danish Business Register (CVR)	Work towards establishing a mechanism for verifying company data in CVR.	Medium	Low	Low	Medium	5
MyID (MitID)	As the MyID-solution is implemented, determine whether MyID can be used more broadly than EasyID (NemID) to verify identities.	Medium	Low	Low	Short	6
Expansion of existing infrastructure						
PEP-solution	Establishment of solution for screening for PEPs and RCAs under a public authority.	Medium	Low	Low	Short	7
Generalised scenarios	Establish sector-wide coorperation focused on identifying generalised scenarios (typologies) that can be used in transactionmonitoring.	High	Low	Medium	Medium	8
Increased access to data held by authorities	Identify opportunities to grant access to aggregated company data or assessments under the Danish Business Authority. Availablity of other public data should also be considered.	Medium/High	Medium	Medium/High	Medium/Long	9
Sharing of risk flags	Decide whether to work towards enabling the sharing of risk flags. Either directly between banks, which requires an amendment to the confidentiality requirements under the AMLD, or through a public authority.	High	High	High	Long	10

Source: The DFSA.

Further work is contingent on a common understanding between relevant authorities, and in particular political support for exploring the relevant initiatives in more detail. Balancing the value in relation to the fight against ML/TF against the complexity of the initiative, particularly its legal complexity, is key to whether further work is to be done on a given initiative. This weighting is in no way objective, and other stakeholders may weigh things differently compared to the DFSA. The report therefore contains no conclusions, but presents the DFSA's proposals for further work.

Note that a decision to proceed with one initiative does not necessarily preclude the possibility of proceeding with other initiatives simultaneously or at a later date. Conversely, further work may demonstrate that an initiative is associated with bigger problems or fewer benefits than first assumed.

It may also be beneficial to focus on potential synergies that may arise, to ensure that further work is not done on different initiatives with the same purpose across obliged entities and authorities.

Better use of existing infrastructure

The increasing focus on improving efforts to combat ML/TF has led companies and persons subject to the MLA, in particular banks, to scale up their resources hugely in recent years. On 27 November 2019, Finance Denmark's Money Laundering Task Force published a report on the financial sector's efforts to combat ML/TF. The report states that the number of employees in banks who had anti-money laundering and compliance as their core task as at November 2019 was 4,300, which corresponds to annual wage costs of approximately 3.4 billion.

The report also includes a number of recommendations pointing, among other things, to the need to further develop common IT solutions so that resources can be allocated and used better. It emphasises that a prerequisite for the sector to be able to use such standardised solutions is that work must be done to establish a form of minimum standard for the content of KYC procedures, in particular.

It is impossible to fully standardise KYC procedures, as they must always be adapted to the specific circumstances of the individual company. The MLA also prescribes a risk-based approach. However, the DFSA acknowledges the potential in working towards harmonisation and streamlining of the approach where possible. The work can be supported by simultaneously ensuring the quality of public solutions and registers.

The DFSA has included these considerations in its work on the report, resulting in three concrete proposals for further work:

1. **Support the development of KYC-utilities:** The focus should be on concretising challenges or opportunities and clarifying the extent to which it is regarded as proportionate to work towards the requisite infrastructural and legislative changes. This exercise should be supported by actual observations from KYC-utilities, which can be obtained as they join the market**.**

2. **Quality assurance of CVR:** Start working with relevant actors, including the Danish Business Authority, Finance Denmark, FSR-Danish Auditors and the Danish Bar and Law Society, with an emphasis on mapping the conditions under which a mechanism can be established in CVR, whereby lawyers and authorised auditors can verify registered company information.

3. **Increased scope for MitID ('MyID' in English):** The DFSA expects that it will be possible to use MitID (MyID) to verify customer identities beyond the capacities for which NemID (EasyID) can currently be used. We will only know this for certain when the MitID Act enters into force and MitID has been issued to a broad cross-section of people in Denmark. The ongoing development of the MitID solution should therefore be monitored closely with this aim in mind.

Measures focused on expanding infrastructure

A general challenge in terms of ensuring an effective fight against ML/TF is that, to a certain extent, customer knowledge is fragmented across obliged entities and authorities. In principle, this means that customer knowledge needs to be built up from scratch whenever a new customer relationship starts. Obliged entities also do not always have the right prerequisites for effectively countering relevant risks in transaction monitoring.

These considerations have been echoed in recent years by a large number of European authorities and international organisations. Among other things, the Financial Action Task Force (FATF[3]) published a report in 2017 highlighting the potential for broader sharing of information among private sector actors[4]. The European Commission's Action Plan for effective combating of ML/TF also highlights the value of so-called Public-Private Partnerships (*PPP*)[5]. In addition, Finance Denmark's Money Laundering Task Force has also highlighted the potential for better data and knowledge sharing.

The DFSA has identified four initiatives that could potentially support more effective efforts. Each of these initiatives is associated with legal challenges of various kinds, and any concrete assessment of the legal consequences is dependent on the form that the initiative take in practice.

Three of the four proposals have been prepared using banks as the starting point. This is because needs vary depending on the industry, and the potential is assessed as being greatest for banks, which have a particular role to play in the fight against ML/TF. Banks have the broadest customer segment and offer the broadest portfolio of products. At the same time, in the past decade there have been a number of examples of banks being misused for the purpose of ML/TF.

The initiatives may also be relevant in varying degrees to other companies and persons subject to the MLA. When and if it is decided to continue working on these initiatives, the potential for expanding them to other obliged entities should also be considered.

On this basis, the DFSA recommends the following four initiatives:

1. **Establishment of a PEP-solution in the public sector:** Decide whether further work is to be done on the two proposed solution models, and if so, decide the authority in which the PEP-solution is to be anchored. Both models require amendments to the MLA and the PEP Executive Order, which should be initiated if work continues on this initiative.

2. **Development of generalised scenarios:** Decide whether the cooperation between authorities and banks should be expanded with the aim of developing typologies for relevant scenarios (generalised scenarios) that should be identified in transaction

[3] The Financial Action Task Force on Money Laundering and Financing of Terrorism is an inter-governmental body under the auspices of the OECD, founded in 1989 on the initiative of the G7 to develop policies and recommendations to combat money laundering and terrorist financing. FATF's recommendations form the basis for the EU anti-money laundering directives, which have been implemented in Danish law in the Anti-Money Laundering Act, among other areas.
[4] Financial Action Task Force on Money Laundering, Guidance – Private Sector Information Sharing, November 2017.
[5] European Commission – Communication on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, May 2020.

monitoring. It makes sense to position this work within the framework of a Joint Anti-Money Laundering and Terrorist Financing Intelligence Taskforce (referred to by the Danish acronym, FEHT) if or when this is established.

3. **Increased access to data held by authorities:** Decide whether to start focusing on the possibility of banks gaining access to composite company data or assessments under the auspices of the Danish Business Authority. The decision should be complemented by considerations as to whether such work should also affect opportunities for wider access to data from other authorities

4. **Risk flag sharing:** Decide whether to start working on enabling the sharing of risk flags between banks. As part of this, a decision should be reached as to whether work should be done to enable banks to share risk flags with each other, and thus for a change in the confidentiality provisions in the AMLD, or whether further work should focus on sharing exclusively through a public authority.

In regard to this, note that a crucial premise for effective implementation of initiatives focused on data and knowledge sharing about customers is that it does not lead to increased de-risking of the customer portfolios (termination of customers) by companies and persons subject to the MLA. This is both due to concerns as regards the legal rights in connection with this and to the risk that criminals will instead try to operate on the black market, making them even harder to identify.

Structure of the report

Sections 1 and 2 introduce the requirements for KYC procedures under the MLA and the overall legal considerations on which any assessment of further access to sharing data on customers should be based. Section 3 deals with considerations regarding the opportunities for more widespread use of advanced technologies. The measures focusing on better use of existing infrastructure are then introduced in sections 4, 5 and 6, while sections 7, 8, 9 and 10 cover proposals for expanding the infrastructure. Section 11 summarises the process for further international work, particularly under the auspices of the EU, which will be necessary or appropriate to pursue in order to realise several of the concrete initiatives and make them fully impactful.

Sections 4–7 and 10 are structured in such a way that the introduction summarises the analysis and the initial results. The remaining subsections for each section constitute the actual analysis and legal considerations. Sections 8 and 9 open with an introduction to the analysis, after which the subsections deal with legal considerations.

1. KYC procedures under the Money Laundering Act

The MLA stipulates that the obliged entities must identify and assess their inherent risk of being used for the purpose of ML/TF. 'Inherent risk' follows from the chosen business model (product range, customer types, geographical areas, etc.), without taking into account any measures implemented to limit this risk.

The MLA also stipulates that companies and persons covered by the MLA must carry out KYC procedures when establishing a business relationship with a customer, when the customer's relevant circumstances change, and otherwise at appropriate times. The KYC procedures must be carried out for both natural and legal persons. Depending on the type of customer, this includes obtaining:

1. Identity information about the customer or beneficial owners and information that can clarify whether the customer is a politically exposed person (PEP) or a relative or close associate of a PEP (RCA).
2. Information about the purpose of the customer relationship.
3. Information about the intended nature of the business relationship or the customer's expected use of the product. This could be the expected type, size, number or frequency of transactions that the customer expects to complete.

The obliged entities must also carry out a risk classification of the customer relationship as part of the KYC procedures. This risk classification forms an essential part of the procedures, as it determines the scope of these based on the specific customer relationship. One purpose of the risk classification is to help set a framework for the frequency of the ongoing maintenance of customer knowledge as well as the scope and nature of subsequent monitoring of the customer relationship. In some cases, this may require the company to obtain additional information before initiating or continuing the customer relationship. Risk classifications may thus lead to the obliged entities carrying out simplified or enhanced KYC procedures for a given customer relationship.

The obliged entities will, and must always be, responsible for ensuring that customer knowledge is adequate.

The MLA also stipulates that the obliged entities must continuously monitor their customers and examine the background to and purpose of all transactions that are complex, unusually large, carried out in an unusual pattern relative to the knowledge of the customer, or do not have an obvious financial or legal purpose (transaction monitoring). Observed and questionable matters in transaction monitoring are also known as 'risk flags', which are raised for a transaction made by a customer whose behaviour is suspicious.

Should an obliged entity, based on an examination of a risk flag, become aware of, suspect or have reasonable grounds to suspect that a transaction or activity is or has been associated with ML/TF, the entity must immediately file a report to the Danish FIU. Transaction monitoring also helps the obliged entity to get to know the customer better with a view to future monitoring.

2. General legal considerations in regard to data sharing

Regardless of which specific model is used, any sharing of data on customers (companies and persons) between companies and persons subject to the requirements of the MLA will have to comply with the general requirement for a legal basis for processing data. At the same time, the legal rights of the person or persons to whom the information pertains must also be considered. In this context, 'legal rights' must be understood as the individual's ability to know what information is being exchanged about him, and assurance that the individual will not face penalties or reactions based on information that he has not been able to counter or been aware of. Finally, more comprehensive models for sharing information without consent must be considered in relation to, for example, the right to privacy.

The legal considerations in regard to data sharing either between the obliged entities or between authorities and the obliged entities concern three matters in particular:

1) The proportionality of the infringement.
2) The legal impact on the data subject.
3) The legal basis to process data.

The proportionality of the infringement

Arrangements allowing access to the exchange of information on one or more natural or legal persons without the consent of the person concerned may, depending on the circumstances, constitute an infringement of the right to privacy pursuant to Article 8 of the European Convention on Human Rights (ECHR).

Article 8 has a broad scope that is adapted on an ongoing basis to technological developments. The provision therefore also includes personal information, etc.[6] Authorities may therefore only record and store such information for objective and compelling reasons and must process the information in a way that is legally sound so that it is not unduly disclosed. Similar requirements apply to private companies, where the state has a duty to safeguard its citizens against private infringement of people's civil liberties, such as the right to privacy and family life.

Article 8(2) implies that any infringement of privacy and family life must have a legal basis and must be necessary in a democratic society (proportionate) in order to look after the important rights of society or others.

In immediate terms, the DFSA judges that the exchange of information on, for example, master data or risk assessments of customers, including risk flags raised as part of a bank's transaction monitoring, or similar information, could constitute an infringement of the right to privacy pursuant to Article 8.

Any scheme involving such an exchange would therefore have to have legal basis and take into account important societal considerations. Among other things, Article 8 implies that it may be in the interests of national security, public security or the economic well-being of the

[6] See among others *Leander* (1987, paragraph 48) and *Amann* (2000, paragraphs 65 and 69).

country, to prevent unrest or crime, to protect health or morality or to protect the rights and liberty of others.

Information on risk flags, risk assessment, etc. is meant to be exchanged in order to more effectively prevent money laundering and terrorist financing. The following is stated in recital 42 of the preamble to the EU's 4th AMLD (excerpt):

> *"The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States."*

The DFSA considers that in this context, and as this is an infringement aimed at preventing crime, it can be assumed that the fight against money laundering and terrorist financing must be regarded as a weighty societal consideration in the sense of Article 8(2), i.e. an infringement that would thus be able to justify infringement of the right to privacy and family life.

Assuming that the infringement would be legitimate under Article 8, whether the infringement is proportionate to the consideration pursued will still require assessment. The proportionality assessment consists of three elements:

1. Suitability: The infringement must be suitable for achieving its purpose.
2. Necessity: The infringement must be necessary for achieving its purpose.
3. Proportionality: The infringement must reflect a reasonable relationship between objective and means.

Whether the infringement is proportional should therefore be assessed for each model. In other words, an assessment of the necessity and proportionality will determine whether the proposed models could constitute a lawful infringement under Article 8. An infringement will only be necessary if the same result cannot be achieved with a less radical infringement.

In general, the considerations imply that the more far-reaching a model for information sharing is, the more weight should be given to the proportionality assessment, and the more important it becomes to be able to explain necessity and proportionality.

The legal impact on the data subject
Arrangements allowing the exchange of information on natural and legal persons without consent give rise to considerations as to what the legal effect of this information will be, including the right to know and, if necessary, verify the accuracy of the information.

It should thus be ensured that a model with the exchange of information without consent does not imply that customers of companies and persons subject to the MLA are at risk of exclusion as customers on the basis of information of which they have no knowledge and which they do not have an opportunity to verify (blacklisting). It will therefore be of concern for the individual's legal rights if the sharing of information on risk flags, assessment of risk flags and risk assessments implies that customers encounter reactions based on information about their business that they are neither familiar with nor able to gain insight into. For example, there may be cases where a bank refuses to allow a customer to open an account on the basis of information about the customer's previous transactions that the new bank has

received without the customer's knowledge. These concerns are exacerbated in cases where there is not only objective information but also assessments of that information.

At the same time, the ability that the person to whom the data relates has or must have to appeal against any records or risk assessments which the person concerned feels to be incorrect should also be considered. If information about customers is given legal effect vis-à-vis the customers, without the individual customer being able to gain knowledge of the information or to verify its accuracy, this thus implies concerns in terms of legal rights. This is especially true if the data in question is shared in a wider circle.

In addition, all consumers are entitled to a basic deposit account in accordance with good practice rules. Section 11 of the Danish Payment Accounts Act states that banks must offer a consumer a basic payment account unless opening such an account will lead to a breach of the MLA. In addition, banks may refuse to make a basic payment account available to a consumer if the consumer:

1. cannot demonstrate a genuine interest in a basic payment account
2. has committed criminal offences against the bank, or
3. has acted to the inconvenience of the bank's other customers or employees.

The legal effects of the information exchanged will thus have to be weighed up against the consumer's right to a basic deposit account and a basic payment account. This means that a bank cannot refuse to set up a basic deposit or payment account for a consumer if the conditions in the Payment Accounts Act are otherwise met.

The legal basis to process data
Sharing customer data raises questions about the processing of customer data, including in particular the ability of obliged entities to process and exchange information about private customers without the consent of the person concerned.

The considerations in regard to the General Data Protection Regulation (GDPR) are only relevant for information on natural persons, as it does not apply to legal persons.

According to the GDPR, any processing of personal data must comply with the requirements of legality, reasonableness and transparency. In addition, collected data may in principle only be used for the specific purpose for which it was collected (the purpose limitation).

This means that a legal basis for processing will always be required (processing authority) in order for obliged entities or public authorities to process personal data, for example as part of KYC procedures and the fight against ML/TF. Obliged entities and public authorities must therefore ensure that the correct regulatory basis is in place before they share, obtain or otherwise process personal data.

The GDPR provides for access to the processing of personal data without the consent of the data subject. In order for an obliged entity to be able to process information without consent, it must have clear processing authority.

The processing of personal data on the basis of the rules in the AMLD is considered to be in the interests of society, cf. Article 43. This constitutes a lawful legal basis for processing under Article 6(1), letter e of the GDPR, cf. subsection 3, letter a. Companies and persons subject to the MLA thus currently have a basis for carrying out data processing covered by the MLA.

In assessing the potential measures individually, whether the purpose for which the information has been collected equates to the purpose of further processing should be considered.

The DFSA is of the opinion that, regardless of the model, it should be ensured that there is a clear legal basis for the desired processing, regardless of whether it is an exchange between obliged entities or an exchange between an obliged entity and a public authority.

3. The potential of advanced technology

There is generally a strong international focus on the scope of application of more advanced technological solutions, such as machine learning, in relation to the fight against ML/TF. The German Presidency of FATF has also included it as one of its priorities for FATF's work until the end of 2022 and has initiated a project that the DFSA is involved with[7].

One of the challenges of using machine learning for transaction monitoring is that in many cases it can be difficult to explain the model's decision-making processes. This may affect the extent to which the results of such models can be used as a basis for filing a report to the Danish FIU and actual sanctions against the customer. Requirements for clarity, either internally in an obliged entity or externally in relation to the DFSA or the Danish FIU, are expected to vary, depending on how extensive the result of a model is. For example, a model with very low explainability may well be useful in a process of monitoring and screening, where individuals or companies are selected for manual examination. If a more far-reaching decision is made, for example to file a report to the Danish FIU, it will probably be necessary that the results of the model can be explained in detail. In practice, at present this means that the most advanced versions of machine learning should not be used to make autonomous decisions that have an impact on individuals. Fundamentally, obliged entities that apply machine learning should assure that that the internal governance set-up is sufficiently robust for such assessments to take place and not be overridden on the way.

The quality of a machine learning model is also conditional on the extent of historical data available to train the model. This applies in particular to information about the actual results that the model will be used to identify. This may be problematic in relation to the use of machine learning in transaction monitoring, as in principle, the obliged entities only have access to information about questionable matters that are identified during existing processes, as well as any actual reports filed to the Danish FIU. At the same time, the possibility of gaining insight into the results of the authorities' investigations of cases on the basis of specific reports is limited. If actual reports to the Danish FIU are used, for example, as a success criterion when training a machine learning model, the quality of the model will then depend on the quality of the transaction monitoring proces. This entails a risk that inefficient transaction monitoring processes may create bias in the applied models, cf. section 10.4.

The DFSA's evaluation of compliance with the rules for transaction monitoring in banks also showed that the use of machine learning techniques is not particularly widespread at present[8]. However, network analyses and the prioritisation of alerts as well as the calibration of existing scenarios and the development of new ones, show particularly good potential. Initially, therefore, machine learning techniques are thought to be useful as an effective tool in transaction monitoring and not as an alternative to existing processes, cf. section 10.1.

Under the auspices of the DFSA's innovation hub, the DFSA has followed developments in regard to the possibilities for better data sharing through the use of new technologies. Among other things, in 2019 the DFSA participated in the UK Financial Conduct Authority's TechSprint, which focused on how encryption technologies *(privacy enhancing technologies)* can

[7] FATF, Objectives 2020–2022,
[8] The starting point for the analysis of the possibilities for sharing risk flags, cf. section 10.

facilitate improved data and knowledge sharing in the sector[9]. This led to a subsequent dialogue with one of the participating companies, whose solution enables the merging of data from different companies so that transactions can be monitored on the basis of this merged data. The intention is to allow all relevant transaction data to be shared between, for example, all banks, without exchanging either personal data or payment data. The encryption ensures that all legislation is complied with, while improving the quality of transaction monitoring. Such a solution may, for example, make it possible to track the money through a network of banks. However, this solution also means that it must be possible to decrypt data, for example as a result of a court order, if the data is to be used as the basis for any investigation.

An example like this highlights the great potential offered by the use of more advanced technologies. However, the development and application of such technologies is still at an early stage. At the same time, obliged entities may also be reluctant to make major investments in such solutions, due partly to uncertainty about how to arrange adequate governance with such solutions, but probably also due to the risk associated with being a first mover.

The DFSA is therefore of the opinion that initatives based on advanced technologies are associated with a longer time frame before they can be used widely in practice. The authorities should continue to focus on closely following developments, and in particular on ensuring the appropriate guidance for the use of new technologies. In 2019, for example, the DFSA published its first proposal on what financial institutions should have in place before using supervised machine learning[10]. In particular, work such as this can support the sector in safely adopting new technologies.

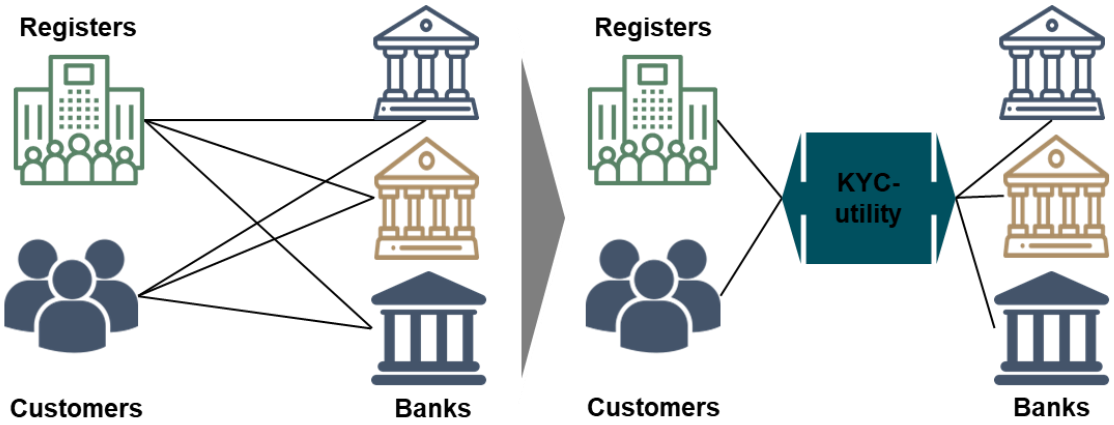
[9] Part of this event involved a number of companies competing to demonstrate how such technologies could best be used to combat money laundering and terrorist financing.
[10] The DFSA's *Recommendations when using supervised machine learning* – https://www.dfsa.dk/Supervision/Fintech/Machine_learning_recommendations

4. Sharing customer information through KYC-utilities

The DFSA recommends that the DFSA continue to follow and support the development of the KYC-utilities described and other similar ones. The focus should be on concretising challenges or opportunities and clarifying the extent to which it is regarded as proportionate to work towards the requisite infrastructural and legislative changes. This exercise should be supported by actual observations from KYC utilities, which can be obtained as they join the market.

The scope of information (master data) that must be obtained and verified as part of KYC procedures, particularly in relation to companies, can be extensive and resource-heavy. These resources could potentially be used more efficiently elsewhere if the collection and verification of customer master data could be standardised and centralised to a greater extent, cf. figure 4.1. Customers will also benefit greatly, as they can simply submit and update information in one place, and control who has access to this information from there.

Figure 4.1 – Increased centralisation through KYC utilities



Source: The DFSA

Banks themselves are in the process of developing various measures to undertake this task, thereby both improving the sector's efforts to combat ML/TF and reducing the costs of this. This is done by ensuring a common starting point and IT-infrastructure for the KYC procedures (KYC-utilities) where possible. The DFSA has continued to follow and to some extent guided two of these initiatives. Essentially, the purpose of these initiatives is to improve the return on the resources used in this area:

- A Danish initiative which seeks to improve KYC procedures in Danish banks for the segment of Danish private customers residing in Denmark.

- A Scandinavian initiative that gathers the information that is most necessary to banking KYC procedures for large corporate customers.

Other companies have also moved into this area.

The DFSA is of the opinion that the establishment of KYC-utilities is of significant value, as they reduce both hassle for customers and the amount of resources that obliged entities must

allocate in order to obtain adequate customer knowledge. The work of developing and implementing such measures should therefore be monitored and supported by relevant authorities to ensure effective implementation. This includes:

- Clarifying which customer information the obliged entities should obtain, where possible, including when customer information has been adequately verified. One premise for such work is that public solutions and registers must be accessible and credible, cf. sections 5, 6, 7 and 9.

- Further harmonisation and, where possible, standardisation of the anti-money laundering rules with regard to KYC procedures, including the definitions of the master data that the obliged entities must obtain and verify, cf. section 11. This applies to the definition of beneficial owners, for example.

KYC-utilities could potentially also help fortify the foundation of KYC procedures. They will have access to information about customers and their behaviour across a number of obliged entities, such as matches in the residential addresses of different beneficial owners across corporate customers in different banks. Further work should therefore also reveal whether there is any value in implementing the requisite regulatory changes to ensure that banks, etc. can access such information. It is also worth considering whether these solutions can support a higher quality of public records if effective feedback mechanisms are established.

However, none of these measures have yet been implemented in practice. Any concrete decision on the extent to which KYC-utilities can contribute more broadly than for the immediate purpose should therefore wait until actual observations as they enter the market are available.

4.1. Finance Denmark's standard for KYC procedures

As part of their report, Finance Denmark's Money Laundering Task Force published a vision for implementing a joint centralised KYC-utility. This vision is based on an objective of enabling KYC procedures to be performed differently from and more efficiently than today in the near future.

The standard for KYC procedures (the standard) is part of the first step (of three) in this vision[11]. It is the result of a sector-wide agreement, drawn up by a working group with representatives from a number of banks, the Money Laundering Task Force and other contributors. The DFSA submitted its comments regarding the standard on 19 December 2019.

The purpose of the standard is to ensure a common basis for Danish banking KYC procedures, thereby improving the quality on a sector level. The standard has three specific goals:

- To ensure a solid foundation for strong sectoral cooperation, including a common language and definitions.

- To help banks improve the quality of their documentation regarding KYC procedures.

[11] For further insight into this, please refer to the report prepared by Finance Denmark's Task Force.

- To support the long-term aim of being able to share information across the sector in order to better prevent or combat ML/TF.

The standard will not replace the risk-based approach to KYC procedures within each individual bank. Therefore, the baseline for its development was an agreement on the easiest subset: a minimum standard for Danish private customers who are resident in Denmark.

In connection with this, it is worth noting that the standard essentially consists of a number of check questions that banks should consider every time they initiate or update a customer relationship. This means there is no defined template that banks can follow slavishly in their processes. In addition, there is no clear guidance as to how each step, e.g. 'collecting customer information', should be performed. On the other hand, there are sources of information that the sector has agreed can be used.

The DFSA is of the opinion that the standard is important, in particular the vision of eventually establishing a KYC-utility. However, the value of such an initiative is to a large extent conditional on as clear a framework as possible being established for the content of KYC procedures.

Clarification of the content of KYC procedures
One way to support the sector in this work is to clarify which information the obliged entities can obtain in connection with KYC procedures and when the information is adequately verified. Among other things, this requires the authorities and the sector to remain in dialogue about which public registers and solutions the obliged entities can use, and in particular to what extent the quality of these is sufficient relative to the requirements of the MLA. In this report, the DFSA describes and recommends a number of initiatives that may help the sector to become more efficient, cf. sections 5, 6, 7 and 9.

In such guidance, the DFSA must weigh up the desire to support the sector with a view to still being able to maintain effective supervision of the obliged entities. This is a classic supervisory trade-off: the more guidance the supervisory authority provides, the more difficult it then is to supervise.

Under no circumstances is it possible to design a *one-size-fits-all* solution for KYC procedures. The risk classification of a given customer relationship must always determine the scope of the KYC procedures. Among other things, this means that some sources of verification will be adequate only for customers with a given risk classification, while more will have to be done for other customers.

Challenges such as these also emphasise the value of identifying the opportunities for further harmonisation of the requirements in the AMLD, cf. section 11.

4.2. KYC-utility within the framework of Invidem

Invidem is an initiative created by six large Nordic banks[12]. The aim is to establish a KYC utility that makes performing KYC procedures on large corporate customers in the Nordic

[12] Danske Bank, DNB, Handelsbanken, Nordea, SEB and Swedbank.

region more efficient[13,14]. Essentially, the solution will allow all banks to retrieve the requisite information about their corporate customers from one central location, while for corporate customers it means that they only need to update information in one place. The solution reflects a desire for savings among both banks and business. Among other things, there are examples of larger companies with between ten and a hundred employees whose job is to keep this type of data up-to-date with their financial counterparts. Invidem is a few steps further ahead of Finance Denmark, and their KYC-utility is expected to be implemented widely during 2021.

A minimum version will be established for potential subsequent expansion in the same way as for the Danish project. It is also true here that the individual bank cannot be certain that all required data can be retrieved. Information from Invidem must therefore be supplemented with information obtained by the individual bank where necessary.

The potential of a feedback mechanism

When a bank is forming a new customer relationship, the bank needs to obtain from the customer and verify a range of master data. The solution is intended to collect, store and continuously verify this data from the customer on behalf of the bank. The data is verified via a number of trusted third parties, such as the Danish business register in Denmark and equivalent registers in other countries. This means, among other things, that Invidem will be able to detect discrepancies between the data provided by the customer and data obtained from the various registers. These discrepancies may be caused by various factors: for example in some cases information about the customer is not reproduced correctly in public registers.

Everyone, including banks, has an interest in data in public registers being as accurate as possible, cf. section 5. It would therefore be beneficial to look more closely at the value of establishing an effective form of feedback mechanism by which data in public registers could corrected on the basis of observations made by such KYC-utilities. The DFSA understands that the dialogue regarding corrections currently takes place via e-mail, which can lead to inappropriately lengthy processing times and manual processes.

Harmonisation of the content of master data across national borders

Invidem's solution will initially be available across the Nordic countries. This means that, where possible, the content of relevant master data for banks must be standardised across countries. However, this may be difficult in some areas, including in relation to the definition of beneficial owners and the mapping of group structures. The AMLD, for example, does not provide a clear definition of beneficial owners. The way beneficial owners are defined in different countries may therefore vary. Similarly, the way different countries define a parent company may also vary. Such differences could have consequences for the quality of the solutions, including the potential for further integration and standardisation of KYC procedures across the Nordic region and the EU.

Further data sharing between banks through KYC utilities

The business model for KYC-utilities such as Invidem means that KYC-utilities will hold a large amount of information about different companies and their customer relationships with

[13] The project was originally known as KYC-Nordic.
[14] Eventually the aim is also for the solution to be extended to smaller companies.

banks. Situations are therefore likely to arise in which the aggregated data provides an overview of the companies, the relationships between them and the relationships with banks. This can provide KYC-utilities with knowledge that can help identify suspicious customers. For example, this could be knowledge of simultaneous onboarding with multiple banks or the same people appearing in customer relationships across banks, which the individual bank would not be able to identify on its own.

Being able to share this kind of insight more widely could help to improve protection and more effectively combat ML/TF across banks. This could for example be in the form of insight into the same people appearing as owners of multiple companies and insight into situations where different companies with connections to different banks share an address.

4.3. Legal considerations

Use of master data via KYC-utilities

The work of establishing the above-mentioned KYC-utilities implies that a kind of database will be set up, containing factual information about customers across banks. In other words, this is verified master data stored in a central location. This means that customers can simply provide information and have their so-called master data stored in one central location. Customers will know that all relevant data appears here, and banks can get access to all relevant data in the same place. As a minimum in order for the bank to access the collated data about a customer, the bank must obtain the customer's consent.

The initiative coincides with the opinions that have been expressed at EU level in connection with the creation of EU's AMLD. The following is stated in recital 35 of the preamble to the AMLD (excerpt):

> *"In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for customer due diligence should remain with the obliged entity to which the customer is introduced."*

Considerations regarding harmonisation

The above example indicates that, where possible, there should be harmonisation across national borders in relation to the data collected in order to create the optimal solution. Specifically, there have been differences in the approach to identifying beneficial owners, and there are also differences in how countries define a parent company, for example.

The requirements for the information that is to be collected in connection with banking KYC procedures stem from the EU directive, which applies in all EU Member States. As an example, the term 'beneficial owners' is defined in article 3, no. 6 of the 4th AMLD. The definition derives from FATF's recommendations[15]. This means that there will also be some similarity in the definition beyond the borders of the EU. However, it is possible for individual countries to lay down stricter rules.

[15] Recommendation no. 24 and accompanying interpretative note

In order to optimise the efficiency of the cross-border procedure, it may be necessary to ensure greater harmonisation of the standards for data collection, cf. section 11. Alternatively, the stored master data may form a kind of 'minimum package', and some banks in some countries will have to obtain additional information in addition to this data in order to comply with the law of their home country.

Sharing aggregated data under the auspices of KYC-utilities

A secondary effect of central collation of information on customers across companies and persons subject to the MLA for the purpose of KYC procedures is that the KYC-utility gets access to a wide range of data that can be aggregated centrally.

Such information can for example give insights about customers that simultaneously initiate customer relationships with several banks or information on the affiliation of natural persons with several different companies. Such information could be valuable information to include in the risk classification of customers.

The DFSA considers that such sharing of aggregated data with banks will involve the same legal considerations as the sharing of aggregated data under the auspices of the DBA's graph database, cf. section 9.1.

5. CVR as a source for verifying company information

The DFSA recommends that work be initiated with relevant actors, including the Danish Business Authority, Finance Denmark, FSR-Danish Auditors and the Danish Bar and Law Society, with an emphasis on mapping the conditions under which a mechanism can be established in CVR, whereby lawyers and authorised auditors can verify registered company information.

The MLA requires the obliged entities to obtain and verify identity information about their corporate customers while also taking reasonable measures to obtain and verify the identity of these customers' beneficial owners, including indirect owners in the event that the beneficial owner is a business.

For Danish corporate customers, it makes sense to use the Danish business register (CVR), which is managed by the Danish Business Authority (DBA), for this. The register contains all relevant master data about Danish companies, including name, address, business registration number (CVR number), members of the Executive Board and the Board of Directors, legal and beneficial owners and their addresses, and so on.

The credibility of data in CVR may in some cases be limited. This is because the companies themselves provide the information, which the DBA does only verify independently and manually to a limited extend. This correlates with the political will that it should be easier to be an entrepreneur, and with the fact that the DBA's available resources limit the opportunities to manually process all verifications.

The registration process for companies has therefore been automated. This means that a company enters the required information itself when it is registered or updated, and that the DBA based on an automated risk assessment only chooses a selection of these companies to be verified manually. This means that companies can obscure beneficial ownership or other information without it necessarily being discovered. The DFSA has therefore maintained until now that the obliged entities can only use CVR as a source for verifying company information for low-risk customers.

At the same time, however, the DFSA considers that a broader area of application for CVR in connection with KYC procedures through further digitisation could reduce costly manual processes within companies and persons covered by the MLA. This can be done, for example, by removing the need to obtain additional documentation from customers in cases where it is currently judged that CVR alone does not constitute an adequate source of verification.

The DFSA has therefore been in dialogue with the DBA concerning the credibility of data in CVR. This has provided a broader understanding of the relatively sophisticated system that is developed on an ongoing basis to verify data. That said, the DBA confirmed that it is still not certain in all cases that the information submitted in connection with company registrations and changes is correct. At the same time, data updates for companies registered in CVR may be delayed and potentially outstanding, as the companies themselves are also responsible for reporting changes, which does not necessarily happen immediately after the changes have occurred.

The DFSA has also been in dialogue with Invidem, which is developing a KYC-utility for a number of Nordic banks focusing on larger corporate customers, cf. section 4.2. Invidem's solution is therefore dependent on the availability of credible business registers and makes use of such registers in a large number of countries. Invidem noted that CVR is top of the list in terms of data credibility, despite the fact that the organisation continues to observe erroneous registrations[16].

If CVR is permitted to be the sole source for verifying company information, this would limit the ability of the DFSA and other authorities to sanction and respond to obliged entities in regard to their KYC procedures. This could be the case, for example, in situations where data from CVR is inaccurate, but is still used in KYC procedures for corporate customers, resulting in a risk of suspicious customers being overlooked. Examples of such situations are:

1. Companies for which the publicised ownership and control structure is inaccurate, e.g. straw man companies.

2. Relevant company changes which may have consequences for the customer's risk assessment and which are not stated in CVR.

The DFSA is therefore of the opinion that CVR, as it is today, cannot be the sole source for verifying company information without this having consequences for the impact of efforts to combat ML/TF. One possibility for using CVR more broadly would be to give lawyers and approved auditors access in order to verify company information in CVR. This presupposes that:

1. Under the auspices of the DBA, functionality is implemented by which lawyers and approved auditors can verify the registered information.

2. A decision is made as to how long verification is valid for, as the KYC procedures should only accept valid verifications.

3. Lawyers and approved auditors are willing to take on the responsibility in practice and companies that implement KYC procedures will bear the associated cost.

5.1. The requirements of the Money Laundering Act

Article 11, section 1, letter b) of the MLA states that the obliged entities must obtain identity information on corporate customers (legal persons), and section 11, paragraph 2 states that this information must be verified on the basis of an independent and reliable source.

The DFSA's guidelines for the MLA[17] specify that the scope of these verifications depend on a risk assessment. In some cases, looking up a Danish company in CVR will suffice. More will be required in other cases, such as obtaining information from the Danish Tax Administration or a copy of the articles of association and incorporation documents.

[16] The purpose of KYC-utilities is to validate customer information obtained as part of the financial companies' KYC procedures and to continuously update this information. A number of sources are used for verification for this purpose, and in some cases they will therefore become aware of discrepancies between information in CVR and the actual situation in the companies.

[17] https://www.finanstilsynet.dk/-/media/Tilsyn/hvidvask/seminar/Hvidvaskvejledning_November_2020.pdf

Section 11, subsection 3, of the MLA also states that the obliged entities must obtain the identity information on the beneficial owner(s) of a given company and implement reasonable measures to verify the beneficial owners' identity, so that the obliged entities know with certainty who the beneficial owner(s) are. If one or more beneficial owners is a legal person, the obliged entities must take reasonable measures to clarify the overall ownership and control structure.

This is a specific risk assessment with regard to how in-depth examinations initiated by the obliged entities must be to clarify the individual customer's ownership or control structure. In low risk cases, an organisation chart showing shareholdings or information obtained via CVR may be sufficient, while in other cases it may be necessary to obtain proof of shareholdings in the form of articles of association or the like.

5.2. Known issues regarding corporate customers

When corporate customers set up accounts for criminal purposes, they will in many cases use so-called straw man companies. A straw man company is a company in which the appointed management, beneficial owners and so on are generally genuine individuals who do not have a criminal past, but who also do not, in practice, have anything to do with the company. Instead of being able to act on behalf of the companies, they will have passed on the necessary identity information to criminal actors, either intentionally or unintentionally, cf. section 6.5. The primary challenge associated with allowing CVR to stand alone as the sole source for verifying this type of company information is therefore that there is no guarantee that the registered identities also operate and own the company in practice.

In addition, there is a risk that even companies that want to comply with the requirements of the law do not always update the relevant information when there are changes, for example, in the ownership and control structure. In some cases, such changes may mean that the risk classification of the customer relationship should be changed, for example by transfers of ownership interests from a Danish company to a foreign company in tax havens or similar.

5.3. The control environment for records in CVR

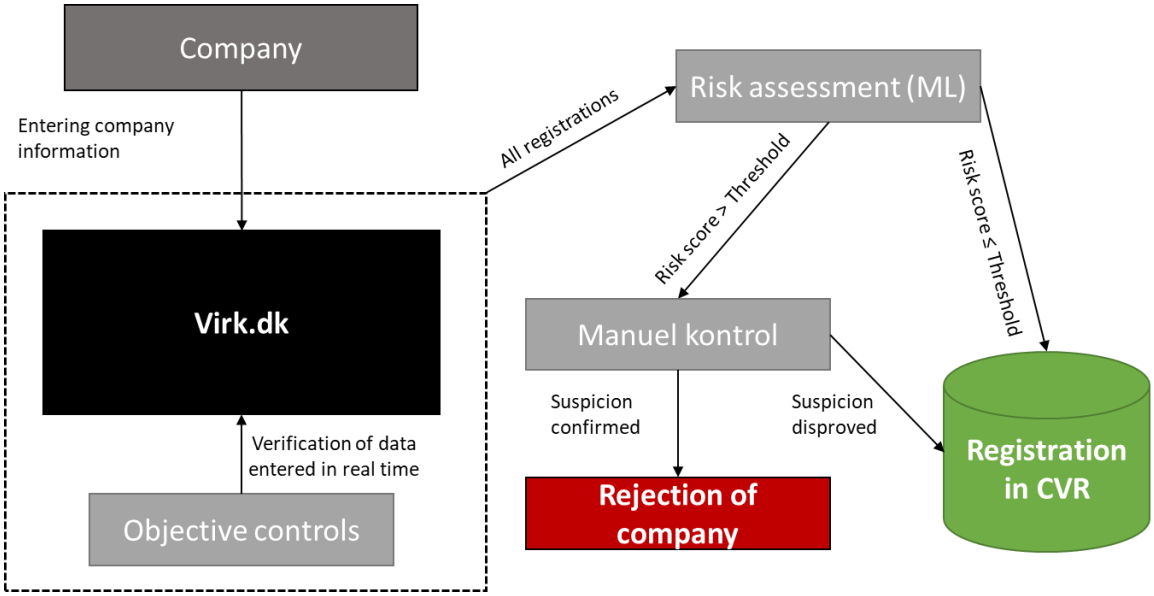
The DFSA and the DBA have discussed the measures that have been implemented to ensure that companies are not set up with incorrect data or that companies are not set up on a false basis.

In general terms, CVR is limited by the fact that companies themselves are responsible for registering relevant changes. This makes it difficult to let the register stand alone as a source for verifying company information. CVR also contains Danish companies only. This means that the obliged entities that have to map the ownership and control structure find that the trail stops when the legal owner is a foreign company. In these cases, they are dependent on foreign business registers or similar to map the full ownership and control structure.

Figure 5.1 shows the overall process for digitally registering a company in CVR or subsequently updating relevant information. The company enters the required information, which undergoes checks based on objective criteria in real time. An automated risk assessment of the company is then performed. The actual risk score is intended to indicate the likelihood of

the business being set up for a purpose other than that described. Companies with a risk score above a predefined threshold are sent for manual verification and are only registered if the risk is disproved. All other companies are registered directly in CVR.

Figure 5.1 – Process overview for registering a company in CVR



Source: The DFSA.

Objective controls

The DBA's web platform has a number of so-called objective controls built in, and where possible, these compare the master data that has been entered with other sources to verify that the information is correct. These controls also act as natural blocks to further registration. If the information cannot be verified, the registration cannot be continued. Examples of these objective controls are:

1. Verification of social security numbers (CPR numbers) entered by cross-checking with the social security register (CPR) – does the registered CPR number exist, and do names, etc. correspond to the information entered?

2. Linking foreign individuals without a CPR number with known individuals with the same passport number.

3. Cross-checking of address with the Danish Central Register of Buildings and Dwellings – does the registered address exist, are there buildings at the address, and are other companies registered at the address?

Selection for manual verification

The risk assessment is carried out using machine learning and takes place in real time. The system uses a number of machine learning models, each with its own focus area, all of which are trained on the DBA's data[18]. This means that risk for new companies is assessed on the

[18] Also involves records from other authorities, due to the DBA's relatively broad legal basis for collecting data, cf. the Act on the DBA's processing of data of 8 May 2018.

basis of historical observations about companies. Some models focus on previous conditions, for example whether a registered beneficial owner has previously been involved in setting up and liquidating a lot of other companies. Others can be used to verify the credibility of a specified passport number or address for a foreign individual. More advanced models look at general patterns for the specific company, for example, observing new contexts that differ from previous ones. One characteristic of the models is that they become better and more accurate as more data is accrued about a given company. The models will thus be able to assess the risk better when the company has been registered for a longer period and has submitted annual reports, and so on.

In addition, the DBA itself determines the thresholds for the individual models on which selection for manual verification is based. The values are determined on the basis of an assessment of the model's results (both when it is developed and when it is used), and a balance between appetite for risk and the available resources. This is also in line with the political priority of making it as easy as possible to set up a company. Conversely, it also means that companies with a criminal purpose, which in the current control environment are not assigned a risk score above the established threshold, will be registered immediately in CVR.

The possibility of objecting to registration

While the control environment is both extensive and of high quality, the credibility of data is still limited by the fact that it is the companies themselves that are responsible for registering the requisite information. In other words, there is still a risk that skilled criminals could succeed in obscuring the intent of a business registration.

The objective controls help to ensure that individuals, addresses, and so on are genuine. However, they do not involve any verification of whether the information for the given company is correct. In addition, the checks are particularly limited for foreign individuals, since, for good reasons, they cannot be assigned a CPR number, but only a name, address and passport number. The risk assessment adds an extra layer of security, but it cannot guarantee that all potential criminal companies are manually examined by caseworkers.

In regard to verifying the identity of associated individuals, however, an extra layer of security is built in when registering individuals in CVR. Danish individuals receive a notification about their registration in their e-Boks[19], while foreigners receive physical mail at the specified address. The purpose of this is both to make people aware of their registration and to give them the opportunity to object to the registration.

For Danish individuals, this extra layer of security may be considered as being particularly effective in avoiding unintended registrations. On the other hand, if the registered individual is aware of the registration and the use of the person’s identity beforehand, the mechanism is likely less efficient, as the incentive to object will not exist. In the case of foreigners, the security layer is particularly limited. This is because the physical letter is sent to the address that the company itself has registered for the individual.

[19] An electronic mailbox available for and normally used by all Danish people.

5.4. Verification by lawyers and approved auditors

In relation to the requirements of the MLA, the DFSA is of the opinion that the existing control environment does not adequately ensure that CVR can be used more broadly as a source for verifying company information. If CVR is accepted as an adequate source, one potential consequence is the lowering of barriers for criminals. Among other things, this would limit the abilities of the DFSA and other authorities to sanction or respond as a result of inadequate KYC procedures. If it is communicated that it is sufficient to verify the necessary information in CVR, the authorities cannot then blame the companies for doing just that.

The problem, as mentioned, is that the quality of data in CVR is not always sufficient. However, this issue could potentially be addressed by giving lawyers and approved auditors the opportunity to verify company information in CVR. This is because they are in a trusted profession and such a mechanism can be equated with other attestations through which lawyers and approved auditors assume responsibility on behalf of their clients. This applies, for example, to an auditor's opinion issued by an approved auditor for an annual report. As lawyers and approved auditors are also subject to the MLA, they should be able to carry out the verification on the basis of the information they themselves obtain as part of their KYC procedures. Such verification of the information in CVR should therefore be able to assure the obliged entity and the DFSA that the information and identities stated are accurate. If this is not the case, the responsibility can be returned to both the company and the lawyer or the approved auditor who has completed the verification.

Since in many cases it is also lawyers and approved auditors who set up companies and update data in CVR on behalf of their clients, the task of verification could be viewed as a natural extension of their role. At the same time, the remuneration is likely to make up a smaller proportion of the overall fee.

Such a mechanism need not be implemented as a requirement for a company to be registered in CVR. On the other hand, creating the opportunity will enable corporate customers to choose for themselves if they feel that the benefits are substantial enough. For example, they will not have to submit documentation to their bank when company changes occur or when customer knowledge is being maintained, which can be an expensive process, especially for larger companies[20]. Rather, they can merely ask the approved auditor or lawyer to revalidate data in CVR. At the same time, companies and persons subject to the MLA will have a financial incentive to demand the implementation of such verification. This is partly due to the fact that they will need to use fewer resources on verifying company information as part of the KYC procedures.

For this functionality to work, however, it is crucial that a clear framework can be established as to the length of time for which a verification can be considered credible, and that the specific information that has been verified is clear. Among other things, it will not be appropriate if the company structure is adjusted after an approved auditor has verified it in CVR and the change is not registered in CVR. However, this can be resolved by requiring that information can only be used if the verification has been updated. For example, there could

[20] Among other things, there may be examples of larger companies with between ten and a hundred employees whose job is to keep this type of data up-to-date with their financial counterparts, cf. section 4.2.

be a requirement for periodic updating of the verification and for the risk classification of a given customer to determine the frequency.

In general terms, the DFSA is of the opinion that increased use of CVR to verify information about corporate customers should be investigated in more detail, taking into account the potential benefits associated with this.

6. Verifying identities using MitID

The DFSA expects that it will be possible to use MitID (MyID) to verify customer identities beyond the capacities for which NemID (EasyID) can currently be used. We will only know this for certain when the MitID Act enters into force and MitID has been issued to a broad cross-section of people in Denmark. The ongoing development of the MitID solution should therefore be monitored closely with this aim in mind.

As part of their KYC procedures, companies and persons subject to the MLA must identify and verify the identity of their customers. There are currently several ways of doing this. What is 'adequate' depends both on the risk classification of the customer relationship and on whether the customer shows up in person.

Customers who do not show up in person at the company or the person subject to the MLA are known as distance customers. A widespread approach to verifying the identity of these customers is currently through the submission of copies of a number of identification documents, such as passports, driving licences and health insurance. NemID is also a widely used source of verification. However, the DFSA only allows NemID as the sole source of verification when the customer, as a result of the risk classification, is subject to simplified KYC procedures. In other cases, additional documentation will need to be obtained.

For a long time, many players in the sector have called for NemID to be used more broadly and act as the sole source of verification, at a minimum, for all distance customers who, due to the risk classification, are not subject to enhanced KYC procedures. This is due to the fact that customers are increasingly onboarded without turning up in person, and also to the fact that the processes regarding verification of identity information today are often manual and therefore associated with significant costs. At the same time, many consumers find it intrusive that they regularly have to submit documentation to, for example, their bank, such as their passports. Finally, submitting copies of identity documents is not necessarily the safest way to verify customer identities, and there is potential not only for easier and less intrusive verification, but also for more secure verification.

The DFSA's assessment of the scope of application of NemID dates back to 2013. The limited scope of application was primarily due to the fact that anti-money laundering rules have historically been arranged in such a way that distance customers were, by definition, subject to enhanced KYC procedures. In recent years, there has been growing acknowledgement of the need to use electronic identity solutions on an equal footing with physical identity papers. For example, both the AMLD and the associated guidance issued by the EBA open up the possibility of making more extensive use of electronic identity solutions. A framework for assessing the security of these solutions has also been implemented in the form of the eIDAS Regulation, which aims to support cross-border use of electronic identity solutions[21].

Despite this development, the DFSA maintains its assessment of the scope of application of NemID in the November 2020 guidelines for the MLA[22]. This is due to concerns about the level of assurance in the NemID solution, in particular the fact that the processes for verifying

[21] Regulation (EU) No 910/2014 of the European Parliament and of the Council.
[22] https://www.finanstilsynet.dk/nyheder-og-presse/sektornyt/2020/hvidvask_vejledning_031120

identities when issuing NemIDs have historically been inadequate relative to the requirements of the MLA, cf. section 6.4. At the same time, the DFSA understands that criminals often use disclosed NemIDs for their activities, cf. section 6.5.

In Denmark, the Danish Agency for Digitisation is well on its way in developing a new electronic identity solution, known as MitID, which will replace NemID. The purpose is to create a more secure solution than NemID, which can therefore be used more widely in both public and private settings. MitID is not yet fully developed, but is expected to be available during 2021.

Based on the current design of the solution and the DFSA's current guidelines on adequate verification processes for distance customers, the DFSA has taken a closer look at the scope of application of MitID. The analysis compares the challenges of NemID with the opportunities inherent in MitID:

1. The security of the MitID solution, including in particular the verification of the identity of the persons to whom a MitID is issued.

2. The extent to which the solution can help reduce the risk of a customer relationship being abused as a result of the disclosure of a MitID.

The DFSA is of the opinion that a MitID at a 'substantial' level under the eIDAS Regulation could act as the sole source of verification for distance customers who are not subject to enhanced KYC procedures. This is because the processes for verifying identities when issuing a MitID are at least as secure as the DFSA expects is the case, in principle, for distance customers under the MLA, cf. section 6.7. In addition, the assurance level of the means of authentication in the MitID solution is higher than in the NemID solution.

One condition is that companies and persons subject to the requirements of the MLA continue to organise their procedures for the risk classification of customer relationships in such a way that the risk of misuse as a result of the disclosure of a MitID is sufficiently reduced.

The DFSA assesses that the MitID solution can also support these processes, cf. section 6.7. This is due to the possibility that MitID brokers[23], by using so-called risk data, are able to establish additional checks that, among other things, can serve as indicators of disclosure. This is conditional on that it is ensured in the MitID Act that companies are able to include the outcome of the extra security layers in their KYC procedures.

Communication about any scope of application for MitID that is broader than NemID will have to be carried out via an update to the DFSA's guidelines for the MLA. In connection with this, it should be emphasised that the DFSA's assessment relates exclusively to verifying the identities of customers. Companies and persons covered by the MLA will still need to perform other necessary elements of the KYC procedures[24].

[23] Access for service providers (banks, etc.) to the MitID solution, cf. section 6.4.
[24] In some specific customer relationships, it may be necessary to obtain other details, e.g. on the purpose and intended nature of the business relationship, cf. section 1, and on the customer's finances, and so on.

The assessment presupposes that the further development of the MitID solution does not change the conditions on which the assessment is based.

6.1 Focus on broader use of electronic identity solutions in the EU

Historically, the anti-money laundering rules have stated that the establishment of customer relationships with distance customers is by definition associated with an increased risk of money laundering and terrorist financing. Article 12(2) of the AMLD3, which entered into force in 2005[25], stated specifically that:

> *"Where the customer has not been physically present for identification purposes, Member States shall require those institutions and persons to take specific and adequate measures to compensate for the higher risk."*

This specific requirement lapsed with the implementation of the AMLD4 in 2015[26]. The wording changed to specify that the KYC procedures should be performed using a risk-based approach. This means that enhanced KYC procedures do not have to be implemented automatically for distance customers. The amended version of AMLD4 from 2018 further emphasises that regulation should be technology-neutral[27]. Recital 22 in the preamble emphasises that the latest technological developments in the digitisation of transactions and payments enable secure remote or electronic identification and that the use of such means of identification should be taken into account in the light of the eIDAS Regulation.

The same view is expressed in the revised guidelines for AMLD, which were prepared by EBA in collaboration with ESMA and EIOPA[28]. The guidelines focus on companies' KYC procedures, including which risk factors companies must be aware of in connection with the risk assessment and risk classification of the customer relationship.

Sections 4.29, 4.30 and 4.31 of the guidelines refer specifically to distance customers. Sections 4.29 and 4.30 state that companies must take sufficient steps to ensure that:

1. the stated identity and the actual person are the same,
2. the company shall take a position on whether the fact that the customer relationship is not established physically results in a higher risk, and
3. whether enhanced KYC procedures must be performed, including an assessment of whether enhanced verification procedures are necessary if the customer relationship is associated with an increased risk.

However, section 4.31 states that the use of an electronic identity solution as a source of verification does not, in itself, give rise to increased risk. Particularly not if the assurance level can be classified as 'high' under the eIDAS Regulation:

> *"Firms should have regard to the fact that the use of electronic means of identification does not by itself give rise to increased ML/TF risk, in particular where these electronic means provide a high level of assurance under Regulation (EU) 910/201420."*

[25] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005.
[26] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015.
[27] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.
[28] EBA guidelines (EBA/GL/2021/02) of 1 March 2021.

At the same time, section 4.33 notes that companies that make use of technological solutions must assess whether such solutions manage or potentially increase the risk of ML/TF. The risk of identity fraud is among the examples highlighted.

The change reflects a recognition that onboarding of distance customers does not necessarily lead to higher risk if credible electronic identity solutions are used[29]. FATF stated the same thing in their March 2020 Guidance on Digital Identity[30].

In light of this, the DFSA is of the opinion that a decision should be made as to the circumstances in which MitID and other similar electronic identification solutions can be used in connection with companies' KYC procedures.

6.2. The Danish FSA's assessment of NemID in 2013

On 13 March 2013, the DFSA published a specific assessment of the scope of application of NemID[31]. The assessment still applies. It stipulates that NemID with an associated Danish Digital Signature (OCES certificate) can be used as the sole source of verification for low-risk customers if:

1. The customer signs documents using NemID as confirmation of the customer's name (identity), and

2. the company compares the information received from the customer with the information in the CPR register to confirm the customer's address and CPR number.

The assessment that NemID can only be the sole resource (together with CPR number) for verification of low-risk customers identities was based on the MLA then in force, from 2013[32], section 19, subsection 2 of which laid down a specific requirement for companies to implement stricter verification procedures for distance customers[33].

> *"When the customer has not been physically present for identification purposes, the undertaking or person shall take further measures to ascertain the customer's identity."*

The requirements in section 19 were implemented in 2006 as part of the implementation of AMLD3. The remarks on section 19, subsection 2 of the Bill state that[34]:

> *"Stricter attention may be paid, for example, by receiving supplementary identification. If the ordinary identification is ascertained via, for example, a driving licence or pass-*

[29] Recital 18 in the preamble to AMLD4 states: "This Directive should also apply to activities of obliged entities which are performed on the internet." Recital 19 also states: "New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk."
[30] "Non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk."
[31] www.finanstilsynet.dk/Tilsyn/Tilsynsreaktioner/Vejledende-fortolkninger/Hvidvask-12-19-NemID
[32] Executive Order on the Act on Measures to Prevent Money Laundering and Terrorist Financing of 13 August 2013.
[33] From remarks regarding section 19, subsection 1, it appears that at that time, distance customers were by definition associated with increased risk: "The stricter identification measures must be based on an assessment of risk and in situations which inherently involve an increased risk of money laundering and terrorist financing."
[34] Legislative Bill on Preventive Measures to Combat Money Laundering and Terrorist Financing proposed on 9 November 2005.

port, the supplementary identification could be, for example a health insurance certificate. The submitted documents can be verified, for example, by comparing the documents or, in the case of a document issued by one of the aforementioned companies or persons, by requiring an attestation of the document."

No specific position is taken on the scope of application of NemID in the remarks on section 19, subsection 2. A review of the subsequent amendments to the MLA of 13 August 2013 reveals that neither section 19 nor the remarks thereon have been amended since they were included in the MLA.

A review of the historical documents relating to the DFSA's assessment of the scope of application of NemID also implies that the assessment was based on section 19, subsection 2. For example, on 4 February 2011, the DFSA referred to section 19, subsection 2, in response to a written official question from a member of parliament directly to the minister (paragraph 20 question)[35]:

"In cases where a customer does not appear physically to identify himself, the Money Laundering Act requires companies to take additional measures to ensure the customer's identity. This may mean obtaining supplementary documentation, or a requirement for the documents submitted to be certified by a relevant authority or lawyer.

"This therefore means that, when establishing a customer relationship, companies cannot rely solely on digital signatures or NemID, as the Money Laundering Act places additional obligations on companies."

The exception for low-risk customers was therefore a relaxation relative to the wording of both the MLA in force at the time and AMLD3.

6.3. The Money Laundering Act after AMLD4

In 2017, the AMLD4 was implemented in Danish law. Among other things, this meant that section 19 of the MLA in force at that time lapsed. The remarks state the following[36]:

"In accordance with the 4th Anti-Money Laundering Directive, the Ministry of Industry, Business and Financial Affairs believes it appropriate to limit the number of cases for which the Act sets stricter requirements for KYC procedures. This means that the fact that a customer has not been physically present to identify himself will not automatically entail an increased risk of money laundering and terrorist financing in the future. This will depend on a specific risk assessment instead."

In addition, section 11, subsection 3 states:

"Companies and entities shall implement all customer knowledge requirements, cf. subsections 1 and 2. However, the scope of the KYC procedure can be implemented based on a risk assessment."

[35] The question was: "Does the Minister agree with the Danish Bankers Association that NemID or a digital signature is not sufficient to identify a bank customer in relation to the 'Anti-Money Laundering Act'?"
[36] Legislative Bill on Preventive Measures to Combat Money Laundering and Terrorist Financing proposed on 13 October 2016.

The obliged entities have thus been given greater flexibility in determining their procedures, but continue to be responsible for ensuring that the procedures are adequate. The verification of customers' identity information remains a sub-element of the companies' KYC procedures, but the specific requirements in regard to distance customers have been dropped.

The risk classification of the customer relationship forms the basis for the scope of the KYC procedures. In regard to verification of a customer's identity, the risk classification primarily influences the scope of the processes, i.e. the number of verifications that must be carried out for a particular identity.

In the guidelines for the MLA, the DFSA describes a number of measures that can help to ensure adequate verification of the identity of distance customers, and maintains that distance customers may be associated with increased risk. This is attributed to factors such as the fact that a photo ID sent over the Internet does not provide the same security as the customer showing up in person with a photo ID.

The guidelines also touch on the use of NemID and other forms of electronic identity solutions as a source of verification and clarify that NemID can be regarded as a reliable and independent source, on the same level with passports or driving licences. In line with the assessment from 2013, they reiterate that NemID can only act as the sole source of verification if the customer is subject to simplified KYC procedures. In other cases, other sources of verification or mitigating measures must be included together with NemID.

The fact that NemID can only act as the sole source for customers subject to simplified KYC procedures is due to a concern stemming from the fact that the process for verifying identities when onboarding people to the NemID solution has historically not been secure enough[37]. At the same time, the associated keycard[38] is relatively easy to disclose to criminals along with other relevant information, so that an identity can be misused for the purpose of ML/TF. For example, it is easy to take a picture of the physical keycard and send it in an e-mail together with a CPR number and password.

6.4. MitID uses better security than NemID

The MitID solution is being developed and will be operated as a collaboration between the Danish Agency for Digitisation and Finance Denmark (the MitID partnership). Unlike NemID, which was owned and controlled by Nets and operates as two separate systems (a hybrid public and private solution), MitID will be one unified system (the MitID core). It has a number of security benefits, and the architecture is also easier to expand as new needs and threats arise. Furthermore, only one public electronic identity solution will be available in the future.

An assurance level of 'substantial' under eIDAS is the starting point

The MitID solution will be registered at two assurance levels (substantial and high) under the eIDAS Regulation. The overall assurance level is determined on the basis of an assessment of three factors:

[37] This is partly due to the fact that digital signatures were migrated to NemID and, in particular, to the fact that banks have handled the issuance of many NemIDs without adequately verifying the identity relative to the MLA.
[38] Part of the security measures in NemID is that a login is verified. Traditionally this has been done using codes that are issued to users of NemID on a physical keycard.

- **Identity Assurance Level (IAL):** Describes the strength of the registration process, including the identity assurance process, i.e. how secure the issuance of a MitID is.

- **Authenticator Assurance Level (AAL):** Describes the assurance level of the means of identification that can be used for verification, i.e. how secure the use of MitID is.

- **Federation Assurance Level (FAL):** Describes the assurance level of the MitID solution itself, i.e. the security of both the solution and the providers included in the solution.

In MitID, the assurance level is calculated as the minimum of IAL, AAL and FAL. It is expected that MitID will most commonly be issued at the 'substantial' level.

The starting point for the identity assurance process (issuance) under MitID is that the person being issued a MitID is physically present and provides proof of identity which is recognised by the state and checked for validity, for example a passport. A number of other checks are also carried out, for example comparing the information provided for persons with a CPR number with information in CPR[39]. The requirements are more restrictive than the requirements that have historically applied to NemID, and also correspond to the requirements for proof and verification of identity at an assurance level of 'high' under the eIDAS Regulation, cf. section 2.1.2. of the eIDAS Implementing Regulation[40].

However, the use of the right technology can ensure that equally secure verification methods can be established to verify identity for issuance to distance customers. For example, many new passports have a built-in chip which, when scanned, provides access to a photograph of the owner, among other things. By establishing the right processes, scanning the chip in a passport can be as secure as the individual appearing in person. An example is the use of digital facial recognition technology, which can be compared with the photograph of the person in the passport. The partnership is therefore also considering the extent to which such alternatives can be used, for example by onboarding through an app. Such methods are particularly relevant for users who are to be migrated from NemID to MitID. Requiring all users to show up in person at, for example, a local Citizen's Assistance service centre to be issued a MitID would be a costly and time-consuming process. However, MitIDs with an assurance level of 'substantial' or 'high' will only be issued, whether as new IDs or via migration from NemID, if the identity verification is assessed as being as secure as if the individual had attended in person.

The primary difference between a MitID with an assurance level of 'substantial' and one with an assurance level of 'high' is thus not the process of identity verification, but rather the associated means of identification.

The keycard that we know from NemID will not be used with MitID. The means of identification instead include an app, a key viewer, a chip solution and a key reader. The first two solutions are primarily aimed at ordinary citizens, who will have access to the app as an

[39] Other possible checks are validation of passports/driving licences in the Danish National Police register, checks by witnesses, other authenticity and validity verification of identity documents, and so on.
[40] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

authentication mechanism, which is a security upgrade compared with the keycard[41]. The MitID chip is primarily aimed at users with access to sensitive personal information. Key readers are aimed at citizens who cannot read a key, such as people with visual impairment and blindness.

The following requirements apply to an authentication solution for an assurance level of 'substantial', cf. section 2.2.1 of the eIDAS Implementing Regulation:

1. The electronic identification means utilises at least two authentication factors from different categories.

2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.

For an authentication solution for an assurance level of 'high', the same requirements apply, with the addition of the following:

3. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential.

4. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

The app is not expected to be able to achieve an assurance level of 'high'. This is not due to the security of the app itself, but rather the security of the platform on which it is installed (for example a mobile phone). Some European authorities still have doubts as to whether the hardware in a mobile phone or computer can withstand attempts at duplication or tampering.

On the other hand, it is expected that the MitID chip will be registered with an assurance level of 'high'. However, there are more costs associated with issuing a MitID chip compared to the app. It will therefore only be issued in specific cases, unless the user pays for it. Specific cases could include a person who has access to sensitive personal information in the public domain, such as personal health data.

Additional security layer at the broker

The MitID core handles the critical functions of the solution such as registering identities in an ID database and issuing means of identification. Users of the solution will only access the core through so-called MitID brokers, which are responsible for integration between the MitID core and the service providers. The contractual relationships will therefore be in three tiers (core-to-brokers and brokers-to-service providers) rather than the two-tier system (core-to-service providers) that applied under NemID.

Among other things, this means that, for example, if a customer wishes to use MitID to log into online banking, this takes place through a broker. The broker receives the user's log-in

[41] This is because 1) there is an additional layer of security in the form of entering a PIN for both phone and username and PIN for the app, and 2) the app – and MitID generally – can only be used in real time (authentication is only sent to the app after the username and password are entered in the log-in window) compared with the keycard (where all keys can be accessed as soon as the keycard is in the owner's possession).

information when it is used to access the service provider and forwards it to the core for authentication. The authentication response is then returned to the broker along with a selection of risk data, including an indication of the assurance level for the given MitID. The broker may use this risk data to build additional security layers, cf. section 6.7. For example, this could be information about the user's geolocation or number of failed log-in attempts, which the service provider can use to assess whether the correct user is using the MitID.

6.5. Disclosures and misuse of NemID in practice

The DFSA has been in dialogue with relevant authorities to identify how disclosed NemIDs can be misused in practice.

There are generally two ways in which a NemID can be disclosed: intentionally and unintentionally. Intentional disclosure is if a person, after issuance, knowingly transfers the NemID to a third party, for example by selling it. People may also be forced to disclose the NemID, or deliberately allow another person to use it without examining why. Unintentional disclosure occurs if a NemID is used without the holder being aware of it. This can happen, for example, if a criminal eavesdrops on a username and password and copies or steals the associated keycard.

It is the DFSA's understanding that intentional disclosure of NemID represents a significant challenge in regard to the fight to combat ML/TF. The problem typically arises when a criminal gains access to a number of NemIDs. This allows the criminal to gain access to, for example, a number of bank accounts set up by other individuals, which can be used to obscure the origin of funds or other forms of ML/TF. This can be done through both private customer relationships and customer relationships for companies in which a particular person is employed as a straw man, cf. section 5.2. This is particularly problematic, as in court it can be difficult to prove that the person whose NemID has been used was aware of the disclosure of the NemID and that the person was aware of the purpose.

The DFSA's understanding is that the use of more than one source to verify a customer's identity (for example NemID and a copy of a passport) will not necessarily counter the problem of intentional disclosure of NemID. This is because people who are willing to disclose their NemID will in most cases also be willing to pass on other identity documents such as passports and driving licences. The disclosure issue thus primarily relates to the fact that, in practice, it is very difficult to continuously verify the identity of a customer who is not physically present when a transaction is initiated. This applies, for example, when a payment is made through a customer's online bank.

6.6. The approach in other Nordic countries

The DFSA has discussed the scope of application for electronic identity solutions in general with the supervisory authorities in Norway, Sweden and Finland. The aim of these discussions was to clarify the extent to which such solutions are permitted to be used as the sole source of verification. That said, none of these countries offer a public solution, although various sectoral solutions are available. The most widely used solution in Sweden and Norway is known as BankID.

In general, the attitude across the Nordic cooperation is that electronic identity solutions should in principle be able to act as the sole source of verification of identities. In particular, this is because the current level of technology means that solutions can be made highly secure and in some cases more secure than existing practices for verification of identities. In connection with this, all three countries also referred to the eIDAS Regulation, but there were differing messages as to whether the level of assurance should be 'substantial' or 'high'. All countries agreed that the risk classification should continue to trigger further steps for verification of identities, for example based on the risk of disclosure.

The Norwegian Financial Supervisory Authority followed up the dialogue via e-mail and confirmed that, in principle, they permit the use of electronic identity solutions, cf. section 4-3, sentence 3 of the Norwegian Money Laundering Regulation[42]. They also pointed out that the assurance level of the solution should be 'high' under eIDAS, and maintained that the scope of application should always be contingent on a risk classification of the customer relationship due to the risk of disclosure.

6.7. MitID in relation to the requirements of the Money Laundering Act

The intention is that regular users will be issued a MitID at an assurance level of 'substantial' and will use the key app as a means of authentication. The DFSA's assessment is therefore based on this scenario.

In principle, MitID is adequate

The assessment of whether a MitID can act as the sole identification factor for distance customers is based on the following example of an adequate scenario for a Danish customer who is not subject to enhanced KYC procedures:

1. The customer provides their name and CPR number.
2. The customer signs with an OCES-certified NemID, and the CPR number is compared with CPR.
3. Additional verification documents are obtained, for example in the form of a copy of the passport or payslip.

In the above example of an adequate identification scenario, the identity is verified first and foremost through the use of NemID and CPR. However, the obliged entity must also carry out further verification procedures by obtaining a copy of a customer's passport. The purpose is primarily to ensure that the NemID that is used has actually been issued to the person to whom it is registered.

As described in section 6.4, the identification process when issuing MitID involves the customer turning up in person with a passport, or the obliged entity carrying out a similar secure check on the customer's identity. In addition, the information provided is also compared with CPR.

The DFSA therefore considers that a MitID issued at a 'substantial' level should be a sufficient source of verification for customers who are not subject to enhanced KYC procedures. This

[42] Regulations on measures to combat money laundering and terrorist financing of 14 September 2018.

is because, in principle, the process for verifying identities when issuing a MitID is at least as extensive as that currently required by the MLA.

The assessment is also supported both by the EBA's Guidelines for the AMLD, cf. section 6.1, and by the fact that the additional security of receiving a copy of identification documents in terms of being able to detect activities as a result of disclosed identities is marginal, cf. section 6.5. At the same time, the assessment is largely considered in line with the approach taken by our Nordic neighbours, cf. section 6.6.

The DFSA is also of the opinion that other electronic identity solutions can act as the sole source of verification of a customer's identity if the assurance level is in line with that stated in the assessment of MitID and the customer is not subject to enhanced KYC procedures.

The risk of disclosure should be included in the risk classification

A MitID with a high degree of security being issued to the right person is not enough if it is easy to pass on. The obliged entities should therefore continue to assess whether it is necessary to subject a given customer to enhanced KYC procedures and thus take further risk mitigation measures in connection with verifying an identity. In practice, disclosures, primarily intentional disclosures, are a genuine problem in terms of ML/TF, cf. section 6.5. This is also supported by the EBA's Guidelines for the AMLD, cf. section 6.1.

It will always be possible to intentionally disclose information for the purpose of identity fraud. In the example above of an adequate process for identification and verification of customer identities for distance customers today, for example, an individual can disclose their personal information, log-in information, passport and NemID keycard. One of the problems with NemID is precisely that it is easy to disclose the keycard, cf. section 6.3. The possibility that the issue of intentional disclosure also applies to the MitID solution thus cannot be ruled out.

According to eIDAS, the risk of unintentional disclosure will also remain for a MitID with an assurance level of 'substantial', cf. section 6.4. All other things being equal, however, means of authentication at this level will be more secure than the keycard in terms of the risk of unintended disclosure. This is partly because it is easier to copy a keycard than it will be to copy the new means of authentication, such as an app or a key viewer. In principle, a criminal would have to either hack a phone or know the PIN for the phone and steal it to gain access to the MitID app. A keycard, on the other hand, can be photographed or stolen. The keys for a stolen keycard will also be available and can be used without the person to whom it has been issued knowing about it. In the MitID app, the user will receive an approval notification each time the MitID is used.

In the guidelines for the MLA, the DFSA emphasises that, depending on the risk classification, it may be necessary to implement so-called mitigating measures when NemID is used. Examples of how this can be done are:

- The customer receives a unique code on their mobile phone number, which the customer can subsequently provide as additional verification.

- The customer's geolocation is verified based on the IP address used, which reveals whether the customer is acting from a location that differs from their usual place of activity – for example, another country.

The examples of mitigating measures in the guidelines can be considered as measures that are intended to complicate the process for criminals. In any case, it will also be more difficult to detect a disclosure when a customer relationship is being established than it is once the customer relationship has been established. This is because, at this time, the assessment cannot be based on actual behaviour observed in connection with transaction monitoring. In the ongoing customer relationship, there will be multiple points of contact, and it will therefore be easier to identify suspicious customer behaviour.

In the MitID solution, the MitID broker has the option of setting up additional security layers based on the risk data with which an authentication response is supplemented, cf. section 6.4. This also involves the ability to identify the user's geolocation based, among other things, on the IP address of the platform on which the means of authentication is installed. Other examples are observations of when the MitID was registered, the time of the most recent authentication and the number of previous failed identifications. Some risk data must be aggregated in order to be passed on to the broker, while other information can be passed on as raw data. In addition, the extent to which brokers can pass on this data to service providers is currently unknown.

The DFSA is of the opinion that the MitID solution also shows greater potential here than the NemID solution in terms of supporting credible verification of the customer's identity. This is due to the potential for building in additional security layers to support the risk classification of the customer relationship in order to take into account possible disclosures in both the establishment and ongoing maintenance of the customer relationship. Properly implemented, such security layers should also, as a minimum, be able to mitigate the risk of disclosure to the same extent as the examples of mitigating measures in the guidelines for the MLA.

These security layers are not built into the MitID solution. It is therefore up to the obliged entities to ensure that the broker they use has established them. In addition, the obliged entities must be able to access the relevant risk data or analyses, so that they can be used in the KYC procedures. The DFSA has informed the Danish Agency for Digitisation of this need in its consultation response to the MitID Act.

7. PEP-solution under the auspices of a public authority

The DFSA recommends that a decision be made as to whether further work is to be done on the two proposed solution models, and if so, decide the authority in which the PEP-solution is to be anchored. Both models require amendments to the MLA and the PEP Executive Order, which should be initiated if work continues on this initiative.

Companies and persons subject to the MLA are obliged to examine whether a customer is a politically exposed person (PEP), or whether the customer is a relative or close associate of a PEP (RCA). The Danish Ministry of Industry, Business and Financial Affairs is currently supporting this process by enabling the DFSA to keep a publicly available list of PEPs, on which the obliged entities examinations can be based.

The process of screening PEPs and their relationships is a resource-heavy manual process for the obliged entities. This is mainly because they are not able to uncover all relationships between a customer and a PEP in CPR and they cannot look people up based on CPR numbers in CVR. This limits the possibilities for automating the process and results in, among other things, that they are instead forced to obtain certain personal data about their customers in order to uncover all possible relationships with PEPs. At the same time, the quality of the screening is contingent on the credibility of the information that the customer shares, or on lookups in other registers on the basis of the customer's name and address.

The DFSA has therefore examined the conditions under which it is possible to support the sector in more efficient screening of PEPs and particularly their RCAs (the PEP-solution). This analysis looks at both a register-based model and a model based on real-time lookups. Both models involve enriching the DFSA's PEP list with CPR numbers of PEPs. Regardless of which model is chosen, the solution involves processing personal data. One condition, therefore, is for the data that is shared to be restricted to information about a given customer that is necessary and legally obtainable.

The DFSA is of the opinion that the creation of a PEP-solution will improve the quality and reduce the cost of PEP-screening, minimise the amount of personal information that companies are required to collect about their customers, and limit access to information about PEPs and their relationships to those companies and persons that are subject to the MLA. This opinion is supported by the recommendations from Finance Denmark's Money Laundering Task Force, which include a specific proposal for a sector-wide and authority-run PEP register. Insurance & Pension Denmark (IPD) has also emphasised the value of such an initiative to the DFSA.

The DFSA assesses that the General Data Protection Regulation and the Data Protection Act do not preclude the establishment of the proposed solutions, but that an API-based solution (Application Programming Interface)[43] is preferable from the perspective of data protection. However, consideration should be given to whether the need for effective and secure PEP-screening outweighs the competition law considerations for private operators providing similar services.

43 An API is a software interface that enables two pieces of software to communicate and exchange information based on certain clearly defined rules. An API has often been compared to an electrical plug, from which precisely defined data can be retrieved. Through an API, parts of a system or infrastructure can be made available to others, allowing them to integrate or develop their own systems on top.

In theory, there could be a concern associated with a register containing information on PEPs and RCAs. The same concern was expressed in connection with the establishment of the existing (more limited) PEP-list under the auspices of the DFSA. However, it is important to bear in mind that the companies covered must collect this information and map the relationships of PEPs in any case. It is the DFSA's opinion that a register or an API solution under the auspices of a public authority – with appropriate restrictions on access to information – will, in fact, ensure a higher level of data protection rather than the reverse.

It will not be possible to implement these proposed solutions using only the DFSA's current competencies and resources. External assistance will therefore be required in the form of consultancy services or cooperation with other authorities if the solution is to be developed under the auspices of the DFSA. In addition to development and establishment costs there will also be ongoing costs for operating the chosen solution and for managing companies' access to it.

7.1. The current rules

As part of their KYC procedures, companies must examine whether a customer is a PEP or a RCA of a PEP. This follows from Section 18 of the MLA.

The Minister for Industry, Business and Financial Affairs is obliged to keep a public list of domestic PEPs, cf. section 18, subsection 7 of the MLA. The list must include the PEP's name, position, date of birth and date of addition or deletion. The PEP-list is maintained on the basis of reports from those with an obligation to report such matters, including political parties and the Executive Office of the Danish Parliament, and is available on the DFSA's website. The list includes both current PEPs and people who have been registered as PEPs in the past 12 months, cf. section 2, subsection 3 of the PEP Executive Order.

It does not contain information about RCAs[44]. This means that, as part of their KYC procedures, companies must themselves uncover potential relationships with a PEP.

Section 2, no. 6 of the MLA states that close family members of PEPs include:

- *A politically exposed person's spouse, civil partner, cohabitant or parents as well as children and their spouses, civil partners or cohabitants.*

Section 2, no. 7 of MLA states that close associates of PEPs include:

a) *A natural person who is the beneficial owner of a company or other legal person along with one or more politically exposed persons.*
b) *A natural person who, in other ways than those mentioned in letter a, has a close business relationship with one or more politically exposed persons.*
c) *A natural person who is the sole beneficial owner of an undertaking or other legal entity which is known to have been created for the benefit of a politically exposed person.*

[44] Nor does the list include foreign PEPs.

7.2. Companies' access to a PEP-solution

An adequate access mechanism must be established to enable companies and persons subject to the MLA to access the PEP-solution. The DFSA finds it necessary that two access solutions are established for the solution to be used effectively by all obliged entities. Both solutions rely on that filtered data can be received from CPR and CVR about the customer's possible relationships with PEPs based on the customer's CPR number.

First and foremost, an API should be established under the auspices of a public authority, enabling companies to integrate their systems directly with the PEP-solution. This will be highly advantageous for some companies in terms of avoiding manual procedures. However, it will not be optimal for all obliged entities as it will require their technical infrastructure to be able to handle this. An access mechanism should therefore also be established through an online portal, from which entities can log in to a website that allows lookups on customers' CPR numbers.

As the solution will process personal data, it is crucial that only the obliged entities have access to it, cf. section 7.5, and that the information that can be accessed is restricted to data that is relevant for the PEP-screening of the specific customer. This means that unique access to the PEP-solution must also be established and assigned. The access may consist of a password, encrypted key file or a similar mechanism, which can be granted either as the obliged entities obtain authorisation or are registered as obliged under the anti-money laundering rules.

In addition, the solution can and should be created in such a way that the obliged entities do not have direct access to the underlying data, but are only able to look up the individual customer's CPR number and receive the necessary information about:

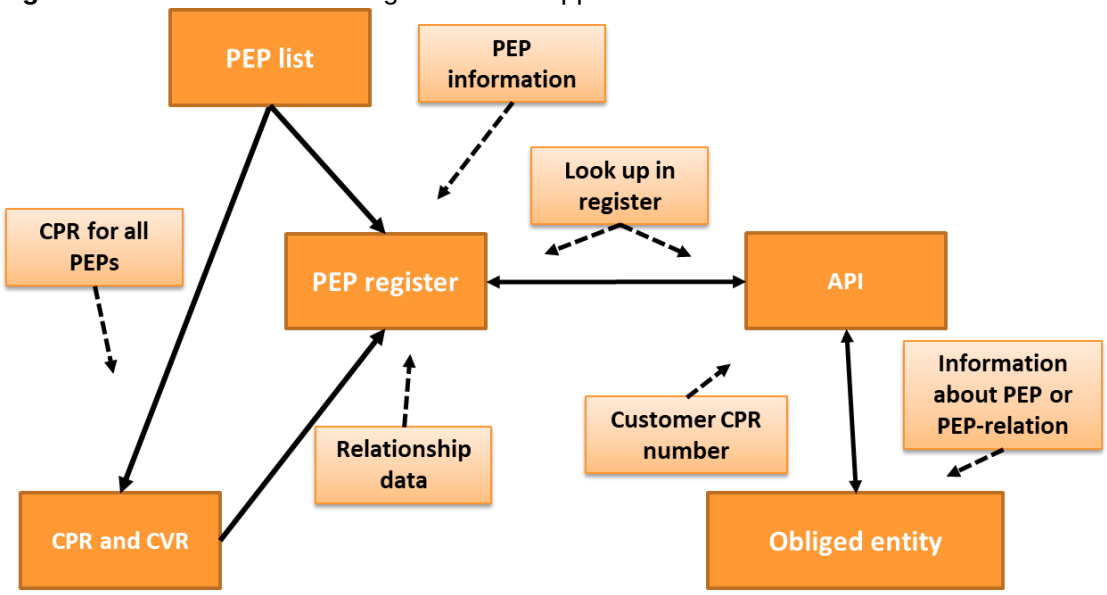
1) whether the customer is a PEP, and
2) whether the customer has a relation to a PEP, which PEP if so, and what their relation is.

7.3. Register-based PEP-solution

A register-based solution means that a register is established on behalf of the Ministry of Industry, Business and Financial Affairs, in which the existing PEP-list is enriched with RCAs from CPR and CVR.

Figure 7.1 illustrates the architecture for such a solution. The PEP list is enriched by retrieving all relevant relationships with all PEPs from CPR and CVR and subsequently recorded in a register under the auspices of a public authority. An API is built on top of the register, whereby entities who are required to PEP-screen a customer, based on the customer's CPR number, will be able to access the relevant information either by integrating the API with their own systems or through direct lookups in the online portal.

Figure 7.1 – Architecture for register-based approach



Source: The DFSA.

Enrichment with data from CPR

Through CPR, public authorities can gain access to the following data that is relevant to the sector's PEP-screening for RCAs, cf. section 2, no. 6 of the MLA:

- Children (including CPR number)
- Spouse, cohabiting partner or civil partner (including CPR number)
- Parents (including CPR number)

Authorities are thus also able to identify a PEP's spouse, cohabiting partner or civil partner, parents and children and their spouses, cohabiting partners or civil partners.

Public authorities can access this data either through the Data Distribution Platform (Datafordeleren) or directly from CPR through CPR Services. The Data Distribution Platform is run by the Danish Agency for Data Supply and Efficiency and is tasked with giving private companies and public authorities access to basic public data through APIs. CPR Services consists of a range of services provided by the CPR office, which offer lookup options in XML format.

The DFSA assesses that both the Data Distribution Platform and CPR Services can be used to obtain data from CPR for use in identifying relatives of PEPs. However, the Data Distribution Platform is based on newer technology and contains data from both CPR and CVR. It will therefore form a more suitable basis for a PEP-solution in the long term. In addition, unlike CPR Services, the Data Distribution Platform can be used without incurring a payment each time a lookup is performed.

Enrichment with data from CVR

The Data Distribution Platform will at some point also be able to support searches for CPR numbers in CVR. It is not yet known when this functionality will be implemented. The Danish Agency for Data Supply and Efficiency has stated that it will happen in the near future.

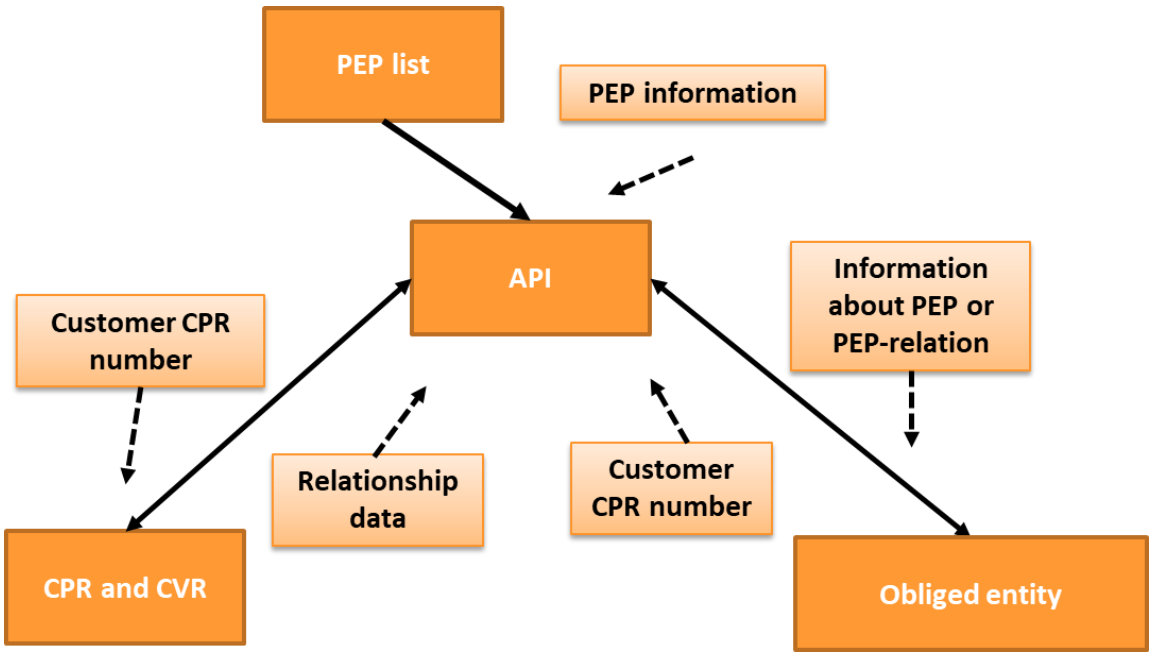
CVR also offers 'system-to-system access', which allows public authorities to search for CPR numbers and thereby obtain information about a given person's involvement in different companies. With system-to-system access, public authorities can thus, on the basis of a CPR number, identify a PEP's close associates as covered by section 2, no. 7, letter a of the MLA.

7.4. API solution with real-time lookup

The primary benefit of establishing an API that performs real-time lookups is that it will not be necessary to maintain a separate register in which PEP-relations are stored, with the data protection challenges that this entails. At the same time, this solution will be able to fulfil the purpose more efficiently, as information is extracted directly from the source and so will always be up-to-date. This means that there will be no need to continuously update an independent register. Only the current PEP-list will need to be continuously updated and will not always be fully up-to-date. This is also the case today.

On the other hand, the availability of this solution will depend on the overall technical infrastructure. Technical errors in CVR and CPR will thus have greater consequences, and the need for ongoing and rapid maintenance will therefore also be greater. For example, it will be necessary to customise the API if the data formats in the CVR or CPR are changed.

Figure 7.2 – Architecture for dynamic API approach



Source: The DFSA.

Figure 7.2 illustrates the architecture behind such a solution. The obliged entities that are to perform PEP-screening for a customer will also be able to access the relevant information here through either an integration of their own systems with the API or via direct look-up in the web portal. Instead of performing lookups in a register, this solution will look up information in CPR and CVR directly, compare with the PEP-list, and thus identify whether the customer is a PEP or has a relationship with a PEP in real time, and communicate the result.

Both the Data Distribution Platform and the system-to-system access to CVR allow real-time lookups. The enrichment can therefore be implemented in the same way as with the register-based solution, but this time based on the customer's CPR number. The main difference is that this functionality must be found in the API and must not be implemented as a parallel update of the register separately from the API. The DFSA has discussed the complexity of such a solution with IPD, who are experienced in the establishment of this type of technical solutions. IPD's assessment is that implementing such a solution is neither particularly complicated nor costly.

7.5. Legal considerations

The rules in the MLA on publication of PEPs, cf. section 18, subsection 6, do not cover their relationships. This means that the PEP-solution, and the particularly the registry-based solution with an enriched PEP-list, is associated with a number of legal considerations. One possibility is changes in the DFSA's authority to maintain and operate a PEP-list. At the same time, it must be ensured that the further processing of personal data, for example when keeping a register, is necessary relative to the purpose of effective measures to ML/TF.

Both models will eliminate the need to maintain a public list of PEPs. The DFSA is therefore of the opinion that the PEP-solution, regardless of the model that is chosen, facilitates improved protection of the personal data of PEPs compared with the current solution.

Necessary amendments to the MLA and the PEP Executive Order

PEPs are currently registered with their name, position, date of birth and date of addition or deletion, cf. section 18, subsection 7 of the MLA. Both models require the PEP-list to be expanded to include CPR numbers. This is because lookups by name in the Data Distribution Platform (or directly in CPR and CVR) will not be able to provide definitive answers about relevant relationships unless a unique identification marker is used. For example, multiple people may well have the same name and date of birth.

This will require an amendment both to section 18, subsection 7 of the MLA and to the PEP Executive Order, so that CPR numbers are included in the information that the authorities and organisations, etc. must report to the DFSA regarding PEPs pursuant to the PEP Executive Order. However, neither model will give users access to CPR numbers of PEPs. They will be used solely to map potential coincidences or relationships with the customers for whom users are performing PEP-screenings. In addition, a few minor changes should also be made to the section 2, subsections 1–3 of the PEP Executive Order so that it is adapted to the selected model.

The General Data Protection Regulation and data minimisation

A technical solution that provides access to PEP names and relevant relationships to customers through CPR, CVR and the DFSA's PEP-list will involve the processing of general personal data, cf. section 9.1.

The purpose of the processing of personal data is to support the obliged entities in conducting PEP screenings. With the proposed PEP solution, the processing will take place through a mechanism that can help companies identify PEPs and their RCAs.

The processing of personal data on the basis of the rules in the AMLD is considered to be in the public interest and will therefore constitute a lawful legal basis for processing, cf. section 2. This means that it will be possible to authorise obliged entities to gain access to specific registers suitable for the purpose in connection with their KYC procedures. When assessing which of the two proposed models is most proportional (suitable, necessary and proportionate), it is therefore crucial to distinguish between how each model processes personal data.

The general personal data of PEPs is already processed in connection with the DFSA's operation and publication of a PEP-list. However, the proposed solutions will also mean that PEPs' relationships with a particular customer must also be processed in the future. If a register-based solution is chosen, all relevant relationships will in the future need to be registered in a separate PEP register. This means that the currently registered group of persons will be larger, cf. section 7.1.

According to article 5 of the General Data Protection Regulation, it is essential that the chosen solution limits the processing of information and only processes the information that is necessary (data minimisation).

In connection with this, the proposed API solution with real-time lookups has the advantage in that it will not require the registered group of persons to be expanded. The API will be able to identify the relevant group of persons for each individual PEP through real-time lookups in the relevant registers and will therefore not be dependent on an extension of the registered group of persons.

In addition, both solutions will be able to take the following protective measures, among others:

- The chosen solution only indicates whether the CPR number has a relationship with a PEP, and if so, which PEP the customer has a relationship with, and what that relationship consists of. In regard to this, it is important that no distinction is made between cohabiting partner, spouse or civil partner, as such a distinction entails the processing of sensitive personal data, which is not necessary for this purpose.

- The PEP-list will no longer be publicly available, but will be accessible through the data sharing mechanism being accessible to the obliged entities.

- All searches in the system are logged. The scope and legal consequences of such logging should be assessed in this context.

Both solutions meet the requirements for suitability, but the API-based solution meets the requirement of necessity better, as it does not require an expansion of the registered group of persons.

The DFSA estimates that the PEP-solution will be suitable in terms of reducing the cost of PEP-screening across the sector, regardless of the model that is chosen. More efficient use will be made of resources, which may help the obliged entities to improve compliance with the MLA. In addition, the quality of PEP-screening is also likely to improve.

Competition law considerations

The CPR Act lays out the framework for private companies' access to CPR. Although pension funds, insurance companies and banks have extended access to information in CPR, which, in addition to providing access to the information listed in section 38, subsection 2 of the CPR Act, also provides access to marital status and date of the marital status, this access does not give companies adequate insight into customers' RCAs according to section 2, no. 6 of the MLA.

In regard to data from CVR for screening of close associates pursuant to section 2, no. 7, letter a of the MLA, all Danish companies can access basic data on Danish companies, including information on ownership, through the DBA's online service (virk.dk and cvr.dk) or through the open API (cvrapi.dk), which is freely available. However, public access to CVR does not allow lookups by CPR number.

The DFSA therefore considers that public authorities, due to their broader access to CPR and CVR, can establish a more effective PEP-solution than private companies, in regard of the group of persons in section 2, no. 6 and no. 7, letter a of the MLA.

However, it cannot be ruled out that such a solution would remove all or part of the business basis of private companies that are able to offer or already offer similar solutions. In particular, this applies to the group of persons in section 2, no. 7, letter a of the MLA, since much of the necessary information can be accessed through CVR. This means that if one of the proposed solutions is established, a situation may arise in which it competes with solutions from private actors.

It will not be possible to use the proposed solutions to screen foreign PEPs and the group of persons in section 2, no. 7, letters b and c of the Anti-Money Laundering Act. This is because this screening cannot be performed solely on the basis of information in public registers. In the future, therefore, there will still be room for private PEP-solutions to complement the public solution. In connection with this, consideration should also be given to whether and to what extent private solutions should have access to the PEP-solution. These considerations should include the rules on assistance from third parties, cf. part 4 of the MLA.

8. Generalised scenarios in transaction monitoring

The DFSA recommends that a decision be made as to whether the cooperation between authorities and banks should be expanded with the aim of developing typologies for relevant scenarios (generalised scenarios) that should be identified in transaction monitoring. It makes sense to position this work within the framework of a Joint Anti-Money Laundering and Terrorist Financing Intelligence Taskforce (referred to by the Danish acronym, FEHT) if or when this is established.

Lack of insight into criminal behaviour limits the ability of banks to effectively detect questionable matters (suspicious behaviour). Firstly, criminals are skilled at concealing their activity, partly by constantly evolving their methods. For example, VAT carousels were once particularly associated with the buying and selling of hardware. Today, other products are also used in this type of fraud – for example, frozen chicken. Secondly, the core competencies of banks do not include understanding criminal behaviour. On the other hand, these are core competencies of a number of authorities, in particular the Danish FIU and other police authorities. Given that banks bear a great deal of responsibility in regard to identifying suspicious behaviour, in order for efforts to be effective it is therefore crucial that, where possible, the knowledge of the authorities is also shared with banks in order to support them in their work.

A number of existing initiatives are currently tasked with undertaking this matter. The establishment of HVF+, chaired by the DFSA, was from 2018 part of the government's strategy to combat ML/TF. The purpose of this forum is to ensure that the authorities and the sector exchange relevant information on developments in the field, and especially to support cooperation in the field.

The Danish FIU also shares both quarterly and thematic reports with banks, dealing with changes in reports received and particularly relevant focus areas. The quarterly reports include information on trends in the reports received, as well as more general examples of areas on which those with a reporting obligation should focus particularly or more extensively. The thematic reports contain more in-depth analyses of specific trends and risks of which those with a reporting obligation should be aware. The Danish FIU has also begun to concretise information about criminal behaviour and provide specific examples of questionable matters that may usefully be included in transaction monitoring in ongoing briefings to those with a reporting obligation.

The recommendations from Finance Denmark's Money Laundering Task Force highlighted a need to be able to go into more depth with development trends. The reason for this was to make greater use of the information held by the authorities, thereby making the work of banks more efficient. The Task Force therefore proposed the establishment of a so-called Banking Forum, which, for example, could work in more depth with the reports provided by banks to the Danish FIU, thereby ensuring a certain amount of standardisation and qualification of the reports. Among other things, it would also create a better basis for the Danish FIU’s analysis work. At the same time, such a forum would be able to support better training for banks.

Taking inspiration from the UK and the ongoing collaboration between the authorities and the financial sector in a *Joint Money Laundering Intelligence Taskforce (JMLIT)*, the Task Force also suggested that a *Joint Anti-Money Laundering and Terrorist Financing Intelligence*

Taskforce (FEHT) be set up in Denmark[45]. The purpose of establishing FEHT is to enable sensitive personal information on specific cases to be shared in order to ensure effective prevention and clarification of matters relating to serious crime, ML/TF in particular.

The DFSA is of the opinion that one way of supporting the work of banks is to support increased cooperation between authorities and banks focused on continuing to concretise scenarios that banks should be aware of in their transaction monitoring. The potential is supported, among other things, by the DFSA's evaluation of compliance with the rules for transaction monitoring, cf. section 10.4. At the same time, results within the framework of Danmarks Nationalbank's Proof of Concept (POC)[46], which makes use, among other things, of three specific scenarios set up in collaboration with the Danish FIU, indicate that this type of collaboration can help to streamline transaction monitoring, because:

1. Suspicious behaviour can be identified much earlier than it is today. More specifically, we can see that applying these scenarios means that an actual risk flag could have been raised earlier in 84 per cent of cases.

2. Suspicious behaviour that is not currently detected is detected to a greater extent using the set scenarios. Specifically, 1,482 cases of 'new' suspicious transactions were flagged.

On this basis, the DFSA assesses that work could usefully start with clarifying the conditions under which this type of cooperation can be supported. A forum such as FEHT is regarded as being able to handle this task best, as the establishment of a confidential space would help to build the trust that is necessary in order to discuss and share relevant observations across banks and authorities. In principle, it is not necessary to share personally identifiable information in order to develop generalised scenarios as to when a risk flag should be raised for a given customer or transaction. The exercise requires mutual trust, however, as everyone will have to offer specific experiences from their day-to-day work.

Announcements from JMLIT also imply that extended cooperation between authorities and the obliged entities can help to improve the efficiency of the work[47]:

> *"Partnerships have contributed to: improvements in the quantity and quality of reports of suspicion related to particular economic crime threats; and to the timeliness and relevance of such reporting to active investigations or live incidents."*

However, it should be emphasised that generalised scenarios should never be considered as best practice for transaction monitoring, but rather as a contribution to how banks can best organise their transaction monitoring, cf. section 10.2. At the same time, there is a risk that criminals will become aware of the scenarios used in transaction monitoring and therefore

[45] FIDA proposes that such a taskforce should be placed under the auspices of the public sector and should include participants from both the sector and the authorities. Participants from the authorities could be the State Prosecutor for Serious Economic and International Crime, the Danish FIU, the Police, the Police Intelligence Service, the Defence Intelligence Service, the Danish Tax Agency, etc.
[46] During the first half of 2020, Danmarks Nationalbank (the Danish Central Bank) developed a Proof of Concept (POC) to investigate whether information from banks' transaction data cross-checked with various government data could support a more effective effort against financial crime.
[47] FFIS (Nick J. Maxwell) – Expanding the Capability of Financial Information-Sharing Partnerships, March 2019

find new ways in which to avoid being selected for verification. The advantages of banks becoming more aware of specific behaviour of criminals, however, will limit the options of criminals, all other things being equal.

8.1. Legal considerations

The legal considerations regarding increased knowledge sharing between authorities and banks depend in particular on the model that is chosen. The above proposals only relate to improving the common understanding of suspicious (criminal) behaviour through better sharing of knowledge, and are not contingent on the exchange of personally identifiable information.

Collaboration on the development of general scenarios

Information on risk indicators, risk scenarios and more general information on the risk factors that should be monitored by banks in order to counter ML/TF can be exchanged both between banks and with the authorities without legal challenges. This means that there is no legal obstacle to setting up a forum in which both the private sector and the competent authorities are represented and can exchange information in summary or abstract form. In this context, it does not matter whether it is created as a subordinate working group in an existing forum or associated with a newly created unit. The effectiveness of such a forum is likely to increase as trust and understanding grow between the parties. The DFSA is therefore of the opinion that it would be sensible and appropriate to set up the forum in connection with, for example, the proposed FEHT.

The exchange of information should not be of such a nature that the investigative methods or similar used by authorities could be disclosed. In this connection, the individual authority must undertake a specific assessment and weigh up considerations before sharing information.

Creation of FEHT or similar

The creation of a unit or forum that can process information about specific individuals, including, for example, information about reports, suspected criminality or similar, will in particular entail requirements in terms of a legal basis for processing, confidentiality and legal effect for customers.

Point 2 of the political agreement of 19 September 2018 on further initiatives to strengthen efforts to counter ML/TF, which deals with cooperation with private actors, includes an initiative for setting up such a unit[48]:

> *"The legal enforcement authorities must assess the need to set up a permanent working group, where specific investigation cases, etc. may be discussed with selected private actors, and whether this can be contained within the current legislative framework."*

The initiative is being addressed by the Danish Ministry of Justice, which will assess the legal aspects. The actual creation of such a forum for the purpose of sharing personally identifiable information is therefore not described further here.

[48] https://www.regeringen.dk/aktuelt/publikationer-og-aftaletekster/hvidvaskaftale/

9. Increased access to data held by authorities

The DFSA recommends that a decision be made as to whether to start focusing on the possibility of banks gaining access to composite company data or assessments under the auspices of the Danish Business Authority. The decision should be complemented by considerations as to whether such work should also affect opportunities for wider access to data from other authorities.

A general challenge today is that a lack of availability of verified customer information can limit and complicate the banks' ability to obtain adequate customer knowledge. This is partly due to the fact that customer knowledge is fragmented across the sector, cf. section 10. It may also be due to the fact that information in public registers is not available to the required extent. Whatever the reason, limited access to verified customer information may have implications for the effectiveness of banks' efforts to counter ML/TF.

The recommendations of Finance Denmark's Money Laundering Task Force also support this assessment. Among other things, the Task Force mentions a range of authorities that hold knowledge and data that could be useful for banks in the fight against ML/TF.

The DFSA's analysis is based on the value of increased access to aggregated data under the auspices of the DBA. Among other things, this is because a positive effect of including this data in transaction monitoring has already to some extent been documented for banks under the auspices of Danmarks Nationalbank's POC[49].

The DBA currently publishes certain company data in CVR. The DBA has established a significantly more advanced internal register of companies, including relationships between companies. This register is known as the graph database. Briefly, the graph database creates an extremely nuanced overview of all companies in Denmark on the basis of all data held by the DBA. The graph database is based on register data[50], including data on relationships such as natural persons associated with companies and the interrelationships between these persons as well as various calculations regarding register data (metadata). More nuanced metadata is also included, for example assessments carried out using machine learning models on the basis of register data and other reported data (annual reports, etc.). Accessing the graph database is an obvious way for banks to gain better knowledge of their corporate customers.

The results of Danmarks Nationalbank's POC indicate that banks can improve their transaction monitoring processes if their data is enriched with information such as data from the graph database. The results are based on a machine learning model (algorithm) and the basis of comparison is the existing transaction monitoring process. Training the algorithm on the enriched dataset[51] raised a substantially higher number of risk flags compared with the existing process[52]. The algorithm was also able to filter out a significant number of cases that were erroneously referred for manual examination during the existing process (so-called

[49] Danmarks Nationalbank's POC is briefly introduced in a footnote in section 8.
[50] Also involves records from other authorities, due to the DBA's relatively broad legal basis for collecting data, cf. the Act on the DBA's processing of data of 8 May 2018.
[51] Primarily enriched with data in the DBA's graph database.
[52] Note that this does not necessarily presuppose that transaction monitoring will improve, cf. section 3. However, this may well be the case.

false positives*)*. The enrichment of data with the graph database proved to be crucial for both results, and was the direct cause of 35 per cent of the false-positives that were filtered out.

Danmarks Nationalbank's results presuppose the use of machine learning techniques to optimise the transaction monitoring processes. This creates uncertainty as to whether a similar effect would be seen if banks were to gain access to the graph database under existing processes, cf. section 10.1. In terms of infrastructure, there are likely to be certain challenges associated with giving all banks access to the graph database. It is a very large data set that is constantly growing, combined with an IT infrastructure that is not necessarily geared for sharing such large amounts of data in real time.

A collaboration with the DBA might uncover the possibility of developing machine learning models that can carry out concrete assessments of the risk (probability) of a particular company being used for ML/TF. The results of these models could be shared with the banks, for example in the form of an overall risk score supplemented by a description of the factors underpinning the risk score. All other things being equal, this will place less of a burden on the existing IT infrastructure than sharing the full graph database. At the same time, the DBA has both the competencies and the necessary experience of using machine learning. For example, the DFSA has been presented with a model based on the same technique, which indicates the probability of a particular company committing tax and VAT fraud. The Danish Customs and Tax administration (SKAT) currently uses the model, which has helped them to more accurately select the right companies for manual examination.

The DFSA estimates that banks should be able to improve their KYC procedures if their data is enriched with data from or assessments made on the basis of the graph database. One next step could therefore be for the DFSA to work with the DBA in assessing the options for either direct access to the graph database or the preparation of the aforementioned machine learning models, and the extent to which data may be shared and is desirable to be shared. Such work could also clarify whether it is worth moving forward with such an initiative, and if so, identify which other actors that should be involved.

Data from other authorities can also be useful

Wider access to data from other authorities could also be useful. This applies, for example, to data from the Danish Tax Agency, Udbetaling Danmark[53], extended access to CPR, access to passport and driving licence registers and the Danish Immigration Service's registers[54]. These data sources can be used to varying degrees. Furthermore, whether a company can get access also depends on the type of company asking[55]. For example, Finans og Leasing (the stakeholder organisation for Danish financing companies) has expressed to the DFSA a wish to be able to verify the country of origin and residential basis in Denmark for foreign loan applicants via access to the Danish Immigration Service's registers. Another desire is to be able to compare passports or driving licences with the Danish National Police registers to see if they have been reported stolen or have expired.

[53] The public authority in Denmark that holds the responsibility for payment of most social security benefits etc.
[54] Expressed, among other things, through the recommendations of Finance Denmark's Money Laundering Task Force and dialogue with Finans og Leasing.
[55] For example, Finans og Leasing has stated that leasing companies do not have the same access to E-tax data under the auspices of the Danish Tax Agency as car loan providers and banks generally have via authorisation from the customer.

9.1. Legal considerations

The starting point for the DBA's graph database is data from various public registers, which is subsequently aggregated to allow for calculating factors such as risk scores (assessments) to prioritise supervision, and so on. The database is continuously enriched with the results of the calculated assessments. The aggregated data generally concerns legal persons and, to a lesser extent, natural persons. However, the data does contain certain information on natural persons, such as directors, as well as sole proprietorships, which are covered by the data protection rules.

Exchanging aggregated objective data from the DBA's graph database

The exchange of aggregated data in the graph database between the DBA and the banks for use in the banks' KYC procedures will not be subject to the same legal challenges as the exchange of the assessments subsequently made by the system.

Where this is information that companies are required by law to report to the DBA, the DFSA is of the opinion that banks will be able to access this if the companies are informed that the DBA will be able to pass the information to the banks in connection with the implementation of KYC procedures.

However, this will require banks to have a legal basis for processing data under the GDPR. Under Part 3 of the MLA, banks are obliged to know their customers, including collecting and storing information on which an assessment of the customer's risk profile, etc. can be based. Banks thus already have a legal basis for obtaining and processing information about their customers.

In continuation of this, whether the DBA's purpose in collecting the information in question can also encompass passing the information to banks, for use in their preventive efforts to counter ML/TF, must also be assessed.

The legal basis for the DBA's collection and processing of data is not reviewed in further detail in this analysis. However, this is a matter of objective data that can support the socially important role that the MLA imposes on banks. In addition, customers will be aware of what information the DBA can pass on, as is the case with data concerning factual matters.

In this context, the DFSA assesses that it will be possible, potentially with an amendment to the DBA's Act on the Processing of Data, to create a legal basis for the disclosure of information for use in banks' ongoing compliance with the rules of the MLA.

Exchanging assessments performed by the DBA

At the same time, the DFSA is of the opinion that giving banks access to aggregated data in the form of assessments and analyses performed in the DBA's graph database is associated with legal challenges.

A model in which banks' KYC procedures are enriched with assessments from the DBA's database, for example on a company's anticipated risk of money laundering, is regarded as involving, in particular, considerations of what the remedies for such an assessment are. For example, whether customers can contest the assessment or take the matter to court.

If such an assessment is included in banks' KYC procedures, the individual customer should have an opportunity to be aware of the information. In particular, this opportunity will need to serve to ensure that the DBA's assessment is based on correct factual information, so that the Authority does not perform assessments on an incorrect or incomplete basis. Consideration should be given to whether and how customers can access information and elements in the assessment, for example the information that is included in the DBA's graph database and the calculation methods (algorithms, etc.). If customers cannot be made aware of the DBA's assessment, and thus do not have the opportunity to know the basis on which they are assessed by banks or the opportunity to correct an assessment or similar, this raises concerns in terms of legal rights.

The exchange of the described assessments also gives rise to considerations about how data is verified, who is responsible for the assessments and how they are used subsequently. There will also be questions as to whether customers have the right to have the assessments amended or deleted.

In connection with this, consideration should be given to whether customers will be able to appeal to another authority regarding the DBA's risk assessment, or whether the DBA could be brought before the courts, for example in connection with matters of liability for financial loss arising from banks' use of assessments from the graph database. A solution in which the DBA shares its assessments with the banks, for example in the form of indications of risk by means of colour-coding, further exploration of the desired set-up, the function of algorithms and the anticipated value that can be added will be required. The legal challenges stated above will also have to be addressed. At the present time, it is impossible to determine whether it will in fact be possible to share public sector assessments.

Access to register data concerning natural persons

As mentioned above, the sector has expressed a desire for access to a number of registers in order to potentially strengthen and streamline their customer knowledge. In this connection, reference has been made to registers which contain a lot of information about natural persons, including registers held by the Danish Tax Agency and the Danish National Police.

Access to registers containing information about natural persons will require the requirements of the GDPR to be taken into account. This is because use of the access represents processing of personal data.

Personal information is any kind of information that can be attributed to a specific person. This applies even if the information can only be used in combination with other information to identify an individual.

The GDPR divides personal data into three types:

- General information, such as name, address and financial circumstances.
- Sensitive information, such as race, religion, and political beliefs.
- Information on criminal offences, such as criminal activities and disqualification.

The division is linked to differing conditions and procedures for processing personal data depending on the sensitivity of the data.

This means that, when assessing which registers can be granted full or partial access, it will be necessary initially to categorise the data contained in the individual register. The need for consent and the requirements of legality, fairness and transparency will then need to be assessed. Collected data may also, in principle, only be used for the specific purpose for which it was collected (the purpose limitation).

This means that a legal basis is always required in order for the obliged entities or public authorities to process personal data, for example as part of KYC procedures.

The processing of personal data on the basis of the rules in the AMLD is considered to be in the public interest and therefore constitutes a lawful legal basis for processing under the GDPR, cf. section 2. This means that it will be possible to authorise obliged entities to gain access to specific registers suitable for the purpose in connection with their KYC procedures in order to counter ML/TF. In this context, the type of data in question will be the determining factor, and the public authorities will need to assess proportionality in this respect (suitability, necessity and proportionality).

As stated above, the data protection rules contain three categories of personal data. General information, to which the lowest protection requirements are attached, sensitive information, for which there are stricter requirements for processing, and finally information on criminal offences, which is covered by special rules.

This means that it is possible to provide access to residential information in CPR, as this is categorised as general information. Conversely, it will probably not be possible to provide access to the Central Criminal Register's information on criminal offences[56].

The public authorities will therefore need to assess proportionality in relation to the individual registers. Regardless of the registers to which the authorities provide access, they must ensure that there is a clear legal basis for exchanges between public authorities and the obliged entities. It is probably possible to exchange the information in certain registers under the existing rules in the MLA, while other registers will require new legal basis if data is to be shared.

56 The Central Criminal Register (Criminal Register) contains information about offences which, among other things. is used to prepare criminal records.

10. Sharing risk flags raised in transaction monitoring

The DFSA recommends that a decision be made as to whether to start working on enabling the sharing of risk flags between banks. As part of this, a decision should be reached as to whether work should be done to enable banks to share risk flags with each other, and thus for a change in the confidentiality provisions in the AMLD, or whether further work should focus on sharing exclusively through a public authority.

The potential for classifying risk fairly when a bank establishes a customer relationship may be limited by the fact that banks are generally not allowed to share customer information. For example, a customer with whom a bank has dissolved the customer relationship due to suspected ML/TF can currently establish a customer relationship with another bank without too much trouble. This bank will not be aware of the concerns that the previous bank may have and it is not possible for the banks to warn each other.

The DFSA is of the opinion that the option of sharing risk flags raised as part of transaction monitoring in the sector may help to address this issue. Essentially, this is because the responsibility for effective KYC procedures will remain with the individual bank, while the KYC procedures, in particular risk classification and subsequent monitoring of customer relationships, can take place on a more informed basis:

- The quality of the banks' KYC procedures is expected to improve at sectoral level if knowledge of suspicious customers is shared to a greater extent across the sector.

- Banks can more quickly obtain information about potentially suspicious customers in their portfolio.

- The potential for detecting criminal networks is improved if shared risk flags are enriched with the correct master data (basic data such as name, CVR number, information about the given transaction, etc.).

Finance Denmark's Money Laundering Task Force has also highlighted the challenges of banks not being able to exchange information on risky customer relationships.

Banks are currently only able to share customer information if the information relates to the same customer and the same transaction, cf. section 38, subsection 6 of the MLA. It is possible that this kind of data-sharing mechanism could be supported better, but the value of this is limited compared with more general sharing of risk flags. This is because such a mechanism would only support more effective sharing of suspicious transaction information by the same customer across their own accounts in different banks, and would not help to identify other higher risk customer relationships.

The DFSA has therefore analysed the value and complexity of sharing risk flags at two points in the transaction monitoring process. These are risk flags raised and prioritised automatically (prioritised risk flags raised early in a bank's transaction monitoring before the transaction is examined manually and the suspicion confirmed or denied), and risk flags that have been examined by a caseworker and where the suspicion has not been ruled out (examined risk flags). Three factors in particular are relevant to this analysis:

1. **Quality of transaction monitoring across banks:** One potential consequence of low quality is that the volume of false positives that are shared (transactions that are mistakenly flagged as suspicious) becomes excessive, with the result that the sharing of risk flags can create more noise than benefit.

2. ***De-risking* of customer portfolios:** Such sharing could have unfortunate consequences if, for example, banks choose to avoid or wind up customer relationships that have been flagged by other banks as suspicious (blacklisting).

3. **Ongoing checks on risk flags:** If the validity of shared risk flags is not checked on an ongoing basis, for example when a suspicion is refuted, there is a risk that shared data will interfere with the overall picture.

The DFSA assesses that examined risk flags will in principle be better fit for purpose than prioritised risk flags. This is due to the quality of banks' transaction monitoring, cf. section 10.4. However, the value in sharing examined risk flags is limited by the fact that the processes cannot be automated. The time that elapses between a questionable matter being observed and it being shared with others will therefore depend on the efficiency of the individual bank's internal processes. The sharing of prioritised risk flags can also contribute to the purpose and could also potentially be fully automated. However, this is contingent on the quality of the banks' automated transaction monitoring being improved. This can be done, among other things, by establishing generalised scenarios as to which risk flags may be shared and when. Transaction monitoring will thereby also to some extent be unified across the banks.

One point to be aware of in connection with the sharing of risk flags is to ensure that it does not lead to increased de-risking of customer portfolios. Shared risk flags should only be included as input in banks' KYC procedures and monitoring, and they must not be used as the sole basis for decisions about the specific customer relationship. This is due both to concerns as regards legal rights, cf. section 10.7, and to the risk that criminals will instead will try to operate on the black market, making them even harder to identify. At a minimum, the sharing of risk flags therefore involves reconciling the expectations of the authorities and banks regarding the challenges of de-risking. For example, it should be clarified that it is not an expectation from the authorities, including the DFSA, that banks should not have high-risk customers in their portfolio, but merely that the monitoring of the customer relationships is contingent on the risk.

Regardless of the type of risk flag that is to be shared, banks are currently obliged to keep secret any reports sent to the Danish FIU, or any examinations that have been or will be launched pursuant to section 25 of the MLA. This follows from section 38, subsection 1. This means that a solution in which banks generally have access to shared risk flags is not possible under the current set of rules.

On this basis, the DFSA assesses that a sector-driven solution with wider sharing of risk flags between banks will require an amendment to section 38 of the MLA. Since the MLA implements the EU's AMLD, any amendment to the former would first require changes to the latter.

Further work on this possibility therefore means, first and foremost, that efforts must be made at European level with a focus on adapting the confidentiality provisions contained in the AMLD.

A Europe-wide initiative aimed at remodelling the AMLD will be launched in 2021, and Denmark's contribution could include something of this kind. The exact form of the remodelling has not yet been clarified, but the DFSA expects that it will be possible to propose an amendment to the confidentiality provisions.

However, opposition to such a proposal may be expected from several sides, as a number of countries are of the opinion that the problem today is not the anti-money laundering rules, but rather their implementation, cf. section 11.

An alternative may be to consider whether a data-sharing mechanism for risk flags could be established under the auspices of a public authority. Banks would thereby have access to relevant data for the risk classification of their own customers. As the confidentiality provisions in the MLA apply only to those with a reporting obligation, the authorities are not bound by them. Conversely, the authorities will be subject to other sets of rules, giving rise to other legal considerations, partly because information about possible criminal offences could in principle be shared, cf. section 10.7.

Centralising the data-sharing mechanism, whether public or private, is likely to be necessary for technical reasons, cf. section 10.6. Among other things, it should be able to support a control environment that, as far as possible, ensures that risk flags are shared only in the event of genuine suspicion, and supports further analysis of shared risk flags.

Regardless of the choice of model, proportionality must be assessed in terms of general data protection rules in regard to the three elements: suitability, necessity and proportionality, cf. section 10.7.

10.1. Effective transaction monitoring in practice

In collaboration with external consultants, the DFSA has evaluated compliance with the rules for transaction monitoring across a number of major Danish banks. Among other things, the study has formed the basis of a generalised methodology for the individual elements of an efficient process. The analysis is based on this methodology.

Figure 10.1 illustrates the individual elements of a generalised transaction monitoring process. The first step is to gather relevant data for the banks' customers into a data set. At a minimum, this involves:

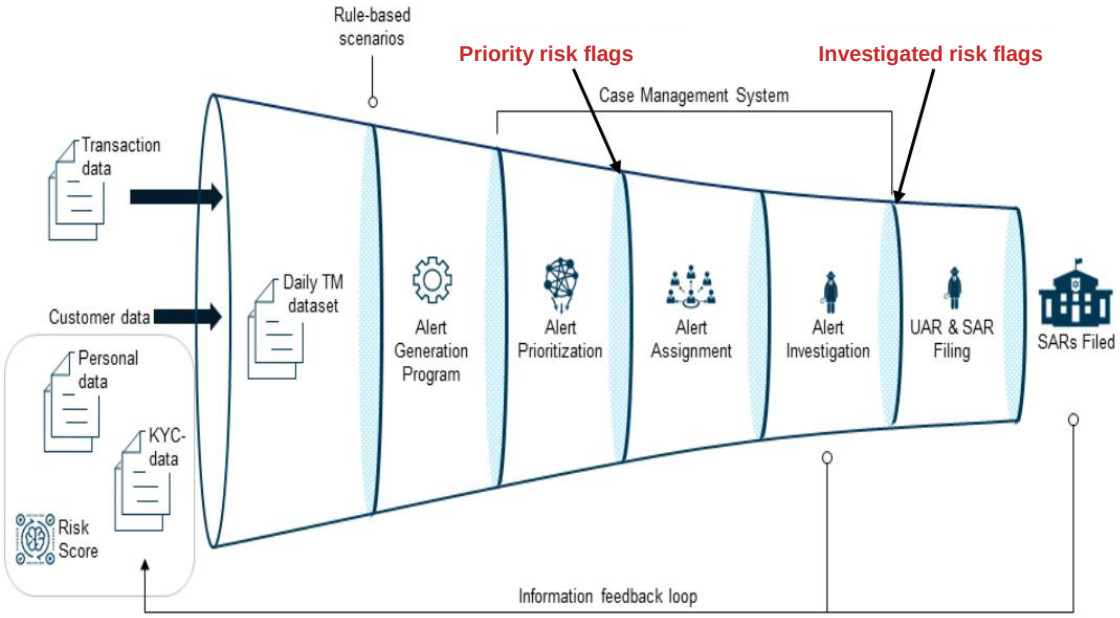
- **Customer information:** identity information, purpose, intended nature and risk classification, cf. section 11 of the MLA.

- **Transaction data:** the full overview of the customer's transactions and activities.

This consolidated data set forms the basis for the banks' transaction monitoring. The quality and scope of the data set is therefore crucial to the efficiency of the banks' efforts.

Effective transaction monitoring should have automated processes that flag questionable conditions (risk flags) and prioritise them in regard to the subsequent examination. Today, risk flags are raised primarily using so-called rule-based scenarios (the scenario method). The scenarios represent questionable matters that are identified on the basis of predefined conditions set out as indicators of potential ML/TF. It is therefore crucial for effective transaction monitoring that the established scenarios are effective, cf. section 10.2.

Figure 10.1 – Generalised architecture for transaction monitoring



Source: The DFSA's evaluation of compliance with rules for transaction monitoring.

The automated prioritisation of the alarms generated in regard to the subsequent examination must ensure that the most critical matters are examined first. This must be done by, for example, prioritising the analysis of specific customer relationships based on the number and, in particular, the nature of alarms raised and by filtering out known false positives[57]. For example, situations could arise in which an alarm is raised again, even though it has previously been raised, assessed and filtered out.

After prioritisation, a given risk flag is examined by a caseworker. This examination may lead to a report being sent to the Danish FIU. Effective case management means that cases are handled using a risk-based approach, and that systems have been established to ensure that all relevant observations about a given customer are included in the examination. This includes master data, KYC information and previously raised risk flags. At the same time, guidelines should be set as to which factors the caseworker must emphasise in a given examination, for example scenario-specific guidelines. Finally, it is important to document the

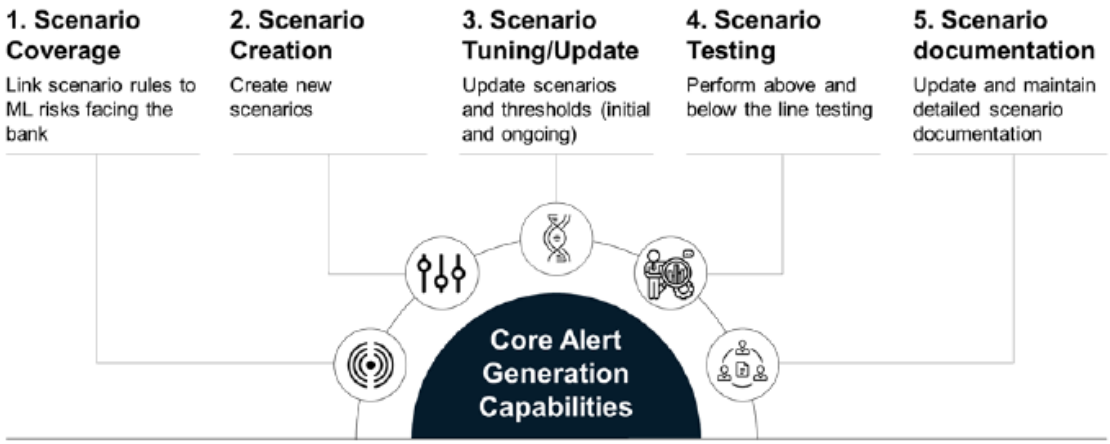
[57] False positives can also occur if a given scenario results in a number of risk flags being raised on a non-material basis. However, this will be difficult to filter out automatically, as the problem relates to the quality of the specific scenario.

results of the examination[58]. This is necessary both if an examination leads to a report to the Danish FIU, and to ensure adequate customer knowledge in cases where it does not lead to a report.

10.2. Effective scenarios

Effective scenarios are characterised by the fact that they cover the inherent risks of the banks' business model, are dynamic in relation to the customer's risk classification, and the purpose of the individual scenario is documented and satisfactory. Effective monitoring across banks is therefore not necessarily the same as everyone using the same scenarios and thresholds[59]. This means that it will not be possible to harmonise banks' transaction monitoring, although there will often be overlap between the risk categories that should be identified. Efficiency improvements should therefore also be shared across the sector. The differences between the banks are likely to be greater than the differences between other companies in other industries. In particular, banks are misused in many different ways, for example by transferring the funds through a wide network of accounts.

Figure 10.2 – Starting point for establishing effective scenarios



Source: The DFSA's evaluation of compliance with rules for transaction monitoring.

As illustrated in Figure 10.2, the preparation and use of the scenarios should at best be based on five criteria. Banks must ensure that the scenarios reflect the relevant risk factors relating to product and customer types, geographical conditions, etc. In addition, all scenarios used should be maintained on an ongoing basis and the thresholds used should be adjusted both in relation to the bank's risk profile and the individual customer's risk classification. This should be done on the basis of ongoing testing of the effectiveness of the scenario. This is partly due to an expectation that the behaviour of criminals will change as their methods are revealed.

The possibility of generalised scenarios

In its evaluation of compliance with the rules for transaction monitoring, the DFSA has noted that there is a certain amount of overlap between the risks identified by transaction monitoring

[58] An examination must be documented through a narrative that describes the caseworker's reasoning for a given assessment, and by including all observations and sources used.
[59] The threshold is the value that must be exceeded in order for a risk flag to be raised. It can be determined on the basis of both specific information obtained about the customer, such as expected transfer amounts, and a more general consideration of when a matter should be characterised as suspicious.

and certain points of similarity between the associated scenarios. The overlaps are greatest for banks that have outsourced transaction monitoring to the same data centres, but can also seen for other banks. The DFSA has categorised the scenarios used into 13 overall risk categories which may indicate that a customer's activities are questionable and should be examined. Examples are:

- **Cross-border activities:** Scenarios that focus on capturing unusual activities related to cross-border transactions. This may be, for example, in connection with cooperation with correspondent banks, where the customer knowledge relates to the correspondent bank or the respondent and not the customer who actually carries out the transactions.

- **Deviations from the customer's KYC profile:** Scenarios that identify activities that differ from the customer profile. For example, if the customer sends or receives a transfer amount that is significantly higher than the stated maximum when the customer relationship was established.

- **Cash activities:** Scenarios that focus on unusual cash activities. These could, for example, be large deposits or withdrawals.

Other examples on that the scenarios can be generalised are FATF's guidance from September 2020 on risk flags for virtual assets[60] and Egmont's review of terrorist financing indicators[61].

10.3. Focus on two models for sharing of risk flags

The ability to prioritise shared information is crucial to the quality of a data-sharing mechanism for risk flags. Among other things, this will require banks using the shared information to be better able to set up processes for this and ensure less 'noise' as a result of false positives in the shared data set, cf. section 10.1.

It is also crucial for an effective data-sharing mechanism that clear guidelines can be set out for the sharing of risk flags. This is because banks will only be able to use shared risk flags effectively in their own KYC procedures if there is full transparency about the cause of a suspicion. One approach is to focus such guidelines on when a shared risk flag is adequately documented. 'Adequate documentation' means that the reason for the raised risk flag must be elucidated to the point that other banks can effectively incorporate the suspicion into their own KYC procedures[62].

An alternative approach is for risk flags to be shared only on the basis of generalised scenarios. In that case, the determination and ongoing development of the scenarios and prioritisation mechanisms will have to be assigned to a responsible body. The responsibility for this could, for example, be placed in the forum, FEHT, proposed by the sector, cf. section 8.

[60] FATF Report – Red flag indicators of Money Laundering and Terrorist Financing.
[61] FIUs and Terrorist Financing Analysis – A review by the Egmont Group. The Egmont Group is a body consisting of participants from 166 FIUs. Its purpose is to exchange expertise and support a joint international effort to counter money laundering and terrorist financing.
[62] For example, this could involve a justification in the form of a narrative and information about the underlying scenario and the thresholds applied for the customer.

If this is the case, it should be clearly communicated that the responsibility for adequately identifying all relevant risks in transaction monitoring rests with the individual bank.

The DFSA therefore estimates that risk flags can be shared at two points in the transaction monitoring process, namely after the risk flags have been prioritised automatically (model 1) or after they have been examined by a caseworker (model 2).

Model 1: Sharing of prioritised risk flags
One advantage of sharing prioritised risk flags is that the potential for automation is high. This is because the scenario method is effectively automated, and the same should apply to effective prioritisation of risk flags.

The sharing of prioritised risk flags presupposes that the banks' transaction monitoring processes are efficient. If this is not the case, there is a significant risk that the sharing of prioritised risk flags will create 'noise' in other banks' KYC procedures. On the other hand, the documentation required will be of a more technical nature, for example, information about the scenario and the customer's individual threshold.

Another advantage of sharing prioritised risk flags is that it is possible to use generalised scenarios directly as a basis for when a risk flag can be shared. This can reduce the complexity for other banks in regards to using the risk flags in their own KYC procedures, as it will create full transparency as to why the flag is being shared. One consequence of this, however, is that the degree of nuance will be lower than if risk flags can be shared freely. This is primarily due to the fact that it will not be possible to establish a framework for all scenarios that should be included in banks' transaction monitoring, cf. section 10.2.

Model 2: Sharing of examined risk flags
An alternative mechanism is one in which banks have the option of sharing the results of caseworker examinations into the risk flags. This model may be useful in two types of cases:

1. The examination raises a well-founded suspicion of criminal activity, and the suspicion is sufficiently well-founded for a report to be sent to the Danish FIU.

2. The examination raises a suspicion, but the suspicion is not yet believed to be sufficiently substantiated for it to be passed on to the Danish FIU. For example, this could apply in cases where communication with the customer about the specific matter has not yet sufficiently dispelled suspicion. A direct consequence of such a suspicion could be an adjustment of the customer's risk assessment.

The DFSA's is of the opinion that the sharing of examined risk flags has certain advantages compared with the sharing of prioritised risk flags:

- **Fewer false positives are passed on:** False positives will have been automatically filtered out and the risk flags will have undergone manual examination.

- **More efficient use:** Examined risk flags are subject to checks and balances via the manual case processing system. All other things being equal, this will mean that the suspicion of ML/TF will be more concrete than for the sharing of prioritised risk flags.

- **Composite package:** The manual examination will be based on the full customer knowledge and thus not individual risk flags. In most cases, sharing will therefore take the form of an composite package containing all risk information for a given customer and transaction.

This model does not presuppose that banks' transaction monitoring processes are effective to the same extent as the previous model.

On the other hand, the potential for automating the sharing of examined risk flags will be more limited. This is because, by definition, the examination involves manual processing by a caseworker. In addition, the documentation required will be more extensive than for prioritised risk flags, since, for example, a qualitative justification for the overall assessment should also be included.

10.4. The value of data sharing depends on the quality of transaction monitoring

The DFSA's assessment of whether the quality of Danish banks' transaction monitoring is adequate for the sharing of risk flags is based on the DFSA's evaluation of compliance with the rules for transaction monitoring in the largest banks. This is due to the expectation that the largest banks are at the forefront in terms of setting up effective transaction monitoring. One thing shared by all the banks surveyed is that data centres deal with all or part of the technical infrastructure.

The overall conclusion of the evaluation is that transaction monitoring has not been sufficiently effective. This is due in particular to the fact that the processes are not adequately documented, and neither do they adequately cover all elements of the banks' risk assessment or the risk classification of individual customers. The DFSA therefore issued a number of orders, some of which were so fundamental in nature that compliance requires changes at the data centres.

The DFSA is therefore of the opinion that the value of sharing risk flags depends on which model that is used and the time perspective that is desired for the implementation of the solution.

The necessity of objective criteria for prioritised risk flags

In the DFSA's evaluation, the challenges facing Danish banks primarily relate to the establishment of adequate scenarios and documenting the specific risks that each scenario individually seeks to mitigate. This entails a risk that actual questionable matters to a substantial extent currently are not flagged at all, and that the activities that are actually flagged in many cases are false positives.

The DFSA is therefore of the opinion that allowing prioritised risk flags to be shared freely is associated with a significant risk of:

1. Customers risk being rejected by a bank on an erroneous basis.

2. Banks are unable to manage the risks associated with customers. Erroneous data could contaminate customer knowledge and thus customer risk classification in banks that make use of the shared risk flags. This is also a problem because, due to inadequate audit trails, banks are unable to reassess the reason why a risk flag was raised at another bank.

3. The value does not justify the cost of establishing a data sharing mechanism, as only a (smaller) subset of the risk flags that could create value across the industry would be shared.

The DFSA's evaluation showed, for example, that in the period from 1 October 2018 to 30 September 2019, an average of 4,450 risk flags per month were raised across the banks surveyed, but only 5 per cent of these risk flags led to a report to the Danish FIU. One explanation for this is probably that several of the banks have not implemented processes for prioritising risk flags. The evaluation also showed that the bank with automated processes for prioritising risk flags filtered out almost 60 per cent of the risk flags raised before these were referred for manual examination. For this bank, just over 40 per cent of the prioritised risk flags resulted in a report to the Danish FIU.

On this basis, the DFSA is of the opinion that freely sharing prioritised risk flags on the basis of adequate documentation is currently of very limited use. The value of such a model requires the overall quality of transaction monitoring to be significantly enhanced at industry level, which should be ensured but will also be associated with a longer time frame.

If generalised scenarios are established for which prioritised risk flags can be shared, it is assessed that this is more useful. However, the time frame of such a data-sharing mechanism would also depend on the time taken to determine generalised scenarios.

Sharing of examined risk flags currently associated with greatest value

On the other hand, the DFSA assesses that, in many cases, examined risk flags that lead either to a report to the Danish FIU or to an adjustment of the risk classification of the customer relationship represent a genuine suspicion. This means that freely sharing examined risk flags will currently offer more value than prioritised risk flags.

This is primarily because the banks' challenges relate in particular to the automated part of the transaction monitoring process rather than the manual case processing of risk flags that have been raised.

However, the DFSA's evaluation also showed that the banks still face a number of challenges in regard to manual case processing procedures, including:

- Lack of clear and detailed guidance (workflows) as to how risk flags raised due to specific behavioural scenarios should be examined by a caseworker.

- Lack of organisation in the distribution of alarms to the appropriate caseworker. The risk flags largely reflect differing risks, and the competencies for assessing a specific risk will in many cases be distributed across caseworkers.

- Limited scope of quality checks and assessments of caseworkers' examinations regarding the risk flags raised.

This could result in both misleading reports and banks failing to provide reports to the Danish FIU of all relevant matters. In practice, the primary consequence of the inadequate processes is likely to be that banks use more resources than necessary when raised risk flags are examined manually[63]. For example, a director of a SIFI bank told the DFSA that the financial gain of an ordinary private customer disappears if this customer is selected just once for manual examination in connection with transaction monitoring.

In addition, inefficient calibration of the automated transaction monitoring process could have downstream effects on the quality of the manual case processing. For example, by:

1. Letting to many risk flags be sent for manual examination resulting in that a backlog arises in connection with manual processing, and thereby that the Danish FIU is not notified in a timely manner.

2. All relevant risk flags not being raised.

The DFSA therefore also estimates that the value of sharing examined risk flags could be strengthened if generalised scenarios are established. This is because the banks are likely to raise fewer false positives and refer them for manual examination, and caseworkers can therefore direct more of their efforts at genuinely questionable matters.

The sharing of risk flags involves costs for banks

Banks do not currently have the ability to share risk flags with each other. The sharing of risk flags will therefore require that they invest in their technical infrastructure if they want to take part in the exchange. This is likely to be associated with significant costs, particularly for larger and older banks, whose IT systems are often more extensive and complex to develop.

One thing all the banks evaluated have in common is that they have each outsourced all or part of the technical infrastructure for transaction monitoring to a data centre. These data centres are partly owned by the banks and play a key role in the implementation and maintenance of the technical infrastructure. The banks are actively involved in their work by means such as steering groups, and in some cases also by allocating resources to the data centres in connection with the implementation of various projects. For example, this applies to the inclusion of new data in transaction monitoring.

The DFSA estimates that the banks will be able to join together to cover some of the costs of developing the infrastructure. At the same time, it must be possible to develop it faster as

63 This is partly due to the fact that the banks that were investigated have implemented systems enabling caseworkers to systematically collect other relevant information that is crucial for a fair assessment.

it needs to be developed in fewer places. However, developing the IT systems must still be expected to take some time.

Another consequence of implementing an initiative that allows for risk flags to be shared is that banks must allocate additional resources to both document and examine the reason for a risk flag being shared. This is because the process of transaction monitoring cannot be harmonised and it will be difficult to justify not dealing with a risk flag that has been shared and received regarding a given customer.

The DFSA assesses that the sharing of prioritised risk flags on the basis of generalised scenarios will be associated with fewer costs in connection with documentation regarding a risk flag that is shared. At the same time, the transparency behind the purpose of such scenarios will reduce the amount of resources that need to be allocated in order to understand the reason for a prioritised risk flag. Costs to banks of implementing such a model are therefore primarily considered to be of a technical nature. This applies, for example, to the implementation of the various scenarios in transaction monitoring.

Resource costs, on the other hand, are likely to be higher in the sharing of examined risk flags. This applies both in terms of documenting the reason behind shared risk flags and for other banks in terms of using the information in their own KYC procedures. However, new costs relating to documentation should be limited, as banks should already have processes in place for documenting their work in examining risk flags.

10.5. The possibility of broader network analyses

As already stated, the starting point for banks' transaction monitoring is the scenario method. Effective transaction monitoring should also involve so-called network analytics, either as part of the automated monitoring process or as a tool to which caseworkers have access. Such analyses are currently only possible internally within the bank or group, for example by mapping suspicious transaction networks internally within the bank. Analyses can also be carried out in the form of taking a more holistic reflection on outliers across the overall customer base. However, this type of monitoring is not particularly widespread among Danish banks today, and in cases where it is used, it only drives a small proportion of the risk flags that are raised[64].

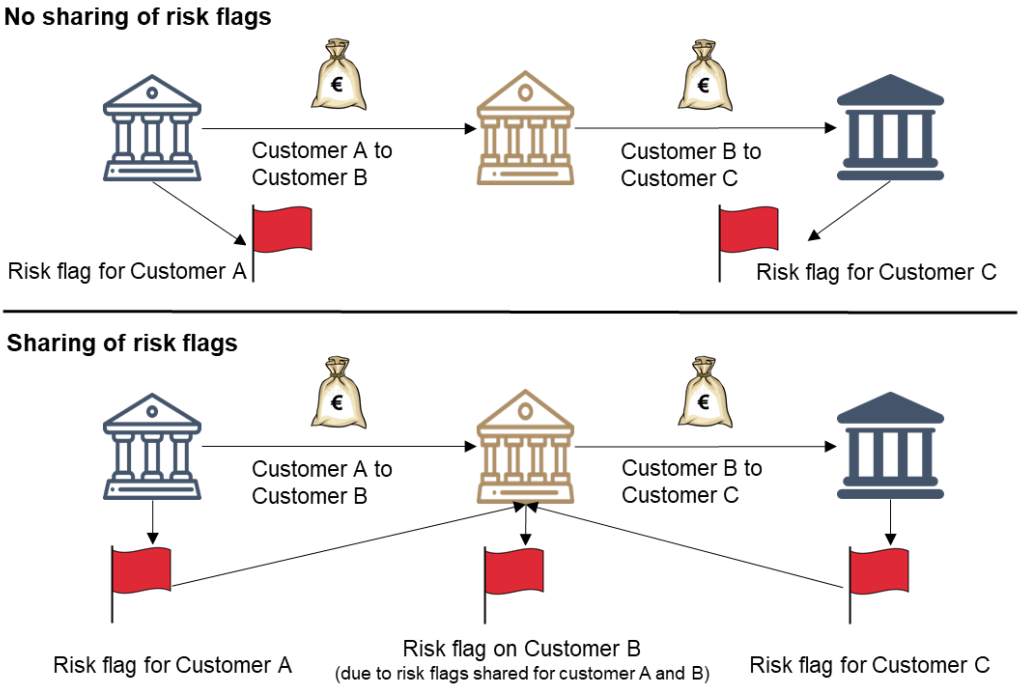
One general challenge, however, is that criminals often obscure their activities through a network of transactions, corporations, and accounts across many financial organisations at both national and global level. The banks' insight into such networks currently starts when funds are transferred to an account with the individual bank, and stops the moment the funds are transferred out of the bank again. This means it is impossible for the individual banks to track the movement of money across the financial sector, which in all probability limits their ability to identify all questionable matters.

If done correctly, the sharing of risk flags across the sector also has the potential to support this type of network analytics. If shared risk flags are enriched with the right master data, such as information about the sender, recipient and other information about the transaction,

[64] Based on observations in the DFSA's evaluation of compliance with rules for transaction monitoring.

this will facilitate the identification of networks of suspicious customers. This applies, for example, if money is transferred through a number of identified throughput accounts across banks, cf. Figure 10.3.

Figure 10.3 – Example of the potential of network analytics



Source: The DFSA.

10.6. The value of a centralised data sharing mechanism

In any case, consideration should be given to whether the risk flags should most appropriately be shared via a central function and whether it should be under the authority or administration of a public authority. Centralising the data sharing mechanism is associated with technical and potentially analytical advantages:

1. Both a standardised data format and a standardised ability to share and retrieve risk flags can be established. The banks will only have to talk to one player rather than the entire industry.

2. The access mechanism can be structured so that only the banks' special compliance officers have access to information – and only information that is relevant to their own customer relationships[65].

[65] For example, see considerations on the disclosure of information in the proposal for an extended PEP solution, cf. section 5.

3. A consolidated database will be created for risk observations across the sector which can be used for analytical purposes, for example to better understand criminal behaviour, or which alarms can be classified as false positives. It will also support network analytics across all shared risk flags[66].

However, the registration of risk flags in a central register must involve considerations about the processing of and access to personal data, particularly as to a great extent this information concerns possible criminal matters. At the same time, a decision must be made as to what responsibility to which this central entity is subject with regard to incorrect recording and verification of the information reported by the banks. For example, it must be ensured that shared risk flags are removed if the underlying suspicion has been dispelled.

10.7. Legal considerations

It is estimated that the sharing of risk flags is associated with legal issues, particularly in relation to the MLA 's rules on duty of examination and duty of confidentiality, cf. sections 25 and 38. The provisions implement Articles 40 and 39, respectively, of the AMLD. Section 25 of the MLA is worded as follows:

> *"**Section 25.**[67] Companies and persons shall examine the background and purpose of:*
> ***1.** All transactions that*
> ***a.** are complex,*
> ***b.** are unusually large,*
> ***c.** are carried out in an unusual pattern, or*
> ***d.** do not have an obvious economic or legal purpose.*
> ***2.** All activities that do not have an obvious economic or legal purpose.*
> *Subsection 2. Companies and persons shall, where appropriate, expand the monitoring of the customer with the aim of determining whether the transactions or activities appear suspicious.*
> *Subsection 3. The results of an examination shall be registered and stored, cf. section 30.*
> *Subsection 4. A registered person has no right of access to the personal data relating to him/her which will be processed in accordance with subsections 1–3."*

This provision means that the obliged entities must examine whether the matter deemed to be unusual provides grounds for suspicion or presumption of ML/TF or whether a possible suspicion can be ruled out. Depending on the circumstances, the examination pursuant to section 25 may entail a duty to notify, cf. section 26 of the MLA.

Section 38, subsection 1 of the MLA is worded as follows:

[66] For example, see the Swedish Bankers' Association's considerations on the sharing of risk flags between banks and authorities (pages 16–18): https://www.swedishbankers.se/media/4425/sammanslutning-mot-finansiell-brottslighet_vf.pdf

[67] Reproduced as newly drafted in connection with the Special Consolidating Act of October 2020, which is expected to be adopted in the current period. Amended in the light of the Commission's reasoned opinion.

*"**Section 38.** Companies and persons covered by this Act as well as the management and employees of said companies and persons as well as auditors or others who perform or have performed special tasks for the company or person are obliged to keep secret that a report has been submitted in accordance with Section 26, subsections 1 and 2, or that this is being considered, or that an examination has or will be launched in accordance with Section 25, subsection 1."*

The obliged entities are thus obliged to keep secret the fact that they have notified the Danish FIU or that an examination has been or will be launched pursuant to section 25. However, the provision allows the obliged entities to hand over the information to authorities and organisations that supervise compliance with the MLA, i.e. the DFSA, the DBA and the Danish Bar and Law Society Council. The information can also be shared within the company or with companies in the group.

Finally, section 38, subsection 6 allows for the possibility of sharing the information with other obliged entities, including banks (section 1, subsection 1, no. 1) if:

1. the information concerns 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 Anti-Money Laundering Directive, and

3. the recipient is subject to obligations with regard to confidentiality and protection of personal data.

The ability of banks to share information about their customers today
Section 38, subsection 6 of the MLA thus permits banks to share information on the above matters if the information relates to the same customer and the same transaction. Banks can therefore already share this type of information when the information is specifically relevant to their tasks in connection with the prevention and countering of ML/TF. Provided that banks observe the general rules regarding data processing, such as their responsibilities as data processor, and comply with the objective criteria (only information on own customers and joint transactions), there is no immediate impediment to prevent them sharing in this way via a central mechanism.

The confidentiality provisions do not support the sharing of risk flags
A model involving general sharing of examined risk flags and information about customers between banks will contravene the existing provision on duty of confidentiality in the MLA, as this is covered by the examination in section 25.

In the first instance, prioritised risk flags are also regarded as being covered by the provision on duty of confidentiality, since section 38 imposes a duty of confidentiality in connection with the fact that "an examination has or *will be launched*". The banks' monitoring systems are designed to identify suspicious matters that require examination. Risk flags are thus regarded as part of this process, probably at the stage where an examination *will be launched* either to disprove or confirm a suspicious matter (activity or transaction).

The solution involving general sharing of examined and prioritised risk flags thus requires that changes be made to section 38 of the MLA, which is an implementation of article 39 of the AMLD, which reads as follows:

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

Amendments to the provisions of the AMLD must be regarded as a more comprehensive process, ultimately requiring agreement among EU Member States, cf. section 11.

Proportionality of the infringement – examined and prioritised risk flags
Before further work is done on a solution that will require changes to the rules of the MLA and thus negotiations at EU level, a number of factors should be taken into account.

The purpose of sharing risk flags between banks is to strengthen society's ability to combat ML/TF. Improving the ability to share information about customer behaviour, transactions and activities means that banks, and thus society as a whole, can prevent criminals from continuing to act unlawfully. For example, today criminals can switch banks, meaning that the new bank needs to build up knowledge of the customer after the switch, or can use a network of accounts with different banks, meaning that the individual bank is only aware of a subset of the overall transactions. In the opinion of the DFSA, therefore, an option for sharing risk flags or other types of information will be appropriate in order to achieve the intended purpose.

Wide sharing of risk flags or other information about suspicious transactions, activities or behaviour is likely to offer tools to ensure a stronger effort to counter ML/TF, particularly in relation to crime that extends across one or more obliged entities. The DFSA's initial assessment is that a model including general sharing of risk flags and similar information offers the greatest potential.

In regard to the proportionality of the model, it may be regarded as meeting an urgent societal need, since the fight to combat ML/TF is an essential societal task. Under the current rules, obliged entities are already required to raise and examine risk flags based on a customer's behaviour, transactions, and so on. It is therefore not a question of registering new information about customers, but rather that information already held by banks be made available to other banks, for the same purpose for which it is collected.

It should be noted, however, that the lower the degree of assessment and examination that the individual bank has undertaken, the greater an intrusion it will represent in regard to customers. Among other things, risk classification of the individual customer forms the basis for the established parameters (thresholds) as to when the systems should generate a risk flag. Considerations should therefore include the extent to which high-risk customers, such as PEPs and RCAs of PEPs, will be more likely to trigger a risk flag, even if, on closer examination, there is nothing suspicious about a transaction or activity.

This suggests that a solution will have to be built with a high degree of assurance that the suspicion is substantial. This could, for example, be in the form of objective criteria for priority risk flags if other banks are to share and use them. The balance of proportionality may also vary, depending on how many and which employees in the banks have access to information, and on whether information can only be accessed about the bank's own customers or about all customers in the system.

The smaller the number of employees who have access to the information and the less information that is made available, for example for the bank's own customers only, the less intrusive the model will be. A model in which only information about the banks' own customers regarding transactions in the bank is shared is, in principle, accommodated by the possibilities of section 38 of the MLA.

A model of this nature, however, requires the establishment of a mechanism that is sufficient to handle these criteria, just as criteria for deletion, updating, and so on will need to be established.

De-risking

Regardless of which model is considered, it is important to avoid de-risking and blacklisting. Among other things, it would be questionable in terms of legality if information about examinations or reports to the Danish FIU performed by other banks were automatically to result in other banks rejecting the customer, or automatically filing a report to the Danish FIU, cf. section 2.

Considerations regarding a centralised public register of personal data

Among other things, a central data-sharing mechanism under the auspices of a public authority has the advantage that it will be clear what information the individual banks share about their customers, and that they do not, for example, share information that is not related to ML/TF or similar. In addition, public authorities are generally experienced in establishing a secure and easily accessible digital infrastructure, for example in connection with the processing of personal data.

Registering information and sharing it in a public register will involve considerations about the processing of and access to personal data. This is because risk flags, examinations and reports to the Danish FIU are based on a suspicion of or link to ML/TF. In principle, such information will be characterised as information on possible criminal offences committed by natural persons. This means that the rules of the GDPR must be observed, unless the processing is covered by the Danish Law Enforcement Act[68].

The provision on confidentiality in section 38 of the MLA is only directed at those companies and persons that are subject to the MLA, and does not include authorities that receive information about customer relationships, examinations and reports to the Danish FIU as part of the exercising of their authority. The possibility of sharing risk flags will thus not necessarily be contingent on an amendment to the AMLD. On the other hand, public authorities are subject to other sets of rules regarding professional secrecy and disclosure.

[68] Act on the Processing of Personal Data by Law Enforcement Authorities, Act No. 410 of 27 April 2017.

Creating the register in the public sector also gives rise to a large number of other legal considerations, for example in connection with:

- Who is responsible for data, validation, control, etc.

- Deletion, the right of access and the question of possible liability in the event that erroneous information has been shared or where shared information has been used contrary to the purpose and, for example, has affected a customer's ability to obtain a business loan – resulting in financial loss.

- Administrative and financial costs to the public sector, which will have to be weighed against the anticipated impact on the prevention and clarification of ML/TF.

A specific position must be taken as regards the structure of the register and the expected criteria for sharing, etc. before any final legal assessment of the possibility of establishing such a register in the public sector can be made.

11. The process for further international work

The DFSA recommends that in connection with the decision on further work with the proposals identified in the other sections of the report, a decision be made to simultaneously initiate a prioritised Danish effort under the auspices of the EU to realise and strengthen the impact of these proposals. This refers in particular to increased harmonisation of the current provisions of the AMLD on KYC procedures and identification of beneficial owners, targeted changes to the provisions on duty of confidentiality and increased use of new technology. These aspects must be viewed as a whole. A Danish effort could be launched prior to or in connection with the expected revision to EU rules as part of the Commission's forthcoming proposal in this area in the second quarter of 2021. However, a Danish effort may be expected to extend over a longer period, due to both the political and technical scope of the EU negotiations, while it may be difficult to obtain the necessary support for certain changes from other entities, such as other EU Member States, the European Parliament and the European Commission.

For a number of the specific proposals mentioned in other sections of the report, particularly in sections 4 and 10, action will be necessary or appropriate at international level, in particular within the EU, to remove potential impediments in existing EU regulations or to strengthen the full impact of the proposals.

The EU is currently preparing new measures to combat ML/TF. At the beginning of May 2020, the Commission published an action plan for new EU measures, and is expected to present concrete legislative proposals in the second quarter of 2021. However, the legislative proposals are likely to be discussed at the level of the Commission's Expert Group on ML/TF (EGMLTF) before then. Among other things, the expected measures include better harmonisation of EU rules in the area of money laundering through a proposal to amend the AMLD, including moving parts of the Directive to a Regulation.

Denmark thus has a window in which to contribute specific views and raise issues either prior to or in connection with these EU negotiations. However, amendments to the provisions of the AMLD must be considered as a more far-reaching process, which ultimately requires a qualified majority of EU Member States and the support of the European Parliament, which is a co-legislator. In practice, the Commission should also support the changes in order to ensure broad support and legitimacy.

A prioritised Danish effort under the auspices of the EU is particularly relevant to two key parts of the current AMLD if further work is to be developed: Better harmonisation of rules regarding matters such as KYC procedures and identification of beneficial owners (section 11.1) as well as targeted relaxation of confidentiality provisions (section 11.2).

11.1. Better harmonisation of rules

Improved harmonisation of the rules on KYC procedures and identification of beneficial owners could result in more effective countering of ML/TF and open up new and more effective opportunities for the sector, cf. section 4.

In November 2020, ECOFIN adopted Council Conclusions on anti-money laundering and countering the financing of terrorism[69], which represents the Council's strategic and prioritised input to the Commission's forthcoming package of proposals in this area. Among other things, the Council Conclusions state that the Council invites the Commission to move specifically mentioned parts of the AMLD to a Regulation:

> *17. INVITES the Commission to present a legislative proposal for a regulation based on an assessment of the relevant risks and impact with a view to further harmonising substantive law, taking into consideration the following areas: […] customer due diligence requirements – including adequate remote due diligence solutions as well as electronic identification and verification –; provisions on due diligence for domestic and foreign politically exposed persons; […] provisions on determining beneficial ownership […]*

In principle, therefore, there is broad support for further harmonisation of these provisions in the AMLD by moving them to a Regulation. At present, however, it is unclear whether the specific wording of the provisions of a regulation would be adequate in order to deliver the desired added value. That said, Denmark will be able to prioritise trying to make sure of this. In addition to this, Denmark has a number of other priorities in relation to the conversion of the AMLD into a Regulation, including ensuring that the existing strictness of Danish national anti-money laundering rules is not weakened during this process.

11.2. Relaxation of the confidentiality provisions

The ability to proceed with the proposal to share risk flags between banks, cf. section 10, is contingent on a relaxation of the confidentiality provisions in the AMLD. As can be seen from that section, there are opposing considerations, both of which carry substantial political weight.

On the one hand, within the EU as well as at international level, there is a strong focus on countering ML/TF, and cooperation across authorities and the sector, in particular, is viewed as an opportunity to significantly streamline efforts. This means it cannot be ruled out that a proposal providing for the possibility of information sharing in the sector in order to support this agenda could gain a foothold in the EU negotiations during the expected revision of the EU Anti-Money Laundering rules and result in decisions that can facilitate workable solutions in regard to the potential relaxation of the confidentiality provisions.

On the other hand, it must also be assumed that it will be very difficult to obtain the necessary support from other Member States in the Council and from the European Parliament, including, in practice, the Commission, for changes to the provisions on confidentiality if this entails a risk of coming into conflict with the crucial consideration that suspicious customers are not (directly or indirectly) informed that the bank suspects them of anything (the so-called tipping-off ban). There may also be opposition to sharing information about customers, since the Commission, the European Parliament and some EU Member States have a very strong desire to give very high priority to data protection. In addition, there is a fear, perhaps not

[69] https://data.consilium.europa.eu/doc/document/ST-12608-2020-INIT/da/pdf

entirely unfounded, that it could lead to further de-risking. Any attempt to change the provisions on confidentiality will therefore require a targeted, carefully worded derogation with adequate protection of customers.

The aforementioned ECOFIN Council Conclusions also address this issue and the tension between the various considerations:

> *20. INVITES the Commission to widen the scope for the use of data within the limits set by data protection provisions, also by making better use of digitisation. INVITES the Commission, while maintaining the tipping-off ban and providing sufficient safeguards for information protection, to consider the expansion of information-sharing possibilities within groups of companies as well as between other obliged entities not belonging to the same group or the same sector, so as to allow better monitoring and compliance.*
>
> *21. URGES the Commission and the European Data Protection Board to provide clarification on how to reconcile the AML/CFT framework with the applicable data protection legislations, notably with the General Data Protection Regulation in order to provide more clarity on the data that can be shared between obliged entities, as well as between obliged entities and competent authorities, and to ensure a high level of data protection, and to resolve, for example, inconsistencies between data protection provisions and the tipping-off ban. Furthermore, all possible synergies with other EU legislative acts should be taken into account.*

The Council therefore immediately supports considering increased data sharing across obliged entities, but with adequate security measures and without undermining the tipping-off ban. If it is decided to proceed with the proposal, further work is required in order to formulate a relaxation of the rules that is targeted and narrow enough to support the sharing of information without compromising other considerations.