FINANŠU NOZARES ASOCIĀCIJA

Doma laukums 8A-6, Rīga, LV-1050
Reģ. Nr. 40008002175
Tālrunis: 67284528
info@financelatvia.eu
www.financelatvia.eu

RIGA

19 June 2019

REPORT
regarding KYC utility

[1] Scope

This report addresses creating a legal framework to enable businesses to launch KYC utilities shared by several obliged entities beyond a consolidated group (hereinafter **– the shared KYC utility**).

The improvement of customer checks and the introduction of information sharing tools for strengthening ML/FT risk management has become a global topicality. Each state and financial institutions operating region-wide pick solutions that are most convenient for them, which make such solutions individual, therefore it is important for each state, acting together with the industry and possibly the representatives of the largest stakeholders to decide on the best form for setting up the shared KYC utility, to reach the highest compliance standards and therewith improve the reputation of the state and cut the total customer verification costs.

On September 25, 2018 the Cabinet of Ministers of Latvia on approved a plan on AML/CFT activities for implementation by the end of 2019. Paragraph 4.10 provides that the shared KYC utility might be one of the solutions. Finance Latvia Association is mentioned as one of the responsible organizations.

The Council of Finance Latvia Association on December 3, 2018 tasked the Board to evaluate the option of creating a KYC utility, hence this report is drafted, and to maintain this issue in relations with the government as an important policy objective.

The report has been circulated to Association's Legal Committee and co-chairs of the AML committee as well as Data protection working group. The proposals received are included in the report.

This report shall be considered as a policy document which gives an overview on the topic and contains observations and proposals that are not final and are intended for further elaboration after submitting it to the Ministry of Finance.

This report is not about establishing any particular shared KYC utility.

[2] Introduction to the model

The proposals in this report stipulate that according to the law in force in Latvia there are four main information sharing possibilities:
1) in-between the parties involved in executing a single transaction;
2) within a consolidated group;
3) via private-private information sharing about the clients with whom business relationships have been terminated or they were refused to establish due to ML/TF concerns;
4) public-private information sharing partnerships akin to UK JMLIT.

Besides this report considers that banks are entitled to access several public registries (population, vehicle, invalid document register, state revenue service data, land book) free of charge for KYC process needs and use licenced credit bureaus as a single access hub.

PEP register will be accessible to obliged entities as of August 2019.

The shared KYC utility is not intended to be a *super* system covering all aspects of KYC process, shifting liability or creating a "one size fits all" solution/a model.

Obliged entities can create the shared KYC utility by outsourcing to one service provider parts of KYC process, and this model does not require licensing other than provided for by the competition law. Such model could be described as a privately-owned shared KYC utility. **This type of shared KYC utility is more suitable for the banking sector** (like Nordic KYC project).

The shared KYC utility or a part of it can be organized as a channel to obtain information from public registries and use it to identify a client or create a profile of a customer what could afterwards be shared with other obliged entities for identification purposes (usually upon clients request). Such model would require access to public registries and mostly would apply to private individuals.

The shared KYC utility mainly should cover sharing information concerning some significant parts of the KYC process defined by law, based on AML/CFT experts' advice, and is not covered by this report. Such shared KYC utility would provide information to its clients as a service. For example, significant parts of a KYC questionnaire or in case when a person is put on specific lists (sanctions list) or can be associated with higher risk (PEPs). It should not include all clients of all obliged entities; different variations are possible.

Therefore, the shared KYC utility operates like a credit bureau (provide a part of information necessary in loan issuing process), **and mostly is necessary for non-banking sector**. This report acknowledges that data protection should be addressed as a part of the framework of the shared KYC utility. In this respect the report suggests focusing the type of shared KYC utility described in this section only to corporates and individuals associated to corporates, and individuals mentioned in this section. Thus, a licensing regime should be considered to such model of shared KYC utility.

Information exchange in-between several shared KYC utilities shall be possible and is dependent on whether obliged entities would be interested in implementing it.

The proposal does not consider an obligation to participate in any shared KYC utility.

The report does not propose to regulate KYC tools that are available on the market and offer information gathering from publicly available resources.

[3] Background

In the evaluation report *Moneyval* indicates that a number of areas that are associated with the identification and prevention of money laundering and financing of terrorism (hereinafter – **ML/FT**) risks in Latvia require significant improvements.[1]

The Action Plan for implementation of the recommendations set out in the *Moneyval* report by 1 March 2019 was approved by the CoM on 25 September 2018. It foresees "to draft an assessment on the legislative amendments required for the introduction of a KYC utility allowing the obliged entities to make use of customer due diligence information collected by other obliged entities".[2]

It is generally accepted that a sound and functional economy requires an appropriate risk culture. Processing of huge amounts of information on borrowers for credit exposure management is conventional and regulated. The contemporary ML/FT and international sanctions risks are gaining in relevance and thus it is necessary to come up with a tool allowing use and collection of such information in a sufficient manner.

The countries that have implemented *KYC utilities* recognize that the "know your customer" remains *painful* industry-wide from the perspective of regulatory risk, operational cost and customer experience. The persons willing to use or which render assistance for the use of the financial system for illegitimate purposes, have a good chance of making use of the differences in the access to information by obliged entities and other corporates which have to and which safeguard that no such persons could undisturbedly access the financial system. The KYC utility is a tool intended for preventing[3] and to allow transition from withholding or from refusing to face risks to more qualitative and appropriate risk management.

[4] The scope of the shared KYC utility

Before establishing and while upkeeping a business relation, every obliged entity within the meaning of the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter – AML/CFT Law) must perform customer identification and assessment, by additionally also conducting transaction monitoring. KYC – **Know Your Customer** – comprises all these measures for the identification of the customer, its operations and cooperation partners.

In order to ensure a comprehensive accomplishment of this task, it is worked upon development of technological tools (hereinafter – IT) for importing data from several sources to a single

[1] See Latvia Fifth Round Mutual Evaluation Report. Moneyval, Strasbourg, 2018. Available under: https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b

[2] Action Plan for Anti-Money Laundering and Counter Terrorism Financing for the term till 31 December 2018, Paragraph 3.2. Available under: https://likumi.lv//ta/id/302218?&search=on

[3] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapore. Available under: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

platform – comprising publicly accessible and restricted, state-maintained, as well as private information provided by the customer of the shared KYC utility.

The tool share transactions when operating within a single obliged entity or a group of companies, however it may also operate as a data aggregation which ensures data sharing and comparison without accumulating such data. **An individualised solution** at the level of a single obliged entity may though exist, however, such a solution will not account for significant overall contribution.

A **centralised data repository** or a **decentralised data processing tool** are both possible by considering the solution of a specific developer, the applicable legislative requirements and personal data protection requirements.

It is also possible to combine both these models, e.g. at credit information bureaus part of information is kept within a single database, whereas part of information is obtained for immediate sales purposes and/or rating purposes.

Irrespective of the model of the data processing tool, it requires setting up a safe information sharing medium, a machine-readable data structure and a single/open standard for technical solutions available to the public as well as private sector (including API). Thus, it would be recommendable to introduce a single channel (aggregator) for the transfer of data of public registries.

[5] Information Sharing

Effective management of ML/FT risks requires cooperation of a number of obliged entities and public institutions, including information sharing, which can be described as private-private or public-private information sharing. The current wording of the AML/CFT Law foresees information sharing or acquisition limitations, for the most part focusing on sharing information pertaining to a single transaction.

AML/CFT Law provides, predominantly, for information exchange channels only for the use of financial institutions. Only financial institutions may mutually recognize customer assessment and mutually exchange the data (Article 29, Credit Institutions Law, Article 62(8)), provide information to correspondent banks (Article 44), to other financial institutions for the purpose of specific transactions (Article 38), access different state registers free of charge (Article 41) and exchange data on customers with whom transactions were not started or have been terminated due to ML/FT risks (Article 44). Separate obliged entities may disclose to the FIU the fact of certain transactions (Article 38) and acquire data from the Register of Enterprises (Article 5.[1]). All obliged entities have the right to engage in mutual exchange of information, likewise, exchange information with state authorities within the framework of the FIU's **Cooperation Coordination Group** (Article 55).

Thus, currently the possibilities of all obliged entities to acquire and exchange information are limited. Nevertheless, it is rather complicated to set up infrastructure that would enable participation in the acquisition, analysis and information sharing of all the entities due to considerations of data safety, limited resources and differing interests in the acquisition and

further use of certain data. Thus, it is necessary to introduce legal and technological tools for addressing this matter (*see Paragraph 4).*

Countries are encouraged to assess how voluntary information sharing which is beyond what is required by the FATF Standards can improve their possibilities of identifying and preventing potential ML/FT risks and to align their legislative framework to enable such information sharing.[4]

[6] KYC utility and shared KYC utility

A KYC utility is one of the tools that can be used for effective information sharing, it enables moving from a case by case basis to a systemic and structural solution. A KYC utility which incorporates several individual and public data sources to ensure information exchange options is a contribution of general public importance. It is possible to distinguish several levels of cooperation. The first level deals only with the structuring of generally accessible information, the second level involves interconnection with public registers, third – sharing of customer questionnaire data and customer due diligence information, besides, considering that the levels two and three would involve several obliged entities, hereinafter it would be referred to as the shared KYC utility.

It increases efficiency of processes as several obliged entities do not have to engage in repeated acquisition of information regarding one and the same subject-matter, although it does not exempt the obliged entities of the duty to identify customers and to clarify basic information. Secondly, it significantly encumbers the "migration" of individuals engaged in unlawful or suspicious activity from being serviced by one subject of the law to another, in order to misuse the time required for the obliged entity for undergoing risk identification anew. Thirdly, without limiting the possibilities of the obliged entities possessing large resources to obtain data from other data sources, a utility creates a platform for the disclosure of the acquired data to the obliged entities with limited resources. The platform is supplied with data that potentially useful for all obliged entities. Such data may also serve the purpose of identifying (verification) of controversial information. Fourthly, the launch of the shared KYC utility will allow information sharing by the obliged entities therewith cutting the total investments in ensuring the compliance function.

The role of financial institutions in fighting financial crimes is to identify, accordingly verify and report on, suspicious activity to prevent non-compliant actors from accessing the financial system. The role of information sharing partnerships is to participate in the performance of this obligation, to do it more effectively and with less investments for a possibly wider range of obliged entities.[5] This function is already implemented by financial institutions who invest considerable resources in performing the same.

The introduction of the shared KYC utility will allow for easier identification of ML/FT risks, considering that in case one obliged entity has performed assessment and identified high ML/FT risk for a certain customer or its transactions, the obliged entity would feed the given data into

[4] Guidance on private sector information sharing. FATF, Paris, 2017. p. 25.

[5] Standard Chartered Wants Greater Sharing of Financial Intelligence. Available under: https://blogs.wsj.com/riskandcompliance/2018/09/27/standard-chartered-wants-greater-sharing-of-financial-intelligence/

the shared KYC utility and other obliged entities will have the chance to make use of these data in their operations. Thus, the obliged entities would not have to start the evaluation from zero, therewith identifying and bringing to a halt the use of proceeds from suspicious or unlawful acts considerably faster. In fact, this means that the obliged entities under AML/CFT Law not possessing sufficient IT and human resources are reasonably incapable of completing all necessary tasks to verify that the customer or its transactions cause no ML/FT risks.

The shared KYC utility is comparable to a credit information bureau, namely, as databases receiving information from users of credit information and certain national registers, and that are accessible to all users of credit information who simultaneously also share such information (the principle of acquisition of information by credit information bureaus: **you can receive information if you contribute, however you cannot receive without giving).** The operations of the shared KYC utility would be based upon a similar principle.

To sum up, the shared KYC utility is a customer due diligence tool which operates as a data repository where financial institutions, other obliged entities, state institutions and companies feed information and the outcomes of customer due diligence available to them for possibly effective identification and prevention of potential ML/FT risks and financial crimes.

[7] Possible legislative framework

Similarly, as in case of establishing a credit information bureau, the introduction of the shared KYC utility platform requires a **legal framework –** legal basis for data sharing.

If the shared KYC utility is maintained by a private law subject, it requires a licence, in case it is involved in the sharing of information contained in public registers or acquired as the result of customer due diligence. The supervision of such obliged entities at state-level is mandatory (could possibly be carried out by the Data State Inspectorate or the FIU).

The solution will require amendments not only to the AML/CFT law, but also require enactment of separate Cabinet of Ministers Regulations that would govern a number of detailed issues (deadlines, licences, information structure etc.). It will be addressed at the end of the document.

[8] Liability

The shared KYC utility does not exempt the obliged entity from liability for the sufficiency of ML/TC risk management. The utility serves the purpose of an effective ancillary tool for accomplishing this assignment.

In case the law permits recognition of customer due diligence outcomes among the obliged entities, a model is possible under which certain obliged entities maintain a single customer profile (portfolio). However, in practice the setting up of the shared KYC utility as a single customer due diligence and information storage platform turned out to be unsuccessful due to high costs. Thus, by considering the practical examples, it would be more appropriate to develop

a tool for sharing specific information only without setting up joined customer profiles that would be used by all obliged entities on a single platform.[6]

[9] One-stop agency principle

The shared KYC utility can also be used as a single-entry point for customer on-boarding. Customer identification may be offered by corporates to obliged entities as an ancillary service (although usually it is considered a risk increasing factor, in case the customer is identified by a third-party agent) or any of its stages.

A KYC questionnaire that is filled out by the customer for one obliged entity does not automatically exempt the other obliged entities of the duty to identify the customer and undergo customer due diligence. This is an ancillary tool for identification and verification of information. However, for convenience purposes it would be admissible that the customer uses the same technical data template for several obliged entities.

For example, it has been recognized in Singapore that customers may not interact with the shared KYC utility; this should be left for the obliged entities.[7]

Latvia should stick to this principle. The same should be attributed to the right of law enforcement institutions to access information and it should be acquired directly from the obliged entities. The FIU would have the authority to access data directly from the platform, analyse customer structure trends and identify problem issues in a timely manner.

[10] Contribution of data: a right or a duty

The law should clearly state whether participation in the shared KYC utility entails a right or an obligation of the obliged entity. It could be set as an obligation for specific obliged entities and as a right for other. In case it is set as an obligation, the regulations of the Cabinet of Ministers should also fix a price formation principle for the use of such data to exclude that the price applied to the obliged entity for performance of its statutory duty by another corporate is incommensurably high.

[11] Shared KYC utility and corporates

The access to the shared KYC utility should be granted to corporates (e.g. SMEs) which although would not be granted the option to process the entire information, however, would have the possibility to verify in a simplified form, e.g. using a risk rating scale, whether their cooperation partner is a high-risk business entity and accordingly refuse cooperation or cooperate only after being granted certain assurances or warranties. In case of limiting cooperation with high risk businesses and better identification and management of risks deriving from such cooperation, the

[6] MAS to shelve 'know-your customer' project due to high costs, work on SME innovation platform. Available under: https://www.straitstimes.com/business/banking/mas-to-shelve-know-your-customer-utility-project-due-to-unexpected-high-costs-ravi

[7] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapore. Available under: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

obliged entities and particularly financial institutions would have to make pro rata investments in transaction monitoring what would also strengthen the business environment of Latvia.

One of the most significant information segments that is faced by business entities includes international sanctions, commonly referred to as sectoral sanctions that cannot be verified based on a specific list check-up approach. In case obliged entities or other business entities would identify such persons, cover-up businesses and other persons assisting in indirectly circumventing the sanctions, this information could be shared with others via the *shared KYC utility*, therewith warning others.

[12] Global trends, lessons learned from them

At international scale there is a regional and overall urgency for setting up a high quality shared KYC utility – multiple recent developments speak for that: five largest North European banks are currently developing a joint KYC tool; HSBC bank recently agreed to sell its compliance system that is intended for customer due diligence as this solution covers cooperative and also institutional clients and to offer it as a service that is accessible also by other financial institutions.

There are several approaches for operating the shared KYC utility. The existing cross-border KYC utilities operate as full-service providers and comprise check-ups and entry monitoring or operate **without** setting up or attraction of any tools for information sharing among stakeholders, however this approach is associated with a high level of information duplication.

Different forms of the KYC utility platforms operate globally for around 5 years.

There are several shared KYC utilities operating models, entailing different advantages and drawbacks:

- **Public model** – the shared KYC utility that is maintained and belonging to the state, involving the necessity to address the issue as to how it will be administered and what does it mean in terms of liability;
- **Public-private model –**belongs jointly to the state and private entities. Thus, it is necessary to determine the form of operation of this model in terms of contributions and potential profit sharing, possibly it should be set up as a non-profit entity;
- **Private model –** the utility would either belong to one financial institution or a special-purpose vehicle (SPV) which would administer the platform and offer it as a service. In case the platform would be owned by a single financial institution it would be impossible to use it on a wider scope and ensure complete independence.

In Singapore it has been recognized that the setting up of a separate entity would be the most appropriate solution.[8]

In all, the most suitable form of operation would be a public - private partnership (PPP) as it would neither belongs to any industry or the state and would therewith ensure independence and higher level of safety as the utility would be overseen at national level (functional supervision, a licensable subject).

[8] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapore. Available under: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

To set up a PPP model, the state should initially invite stakeholders to join in and test the utility.[9] However, it should be recognized that at a global scale more widespread are models which do not involve the state, namely financial institutions agree on the establishment of a joint venture for collecting their KYC information, therewith facilitating customer check-ups.

The leading Nordic banks *DNB Bank, Danske Bank, Nordea Bank, Svenska Handelsbanken, and Skandinaviska Enskilda Banken (SEB)* have announced their plans to set up a KYC utility as a joint venture. The joint venture will be owned and controlled by the founding banks, with a focus on developing an efficient, common, secure and cost-effective utility for sharing confidential customer credentials. After commencing its operations *Nordic KYC utility* plans to service large and midsize Nordic corporates.[10] As per the accessible information, it may be concluded that the solution does not foresee that the state will feed into the utility the information at its disposal. This KYC Utility will be active in the Nordic region offering KYC services consisting in gathering, validating, and providing to customers the information required under the applicable AML/CFT regulations, to facilitate compliance with these regulations.[11]

The South African shared KYC Service is a result of a partnership amongst the largest financial institutions of South Africa and Refinitiv (former name - Thomson Reuters). The South African shared KYC Service make collection and distribution of information easier. Large corporations, hedge funds, asset managers, and others use the South African shared KYC Service as an efficient, centralised solution for sharing KYC documents and information among several financial institutions through a secure and free-of-charge web-based portal. The main reason for the efficiency of the South African KYC service is a KYC information collection policy that has been standardised across all participating financial institutions.[12]

In 2014 the South African Reserve Bank fined the country's four largest banks a collective fine of 8 million EUR for failing to implement adequate anti-money laundering controls and risk measures. 2016 marked the launch of a KYC utility partnered with *Thomson Reuters (current name – Refinitiv)* to efficiently combat ML/FT risks and to reduce the costs of customer assessment.[13] Also in case of South Africa, the state does not supplement the KYC system with information at its disposal.

It must be noted that the African *Afrexim* bank has set up its own *KYC tool – MANSA.* MANSA was intended to serve the purpose of a repository that would cooperate with the leading African banks and regulatory authorities to ensure the most comprehensive *KYC tool* in Africa. Information about MANSA emerged only in July 2018 and no detailed information on its performance in reaching the set goals is available so far.[14]

---

[9] Splitting the bill. The role for shared utility s in financial services regulation. Available under: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-thecityuk-splitting-the-bill-the-role-for-shared-utility s-in-financial-services-regulation.pdf

[10] Nordic banks explore shared KYC utility. Available under: https://www.finextra.com/newsarticle/32178/nordic-banks-explore-shared-kyc-utility?utm_medium=dailynewsletter&utm_source=2018-6-1&member=63850

[11] http://europa.eu/rapid/press-release_MEX-19-3011_en.htm

[12] The South African KYC Service. Available under: https://africa.thomsonreuters.com/en/products-services/risk-management-solutions/kyc-as-a-service.html

[13] South Africa leads the way in KYC compliance. Available under: https://blogs.thomsonreuters.com/answerson/south-africa-leads-way-know-customer-kyc-compliance/

[14] About MANSA. Available under: https://ej.uz/e4p1

In 2017 the Monetary Authority of Singapore (MAS) announced that it is piloting a national *shared* know-your-customer (KYC) utility for financial services, based on the *MyInfo* digital identity service, developed by the Ministry of Finance.[15] Singapore intended the KYC utility to enhance customer on-boarding and verification through the *MyInfo* system.[16] It was planned to put the KYC utility in place by the end on 2018, however due to the costs and also because of insufficient activity of financial institutions in feeding information into the system as it is a complicated process and requires significant investments, the implementation of the KYC utility has hit a snag and the date of launching and putting the utility in operation remains unclear. The managing director of the Monetary Authority of Singapore Ravi Menon notes that, greater complications arose from streamlining KYC processes for corporates than individuals. Financial institutions would among other things, have to figure out the beneficial owners of entities such as shell companies, which creates complications in establishing credentials.[17] In case of Singapore, the assignment of setting up the utility was taken by the state, provided that private financial institutions will furnish information.

In terms of information accessible, the Singaporean model, although not fully operational yet, should be considered the most rational one, although it must be noted that the planed cooperation model (single customer profile accessible on a common platform by several obliged entities) is an expensive and ambitious solution and from this perspective it should not be used as the best example. If the existing South African and the planned North European models foresee that financial institutions share information at their disposal, the Singaporean utility would receive customer information at the disposal of financial institutions and state registers what could reduce one of the major problems faced by KYC utilities, namely, information credibility. The information that is found in state registers has a higher degree of credibility than that at the disposal of financial institutions.

Thus, there is room for the conclusion that globally there are different shared KYC utility models – North European banks are looking forward to set up a private utility, the South African utility is private, though partnered with the international media and information company Refinitiv, the Singaporean utility is set up by the state in partnership with financial institutions.

The idea behind the shared KYC utility is to serve as a tool assisting financial institutions in performing customer assessment and for curtailing and preventing ML/FT risks. However, the liability for customer due diligence would still lie with the financial institution. It is expected to streamline the shared KYC utility in the future allowing a liability shift, i.e. the shared KYC utility would be improved and contain sufficient information to undergo customer assessment and financial institutions will no longer have to perform assessment and assume liability as it would be taken over by the shared KYC utility. This is the ultimate (supreme) and potential future objective of the utility.

[15] MAS to roll out national KYC utility for Singapore. Available under: https://www.finextra.com/newsarticle/30332/mas-to-roll-out-national-kyc-utility-for-singapore

[16] MAS working closely with local and foreign banks to explore a Banking KYC Shared-Services Utility Available under: https://www.opengovasia.com/mas-working-closely-with-local-and-foreign-banks-to-explore-a-banking-kyc-shared-services-utility/

[17] Singapore's KYC utility experiment hits snag: MAS. Available under: https://www.businesstimes.com.sg/government-economy/singapores-know-your-customer-utility-experiment-hits-snag-mas

[13] Range and scope of information available

For the introduction of the shared KYC utility the first decision as to the information scope covered by it should be - whether the customers involved in such information sharing are exclusively legal entities and legal formations or those are also private individuals. In case those are legal formations then mandatory will be the processing of the data of affiliated private individuals only. In case the tool will comprise also private individuals, then it must be determined whether those will be all private individuals or only private individuals associated with legal formations and private individuals causing increased risk due to their political prominence, specific ML/TF events (see. e.g. AML/CFT Law Article 44) or due to the risk of international sanctions.

To ensure flexibility in developing new utility products, generally accessible information and information that can be acquired in accordance with the applicable laws should not be regulated.

The shared KYC utility is not intended for the processing of all information obtained during customer due diligence or transaction monitoring. Instead, the part of such information acquired in accordance with the AML/CFT Law Article 11.[1], as determined by the Cabinet of Ministers or that is generally accessible.

Moreover, a fee would be applied for the acquisition of information from public registers, where the amount thereof should be determined in centralized manner (uniform fee set by the Cabinet of Ministers) allowing for easy and transparent administration.

[14] Seminar thesis

A seminar aimed at **strengthening the "Know Your Customer" principle and information exchange partnerships for more effective combatting of financial crimes — "AML/CFT: RegTech & Partnerships"** was held on 23 November 2018.

The representative of the Latvian Chamber of Commerce and Industry recognized that for the purpose of solving AML/CFT matters, the state should cooperate with business entities, namely, not only supervise compliance with the procedures but also take the role of an "active partner". Business entities do not possess resources for developing effective personalised *KYC utility* tools, to ensure that companies with plenty of customer assessment data would also have the possibility to share them with other businesses.

The head of the FIU supports the idea of setting up such a tool. As to her, for setting up the shared KYC utility, business interests should not prevail, instead, effective combatting of financial crimes should take the primary role. One cannot treat as balanced a solution, where the government imposes significant requirements to the private sector, making it invest millions in the implementation of the compliance function without providing any assistance in effective implementation of that function. The shared KYC utility would be a valuable aid not only for large corporations and authorities combating crime, but also to small businesses in preventing financial crimes.

The Deputy Secretary of State of the Ministry of Justice emphasised the importance of data processing tools. She noted that, notwithstanding that we have put a vital target – to combat economic crimes and achieve business transparency – the achievement of this target will bring along the processing of data of individuals who have nothing to do with these crimes [..]. Due to this we need to address the data minimization principle – to whom it should be applied and how to distinguish between more suspicious or risky clients.

It is beyond doubt that we have to implement a legislative instrument for addressing this issue also because of the General Data Protection Regulation (e.g. exemptions for accessing data, restriction of data processing, data rectification or erasure). Another option for state participation in the shared KYC utility is sharing of information available in public registers. These issues should be governed by the law.

[15] Suggested wording of the amendments to the AML/CFT Law:

"Section 44.[1] Shared KYC utility

(1) In order to undergo comprehensive customer due diligence and transaction monitoring, to verify the accuracy of the data provided by the customer, safeguarding vital public interests to effectively combat money laundering and terrorist financing and in consideration of the threats caused by such unlawful acts to a democratic society and public safety, to achieve the purpose of this law, the obliged entities have the right:

1) to outsource and/or create a private shared KYC utility in order to perform full or a part of customer due diligence without applying the following legal enactments of this Article but respecting the competition law;

2) share and acquire information as a service provided by a company providing the shared KYC utility as a service.

(2) For the objectives set forth in Paragraph 1(2) of this Article obliged entities via the shared KYC utility can process the following information:

1) information that is accessible to general public or can be subject to reuse;

2) information that can be acquired by the obliged entities through the shared KYC utility in accordance with other external regulatory enactments;

3) information from state information systems containing restricted access information, except data relating to criminal convictions and offences and which can be used by the obliged entities in accordance with this and other laws;

4) information that is obtained by the obliged entity in fulfilling the requirements of this Law when performing customer due diligence, including customer identification and concerns legal entities or legal formations and private individuals that are associated with them.

5) information that can be acquired or shared on the client's consent;

6) persons and formations that are identified as subject to international sanctions but are not directly included on the international sanctions lists (sectoral sanctions) and other persons and formations that are used to circumvent international sanctions.

(2) In addition to the forms of application set forth in Paragraph 1 of this Article, the shared KYC utility can be used as hub for information sharing under Article 29, Article 38(4), 41(4) and Article 44 of this Law.

(3) The shared KYC utility is intended for processing information, inter alia, may compare data and discloses the established discrepancies.

(4) The shared KYC utility is entitled to provide its service to obliged entities and other corporates which provide services subjected to licencing and ML/TF risk. In addition, the shared KYC utility is entitled to set specific criteria to which obliged entities and corporates its service is available.

(5) The shared KYC utility is entitled to share the data cross-border according to the terms of its licence and the obliged entity of the other EU member state services or intends to service a client from Latvia. The information supplied to the KYC utility shall not be disclosed or stored outside the EU member state.

(6) For providing information to the shared KYC utility, the obliged entity shall not face legal liability, including third party liability. The KYC utility shall not identify the obliged entity that has provided the information required under Paragraph 2 of this Article.

(7) A company which provides the shared KYC utility services, and which shares information in accordance with Paragraph 2 (3) or 2(4) of this Article among obliged entities which do not belong to the same group of companies or is mentioned in Paragraph 1(1) of this Article, must receive a licence, except for cases when the business entity conforms to the requirements of Article 41(4) of this law.

(8) In case when data of private individuals are involved and their data is processed according to the law without their consent, the data subject may not request rectification or erasure of such data or to restrict data processing. The information provided to the KYC utility shall be deemed non-disclosable other than according to this Article.

(9) The FIU may anytime and without giving any prior notice access the data of the shared KYC utility. The FIU may also use the obtained information for the Cooperation Coordination Group referred in Article 55(2) of this law. Other state institutions shall obtain information from obliged entities in accordance with the statutory procedure and may not request any information directly from the shared KYC utility.

(10) The Cabinet of Ministers shall define:

1) the licencing requirements for the entity which maintains the shared KYC utility, IT solutions, the amount of the licence fee charged by the state, the requirements for staying or withdrawing a licence and set the responsible authority;

2) the terms of use of the shared KYC utility by the obliged entities and/or corporates;

3) the structure of the information that is provided, received or used under the KYC utility and information sharing frequency;

4) the amount of the quarterly state fee that is paid by the business entity which maintains the shared KYC utility, for the acquisition of limited access information from state information systems;

5) the term for keeping and update requirements for the information referred in Paragraph 2 of this Article;

6) machine readable data sharing standards and the procedure for processing individual requests."

The regulation concerns only customers who are legal entities or legal formations and private individuals associated with them (beneficial owners, nominee directors, members of the board, shareholders, nominal directors etc). It would be important to foresee that the data processing is attributable not only to the obliged entities of Latvia, but equally also to EU obliged entities, in case they are customers of the shared KYC utility as they work with customers from Latvia.

[16] Legitimacy of Personal Data Use

The European Court of Human Rights (hereinafter - the ECHR) has concluded that money laundering constitutes a serious threat to democracy.[18]

When addressing the international and EU anti-money laundering laws, the Constitutional Court has recognized that the limitations prescribed by the AML/CFT law generally have a legitimate scope – protection of public safety. To pursue this goal, the state must take measures aimed at controlling capital flows, preventing legalization of proceeds from crime, terrorist and organised crime financing and tax evasion.[19]

Money laundering is also a corruption and organized crime facilitating factor – the easier and more effective it is to implement money laundering schemes, the higher is the corruption and crime level. Considering that money laundering may also have an economic impact on any individual, e.g. raise in inflation, allowing the afore-mentioned groups to undisturbedly legalise proceeds derived from criminal activity, the social consequences may be explicitly adverse for the entire society. Moreover, to accelerate conversion of the proceeds, the offenders are increasingly using globalisation and technological development.[20]

It follows that the public interest in preventing money laundering and terrorist financing is significant. Due to this the available AML/CFT tools must become more effective to maximally reduce the possibility of the offenders to misuse the time resources required for customer due diligence for achieving their criminal targets.

The introduction of the shared KYC utility would limit individuals' rights to the inviolability of private life and the right to property of legal entities, however such a limitation would be proportional.

According to the Constitution of the Republic of Latvia Article 116, the right to inviolability of private life and the right to property may be restricted in cases prescribed by the law, to protect the rights of other persons, the democratic structure of the state, public safety, welfare and morals.

The legitimate aim of data processing under the shared KYC utility would be the protection of the democratic structure of the State, public safety, welfare. The ECHR held that the measures aimed at combatting money laundering and associated crimes without doubt have a legitimate aim that is set out in the second paragraph of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[21] The provisions of this Article correspond to the requirements of Article 96 of the Constitution of Latvia.

In addition thereto, acquisition of information on legal entities could indirectly also affect their right to property under Article 105 of the Constitution. Namely, improved information sharing would allow a number of obliged entities and other business entities to learn previously unknown facts what may result in restricted cooperation with legal entities representing a specific segment.

---

[18] Judgment of the ECHR of 06.12.2012. in the case *Michaud vs France (*Application No. 12323/11) Paragraph 123
[19] The judgment of the Constitutional Court of 28 May 2009 in the case No.2008-47-01, Paragraph 11.
[20] Website of the United Nations Office of Drugs and Crime (UNODC). Available under: https://www.unodc.org/unodc/en/money-laundering/introduction.html?ref=menuside
[21] Judgment of the ECHR of 06.12.2012. in the case Michaud vs France (Application No.12323/11) Paragraph 99.

It could be compared to a situation in which one business entity does not render credit risk related service to a person with a low credit rating.

The introduction of the shared KYC utility will create significant obstacles for money laundering and terrorism financing, specifically by reducing the duration of customer verification procedures as this time resource is currently misused by the offenders for committing illegitimate acts while the identification of risks inherent in them is pending. The KYC utility will allow verification of controversial information and will improve the overall quality of customer verification and more effectively eradicate transactions intended for money laundering or terrorist financing.

The shared KYC utility conditionally consists of four components:

- generally accessible information, the processing of which requires no separate regulation; however, it is mentioned there for the stakeholders not to consider that such a product may not be additionally offered in case of sharing also limited access information;
- limited access information from public registers, however the shared KYC utility does not foresee the right to acquire such information but merely presents a convenient form (channel) for accessing thereto;
- customer due diligence and transaction monitoring information that will be standardised in the law by form/content. This particular component was previously not foreseen and **is subject to the assessment of the restriction of fundamental rights**.

The first component is ensured by companies incorporated in Latvia or abroad which require no licence or are additionally bound by the requirements of the Freedom of Information Law on re-use of information. Whereas the second component is ensured by the provisions of the AML/CFT Law Article 41(4) and other laws, e.g. the requirements of the Law on Duties and Taxes dealing with the provision of tax information.

The rationale for the introduction of the shared KYC utility is not and it cannot be the reduction of costs only. The Constitutional Court has concluded that the simplicity of task administration cannot be the sole substantiation for the restriction of fundamental rights.[22] Therefore the component which entails restriction of fundamental rights, is not meant to provide easy access to certain category of data, but instead deals with new information the sharing of which was previously impossible.

For assessing the proportionality of the restrictions on fundamental rights, the following aspects must be verified:

- are the selected means **appropriate** for attaining the legitimate aim or is it possible to achieve the legitimate aim by the selected means;
- are such measures **necessary** or can the legitimate aim be achieved by means that are less restrictive on the individuals' rights;
- is the limitation **adequate** or are the benefits acquired by the society higher than the harm to the person's interests?

[22] Judgment of the Constitutional Court of 19.10.2017 in the case 2016-14-01 27.2.-27, Paragraph 3. Latvijas Vēstnesis, 2017, No. 209.

When assessing the **appropriateness** of the selected means for achieving the legitimate aim, the Constitutional Court establishes whether the legitimate aim can be achieved by the selected means.[23]

According to the FATF Private Sector Information Sharing Guidance, information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk-based approach and develop innovative techniques to combat ML/TF.[24]

The shortcomings of the information sharing system may cause various issues and make the fight against money laundering ineffective. Likewise, the private sector's role to identify criminal funds in the financial system is often undermined by limited information flow, as regulated entities are prohibited in most countries from sharing financial crime intelligence with one another. As a result, when a bank or another regulated entity decides that the level of suspicion against a client is so high that they opt to exit the customer relationship, the suspect customer may then simply establish a new account with another financial institution. That new financial institution must then start AML investigations from scratch, duplicating effort across the financial system and providing an inadequate safeguard against illicit funds due to delayed reaction.[25]

The suggested wording of Article 44.1 allows simultaneous attainment of several aims. First of all, to exchange information required for the application of the AML/CFT Law by combining the resources of the obliged entities for combating financial crimes. Secondly, it reduces the amount of data to be separately acquired from a person at each obliged entity. This ensures faster reaction and reduces risk of undiscovered suspicious transactions.

The fundamental rights limitation is **necessary,** in case of absence of other equally effective means that would be less restrictive on the persons' fundamental rights.[26]

The suggested wording of Article 44.1 foresees application of an internationally recognized mechanism that is licensed and strictly regulated for sharing data acquired from customer due diligence and transaction monitoring. Moreover, only those data are addressed that are defined in the external regulatory enactment.

There are two hypothetical alternatives for this solution.

First, not to share such information. In such a case the objective is not achieved. Without effective information sharing between the obliged entities the efficiency of the ML/TF risk management is low as a single obliged entity cannot overlook all circumstances effectively and the offender continues his illegitimate acts unnoticed at another obliged entity. ML/TF cases are commonly discovered post factum, however it is important to have a mechanism allowing to prevent such acts and without the shared KYC utility it is impossible.

[23] The judgment of the Constitutional Court of 8 March 2017 in the case No. 2016-07-01, Paragraph 23.
[24] Guidance on private sector information sharing. FATF, Paris, 2017. p. 4.
[25] Maxwell N.J., Artingstall D. The Role of Financial Information – Sharing Partnerships in the Disruption of Crime. Royal United Services Institute for Defence and Security Studies. 2017. p. 4.
[26] The judgment of the Constitutional Court of 13 May 2005 in the case No.2004-18-0106 resolutive part, Item 19.

Secondly, in specific cases permitting information sharing between the obliged entities concerned in case of specific transactions. However, it will also imply a delayed reaction and will leave "weak points" that can be used for committing financial crimes.

Thus, it must be recognized that there are no equally effective solutions for ensuring effective information sharing.

For assessing **compliance** of the fundamental rights limitation with the principle of proportionality, first of all it is necessary to evaluate the consequences caused by the means applied by the legislator, i.e. whether the damage to the rights and legitimate interests of the individual that is caused by the application of the legal norm is not higher than the public benefit. Simultaneously it is necessary to consider the impact of such legal norm on every individual whose interests are affected therewith.[27]

To consider whether the public benefit surpasses the damage caused to the individual by the limitation of the rights foreseen in Article 96 of the Constitution, it is necessary to consider compliance of the limitation with the following basic data protection principles: **legitimacy, fairness, minimality and anonymity**.[28]

It must be taken into consideration that due to impartial considerations in a specific case the **principle of anonymity** cannot be attributed to the regulation of the *KYC utility.*

The principle of legitimacy comprises the requirement that any use or transfer of persona data for other purposes except for the one for which such data were initially obtained, can be effectuated only with the consent of the person or according to the law.[29]

The introduction of the shared KYC utility would be regulated by the AML/CFT law, thus there would be no doubt that the data would be used in accordance with the law.

The **principle of fairness** requires acquisition and processing of data in a manner that would exclude disproportionate interference with the privacy, autonomy and integrity of the data subject.[30] The state may keep only such amount of personal data that corresponds to the legitimate purpose of data processing and requires sufficient means for the protection of rights. The sufficiency thereof depends on the amount of the stored personal data, length of retention and data use and destruction regulations.[31]

The **principle of minimality** foresees that personal data processing is prohibited, unless it is not necessary for significant and previously explicitly determined data processing purposes. Namely, in consideration of the importance of proper data storage, the use of data is admissible only for accomplishing tasks of particular relevance aimed at the protection of some legally important interests.[32] In the context of the principle of minimality it must be clarified if the amount of data intended for processing corresponds to the purpose of data processing. When processing the

[27] Judgment of the Constitutional Court of 19 March 2002 in the case No. 2001-12-01, Paragraph 3.1.
[28] Judgment of the Constitutional Court of 14.03.2011 in the case No.2010-51-01, Paragraph 14, Latvijas Vēstnesis, 2011, No.42.
[29] Ibid.
[30] Ibid.
[31] Judgment of the Constitutional Court of 12.05.2016. in the case No.2015-14-0103, Paragraph 23.3.1, Latvijas Vēstnesis, 2016, No.92.
[32] Judgment of the Constitutional Court of 14.03.2011. in the case No.2010-51-01, Paragraph 14, Latvijas Vēstnesis, 2011, No.42.

respective data, the state must introduce the required measures to reassure that personal data are processed only to the extent truly necessary.[33]

The given principles must be analysed contextually with the General Data Protection Regulation, i.e. with the principles relating to processing of personal data[34] contained in Article 5 of the Regulation.

Above all it is necessary to specify that the suggested wording of the AML/CFT Law Article 44.[1] basically concerns only **legal entities.**

The article is attributable to private individuals only in case such individuals are associated with legal entities or themselves cause increased risk, e.g. politically exposed persons or persons originating from high-risk third countries. The shared KYC utility will be used for processing of such information that is required for customer due diligence and risk identification purposes.

The range of data subjects whose information will be processed is well considered and limited for the shared KYC utility to process minimum required amount of information regarding a limited, predictable and based on specific elements - determinable range of data subjects. No special category of data is processed, except for cases provided for by other laws it they will be providing it in the future.

Equally the shared KYC utility **does not mean that all obliged entities without limitation obtain access to all data contained in public registers**; it is only a channel and does not determine the right to access such information.

The General Data Protection Regulation (hereinafter – the GDPR) *per se* **does not prohibit the introduction of the shared KYC utility in the form offered in the draft, however it requires compliance with a number of detailed requirements for such data processing to be necessary and proportionate.** Prevention of money laundering and terrorist financing is recognised a legitimate aim for data processing and limitation of data subject's rights. It derives from the provisions of the GDPR (Article 19 and 23(1), Article 26(1)) and 27(1) of Personal Data Processing Law, and the suggested wording of Article 44.[1] that the shared KYC utility will be provided and used by **data controllers.**

Personal data can be processed, on the legal grounds that it is a **legal obligation** to which the data controller is subject (according to the Article 6(1)(c) GDPR). Such substantiation can be used only in case the suggested Article 44.[1] obliges the entity maintaining the tool and the obliged entity under the AML/CFT Law to process personal data through the shared KYC utility. However the obliged entities under the AML/CFT Law referred to in Article 44.[1] Paragraph 5 will not be able to use this clause to substantiate personal data processing as they have only the right to perform personal data processing, however in this case those are the **legitimate interests** of the data controller (Article 6(1)(f) GDPR). In such a case the obliged entities under AML/CFT Law must

[33] Judgment of the Constitutional Court of 11.10.2018. in the case No.2017-30-01, Paragraph 18.2.1., Latvijas Vēstnesis, 2018, No.203.
[34] The General Data Processing Regulation Article 5 defines the principles relating to the processing of personal data: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability.

apply the "balancing test" as recommended by the "Article 29 Data Protection Working Group"[35] to weigh the legitimate interests of the controller against the interests or fundamental rights and freedoms of the data subject, which require personal data protection.[36] Therewith the decision-making risk regarding the necessity to perform personal data processing is shifted to the obliged entities under the AML/CFT Law as they will be bound by the obligation to prove that the personal data processing satisfies all requirements of the GDPR.

Special categories of personal data[37] can be processed only if in accordance with the GDPR Article 9(2)(e) such processing relates to personal data which are manifestly made public by the data subject (e.g. it is publicly accessible information on the person's political status) or only in case according to the GDPR Article 9(2)(g), such processing is necessary for reasons of substantial public interest, or according with GDPR Article 9(2)(a) from which it follows that if data subject has provided such data, he/her has given explicit consent to the processing of those personal data.

To process special categories of personal data on the last-mentioned legal ground when the relevant data are not publicly accessible, the entity providing the tool and the obliged entities under the AML/CFT Law will have to prove that no access to the specific data jeopardize **significant public interests**.

The Article 43 of the AML V Directive states that, the processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of **public interest** under Regulation (EU) 2016/679 of the European Parliament and of the Council. At the same time the suggested wording of Article 44.1 itself does not foresee "processing of special categories of data", however in individual cases such information may be clarified for customer due diligence purposes (e.g. belonging to a political party of a politically exposed person, information on the management of a trade union as a customer) or be provided by other law.

What concerns processing of personal data relating to criminal convictions and offences, it must be remembered that the processing of such data must be carried out only under the control of official authority or when the processing is authorised by the applicable laws, providing for appropriate safeguards for the rights and freedoms of data subjects (GDPR Article 10). The suggested wording of Article 44.1 prohibits such data processing.

The tool (utility) is provided by the data controller for the processing of personal data for the purposes foreseen in the draft wording of Article 44.1 and the planned Cabinet of Ministers regulations (i.e. maintenance of personal data within the tool in accordance with the requirements of the applicable laws). Whereas **the user** of the shared KYC utility **is the data controller with regard to the processing of personal data** it will be performed by them to pursue the obligations

[35] Article 29 Data Protection Working Party is an independent European advisory body that addressed the issues on data protection and privacy before 25 May 2018 (effective date of the General Data Protection Regulation)

[36] The opinion of Article 29 Data Protection Working Party of 9 April 2014 No. 06/2014 on the notion of the legitimate interests of data controller, available under: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. This opinion, although it addresses the concept of legitimate interests under the previous regulation (Directive 95/46/EC), nevertheless is topical also contextually with the GDPR.

[37] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

imposed by the AML/CFT Law, inter alia in the area of customer due diligence. It is necessary to set the role of data processing to understand the level of responsibility of the given persons in terms of personal data processing. The data controller is the person that is responsible for the compliance with all personal data protection requirements.

The proposed wording of Article 44.[1] foresees personal data processing objectives and is consistent with the purpose set out in the Constitution, Article 116.

According to the principle of accuracy of personal data that is set out in GDPR Article 5(1)(d), personal data must be accurate and where necessary kept up to date. For this purpose, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The proposed wording of Article 44.[1] does not contain a procedure for keeping the personal data up to date. Nevertheless, the Article contains a reference that the personal data updating requirements will be set by the Cabinet of Ministers.

The afore-listed three issues will be also addressed by the regulations of the Cabinet of Ministers, standardising the shared information that is limited access information, updating and ensuring accuracy thereof. The risk of data being unprecise cannot be fully averted.

The proposed wording of Article 44.[1] (8) does not restrict the right of the data subject to access own data but revokes the right to request to stop processing the data. The GDPR, Article 18 and 23 allows to restrict that right where such a restriction is necessary to safeguard public security, to prevent criminal offences and to safeguard against and prevent threats to public security. The data processed is about individuals associated to legal entities. The data is necessary to mitigate ML/TF risks. If the person was entitled to request to stop processing the data, it would fully jeopardize AML/CTF efforts. Simultaneously, Article 23(2) of the GDPR requires that in the case of limitations of the rights of data subjects, the law setting forth such limitations shall also include the additional information on such limitations. Such information can be included in the AML/CFT Law and / or Cabinet of Ministers regulations.

The ECHR held that in case any private life concerned information is collected and kept in secret registers to combat terrorism, the State has the freedom of imposing various restrictions. For instance in case the disclosure of the information kept in the register to the data subject would jeopardize the purpose of such data processing (e.g. fight against terrorism), the State was entitled to consider that the interests of national security and the fight against terrorism prevailed over the right of the person to the inviolability of private life, namely the rights of the person of being advised of the full extent of the tata collected and stored regarding that person.[38]

The storage limitation principle contained in the GDPR Article 5(1)(e) means that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The proposed wording of Article 44.[1] sets no term for the storage of personal data, however the Article states that the storage limitation will be set by the Cabinet of Ministers. With due regard to the fact that the storage limitation

[38] Judgment of the ECHR of 09.06.2006. in the case *Segerstedt-Wiberg* and others vs Sweden (Application No. 62332/00) Paragraphs 99.-104.

principle is among the basic personal data protection principles, it is necessary to introduce respective data storage limitations to be governed by the Cabinet of Ministers regulations, keeping in mind that the storage limitations may not exceed the term set out in the AML/CFT Law Article 37(2), namely, in case a business entity no longer is a customer of any obliged entity, the data on the associated private individuals must be deleted within the term of five years after termination of the business relationship or a one-off transaction.

The principle of integrity and confidentiality (Article 5(1)(f) GDPR) means that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The proposed wording of Article 44.[1] delegates those issues to the Cabinet of Ministers. The data cannot be transferred or stored outside the EEA. The Cabinet of Ministers will set the minimum requirements for IT safety solutions.

According to the GDPR Article 35(3)(a), the entity providing the tool will have the obligation to perform internal data protection impact assessment as the use of the shared KYC utility will ensure systematic and extensive evaluation of personal aspects relating to private persons which is based on automated processing (including profiling). The GDPR does not prohibit profiling. However, the profiling within the meaning of the proposed wording of Article 44.[1] does not foresee automated decision-making at the level of the shared KYC utility; the procedure for the use of information is set by each obliged entity.