

# **EBA Common Baseline Classification Standard**

## **Data Verification**

**for Corporate-to-Bank KYC in low-risk situations**

Version 1.0  
25 January 2023  
Classification: Public

## 1. Context

Regulated financial institutions are required to perform periodic robust KYC reviews on all their customers. These procedures seek to identify and verify the customer's identity, understand and test the customer's profile, business and account activity, identify relevant adverse information and risk, assess the potential for money laundering and/or terrorist financing to support actionable decisions to mitigate against financial, regulatory and reputational risk and ensure regulatory compliance.

In a pan-European setup, the multitude and the divergences between several sets of requirements foster national and fragmented processes instead of creating an efficient and pan-European procedure for all parties involved, delay the access to finance and other banking products for customers and hamper a future-oriented digitalisation of the KYC process. Legal entities such as corporates as providers of KYC data, and regulated financial institutions as consumers of KYC data, are both faced with a diversity of national, European (and global) procedures, data definitions, guidelines and standards, which is detrimental to fully digitised and harmonised KYC processes. The existing fragmentations prevent legal entity customers from providing one consistent set of data and information to their European banking partners and prevent multinational banking groups from managing AML risks through aligned and efficient EU/EEA-wide AML programs.

The European Commission intends to harmonise and strengthen the current EU AML framework in the proposed Anti-Money Laundering Regulation AMLR.<sup>1</sup> This Regulation will replace previous Anti-Money Laundering Directives and will be directly applicable throughout the EU. Once passed, the AMLR has the potential to significantly reduce national divergences, at least for low-risk customer relationships, and allow for a level playing field across the internal market and a consistent application of provisions throughout the European Union. The EBA fully supports this approach.

However, significant discrepancies between EU countries are likely to remain in relation to the cost and effort required to verify the data-points which are collected from the legal entity customer.

Avoidable barriers to cost-efficient digital processes are mainly the result of a multitude of national registers which, for example, are not aligned in respect to content, might impose language barriers, operate with geographic access restrictions, paywalls and registration requirements, or lack easy digital access to machine-readable data or supporting documents via application programming interfaces (API).

It is the intention of this document to highlight the remaining discrepancies and to propose a harmonised approach to data verification, with the ultimate objective to support the industry's evolution towards customer-centric and regulatory-compliant, cost-efficient, automated digital KYC processes, and to provide a consistent framework or requirements for legal entity

---

<sup>1</sup> REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Brussels 20 July 2021, [https://eur-lex.europa.eu/resource.html?uri=cellar:0a4db7d6-eace-11eb-93a8-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:0a4db7d6-eace-11eb-93a8-01aa75ed71a1.0001.02/DOC_1&format=PDF)

customers who have to provide such data.

## 2. Scope

In February 2022, the Euro Banking Association (EBA) published its “Common Baseline Classification Standard for KYC data for low-risk situations” (EBA CBCS)<sup>2</sup> at the legal-entity-to-bank level in order to support the harmonisation of pan-European KYC processes in low-risk situations. In this context, the common baseline has been defined as those datapoints that, in low-risk standard Customer Due Diligence (CDD) situations, need to be collected from a legal entity customer of a regulated financial institution on a periodic basis. Due to its focus on low risk CDD situations, the CBCS does not cover any additional requirements that a financial institution might have due to the nature of its business with the legal entity customer, or specific information requirements for higher risk enhanced due diligence (EDD) situations.

This document provides additional context from a practitioner’s point of view in relation to the cost and effort required to verify the datapoints which are part of the EBA CBCS, or, once introduced, the data framework included in the AMLR. In particular, it highlights operational deficiencies caused by the lack of a harmonised pan-European approach to identify the ultimate beneficial owner(s) of a legal entity customer, and the current limitations to use national commercial and/or UBO transparency registers to effectively verify and consistently monitor legal entity customer data for changes between periodic review dates. These misalignments and limitations not only increase the cost of regulatory compliance, but also hinder the evolution away from static-date-driven (periodic) KYC towards trigger-event-driven (perpetual) KYC processes.

Feedback provided by the EBA KYC Expert Group (KYCEG) strongly indicates that the most significant areas which require additional pan-European harmonisation relate to primary source data verification via public commercial and UBO transparency registers, UBO determination methodologies and reporting requirements, and the identification and risk-assessment requirements of a politically exposed person (PEP) as an involved party of the legal entity customer.

## 3. Euro Banking Association – Expert Group on KYC related topics (KYCEG)

In February 2021, the EBA created the Expert Group on KYC related-Topics (KYCEG) to define a harmonised pan-European classification standard for KYC data in the field of corporate-to-bank KYC and to agree on a joint interpretation of regulatory KYC requirements at a pan-European level.

The KYCEG is comprised of subject matter experts representing a diverse range of European financial institutions, both in respect to size and region, to ensure balanced representation of the European financial markets and EU countries. The representatives hold senior positions in KYC and/or compliance departments and are typically tasked with the management of KYC

---

<sup>2</sup> EBA CBCS – Common Baseline Classification Standard for Corporate-to-Bank KYC in low-risk situations:  
<https://www.abe-eba.eu/media/azure/production/3276/v2-common-baseline-classification-standard-for-corporate-to-bank-kyc-in-low-risk-situations.pdf>

processes and the execution of KYC due diligence. Due to this background, the KYCEG will only provide practical execution-related advice. Its intention is not to provide EU or national policy recommendations or advocate for the in- or exclusion of particular rules or regulations as proposed, for example, in the AMLR.

## 4. Approach

This analysis covers the legal entity as a customer of a regulated financial institution, with a strong focus on low-risk situations which comprise the majority of customer relationships. However, the majority of findings and recommendations are also applicable to higher or high-risk customers, although different thresholds and/or additional risk management measures may apply which are not covered in this analysis.

In line with the analytical approach used to develop the EBA Common Baseline Classification Standard (CBCS), the KYCEG compared the KYC data verification processes in various countries of operation, both for the legal entity itself, and for the natural persons who are involved as stakeholders in the legal entity customer, with a particular focus on

- Primary source data verification through national business registers, including ease of access, cost of access and digital data availability
- Ultimate Beneficial Owner (UBO) determination and identification methodologies, including the appointment of nominated UBOs (also known as pseudo or substitute UBO), and the current state of UBO transparency registers including ease of access, cost of access, reliability and digital data availability
- The identification of politically exposed persons (PEPs) and their close associates, and the procedural impact of identifying a PEP or close associate as an involved natural person on the CDD process related to a legal entity

The Euro Banking Association and the KYCEG will not make a recommendation for a particular approach or regulation, but stress that definitions, methodologies, and best practices should be consistently applied throughout the EU/EEA to reduce existing and avoid any future pan-European fragmentations.

The comparative analysis performed by the KYCEG identified some key areas in which further harmonisation beyond the scope of existing and proposed regulation could significantly strengthen domestic and pan-European KYC due diligence processes and the ongoing monitoring of customer activity and help to achieve the overarching objective to prevent money laundering and combat the financing of terrorism. At the same time, a harmonised approach to data verification and monitoring could help to reduce the cost of compliance and support the introduction of digital KYC CDD processes for the benefit of both, the financial industry and its legal entity customers.

## 5. Legal Entity Data – Business Registers

The primary source for legal entity data and document verification are reliable trade and commercial registers ('business registers') which are available throughout the EU/EEA.<sup>3</sup> All business registers within the EU/EEA can be accessed online and most are interconnected through one common entry-point.<sup>4</sup>

However, the KYCEG found that business registers provide different depth of data and still show evidence of the lack of a common data sharing policy and a harmonised approach to their content and scope of available information. 'Open-data files' are the exception, and paywalls restrict access to more than just basic (but not harmonised) legal entity information in a number of EU/EEA countries. Language barriers and the lack of consistent definitions further hinder the introduction of efficient pan-European KYC due diligence processes.

In some countries, business registers include a paywall, which means that some information, be it data or documents, is only available against the payment of a fee. The KYCEG is not in a position to comment on fees as such, however, it recommends that all data that is required by law for KYC due diligence or ongoing monitoring purposes should be available before any paywall, which means that legally required data should be free to access on all business registers. This would promote and support the introduction of automated monitoring processes to identify any important changes to customer data on a real-time basis and hence improve the quality of the ongoing CDD process in all obliged institutions.

The KYCEG also pointed out that language barriers still exist as some business registers do not provide an English language service. This lengthens KYC processing time, and hence cost, and increases the risk of misreading the information made available for KYC purposes. Furthermore, the automated processing and cross-referencing of data is hindered through diacritics (the addition of a glyph to a letter to change its sound value) which frequently impact and distort automated database queries.

Finally, the comparison of KYC requirements in various EU/EEA countries found that pan-European misalignments also exist in respect to the acceptable 'age' or 'freshness' of legal entity data and the supporting documentation which is used for the KYC review. Differences not only exist in respect to the acceptable timespan since an evidentiary document was issued (ranging from six weeks to three, six or even 12 months), but also in respect to the reference date which is used to determine the end-date of this period. Here, some regulators define the age of a document as "at time of receipt by the financial institution", whereas others require that data and documents cannot be older than a given timeframe "at the time of the sign-off" (completion) of the review. Time-limits linked to the completion date frequently cause issues, for example when UBO-information has to be obtained from foreign shareholders, whereas shorter 'age-period' restrictions negatively impact banking groups which serve a legal entity customer on a pan-European level as it time-restricts the group-internal 'portability' of the KYC customer file between countries. This also negatively impacts the legal entity customer itself

---

<sup>3</sup> [https://e-justice.europa.eu/106/EN/business\\_registers\\_in\\_eu\\_countries](https://e-justice.europa.eu/106/EN/business_registers_in_eu_countries)

<sup>4</sup> [https://e-justice.europa.eu/489/EN/business\\_registers\\_search\\_for\\_a\\_company\\_in\\_the\\_eu](https://e-justice.europa.eu/489/EN/business_registers_search_for_a_company_in_the_eu)

who cannot use the same ‘KYC information file’ consistently throughout the EU.

## 6. Ultimate Beneficial Ownership – Determination

Beneficial ownership identification and verification is an essential part of KYC onboarding or remediation processes. The beneficial owner (UBO) is the person who ultimately has ownership or control of a legal person.<sup>56</sup>

The KYCEG found significant differences in respect to the determination and identification process regarding the legal entity’s ultimate beneficial owners. Different methodologies, such as the accumulation approach or the domination approach, currently lead to situations where not only the number of natural persons who are identified as UBO differ between countries, but also to scenarios where completely different individuals are identified as the beneficial owner of the customer. Some countries also accumulate shareholdings of ‘close family members’ and deem members of a family together with more than 25% as UBO, even if individual shareholders remain well below this threshold. Additionally, UBO-related personal data collection requirements are not aligned throughout the EU/EEA and add further complexity, including the explicit ID-verification of UBOs which are required by some – but not all – European regulators.

Significant differences also exist in the application and interpretation of nominated UBO guidelines in national regulations or applied best-practices. AMLD4 introduced the notion of a nominated UBO in all cases when, having exhausted all other means of identification, and provided there are no grounds for suspicion, the senior managing official(s) may be considered to be the beneficial owner(s) of the legal entity. The definition who constitutes a senior management official is not aligned, nor is the number of senior management officials who should be taken into consideration when designating a nominated UBO. As a result, in some countries regulatory requirements are met if one senior manager is identified as nominated UBO, whereas other countries require a larger number of individuals, or even the classification of the entire senior management board including the CEO and/or other managing directors as nominated UBO. This leads to significant discrepancies throughout the EU/EEA and, again, makes it very difficult for legal entity customers and internationally active banking groups to introduce harmonised pan-European KYC process policies for their organisation.

The discrepancies related to UBO determination have been recognised and are addressed in the AMLR draft which proposes to identify the ultimate beneficial owner(s) using a threshold of 25% + one of shares or voting rights on every level of ownership (domination approach). As such, the proposed AMLR regulations potentially harmonise major UBO-determination related discrepancies which were identified by the KYCEG, and in principle any such measures are supported by the KYCEG.

---

<sup>5</sup> FATF: Best Practices on Beneficial Ownership for Legal Persons  
<https://www.fatf-gafi.org/publications/methodsandtrends/documents/best-practices-beneficial-ownership-legal-persons.html>

<sup>6</sup> DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 20 May 2015, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&rid=2>



However, the current draft of the AMLR does not seem to provide additional clarity in respect to nominated UBOs and only refers to “senior management official(s)” in Art. 45(3), point b, of the ALMR. The KYCEG recommends that the AMLR revisits this topic and provides clearer and harmonised requirements for nominated UBO which can then be applied consistently throughout the EU/EEA.

## 7. Ultimate Beneficial Ownership – UBO Registers

Introduced in AMLD4 and amended in AMLD5<sup>7</sup>, public national UBO registers for companies and similar legal entities were supposed to be established throughout the EU by January 2020, followed by private registers for trusts and similar arrangements by March 2020. Both directives only prescribe minimum requirements for such registers and allow member states to introduce more extensive registration obligations at a national level. As a result, UBO registers have not been uniformly implemented throughout the EU/EEA.

UBO thresholds vary (25% versus 25% + one share of ownership or voting rights), and some countries have introduced reporting exemptions for companies and their 100% owned subsidiaries if the parent is listed at a regulated stock exchange. Further exemptions might exist for companies under direct or indirect control of public authorities. On the other hand, some countries also include UBOs of non-EU/EEA registered legal entities in their register if any (taxable) activity is performed locally. Further misalignments exist with regard to the initial registration period where deadlines following incorporation range from two weeks via (most common) 30 days up to five months. Typically, changes in its UBO need to be reported by the legal entity within 30 days, but again this differs throughout the EU/EEA.

Beyond the above-mentioned differences regarding thresholds, reporting deadlines and exemptions, the KYCEG found that different methodologies regarding the UBO determination process, access restrictions, paywalls, the lack of digital data, and the current non-reliable status of UBO registers are significantly hindering the efficient use of UBO registers for KYC purposes.

From a pan-European open market perspective, the lack of a common approach to UBO registers becomes even more relevant for cross-border business relationships, e.g., in situations where a financial institution has to follow compliance regulations in its country of registration and hence supervision, whereas its legal entity customer resides in a different jurisdiction and reports UBO information based on its local rules. Overall, the KYCEG reported significant hurdles when attempting to access UBO registers in foreign countries:

- AMLD5 imposed an obligation to EU member states to completely open the access to UBO registers to the public. However, the EU’s intention to open such registers to the public potentially conflicts with privacy concerns in some member states which, as a consequence, require registration of the individual data-consumer before certain

---

<sup>7</sup> Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, with EEA relevance

information can be accessed. Today, various access hurdles or restrictions exist in a number of countries, ranging from registration and/or identification requirements to the limitation of access to nationals or EU citizens only. In some cases, registration is only possible for individuals but not businesses, or the submission of forms is required to justify the UBO information access request. Subsequently, KYCEG members reported significant problems, or the inability, to access UBO registers in other member states, thus defying their intended purpose as a tool for investigation and pan-European KYC due diligence.

- Paywalls have been introduced by a number of UBO registers, and whilst the KYCEG accepts that paywalls are permissible, payment at some registers can only be processed through the use of (personal) credit cards which is highly inefficient for financial institutions which require access to UBO data on an ongoing basis. Paywalls related to the repeated access for legally required data also conflict with the industry's desire to monitor UBO data for changes on an ongoing basis.
- Even if UBO registers can be accessed by institutions based in a foreign country, KYCEG members reported further difficulties due to language barriers as not all UBO registers offer English language services. Google translate can be used reasonably well in some situations; however, this is not deemed to be an acceptable approach from a risk, liability and efficiency perspective, and again prevents the introduction of automated processes. And as only a very limited number of registers offer digital data, language barriers can currently not be overcome through the use of API.
- The personal data of the direct beneficial owner typically includes, at a minimum, name, place of residence, year and month of birth and citizenship, however, this is not harmonised throughout the EU/EEA. In case of indirect ownership situations, complete ownership structures are rarely provided, forcing the obliged institution to perform a number of searches to obtain full transparency about the ownership structure of the legal entity customer, adding time and cost to the due diligence process. Furthermore, some UBO registers do not provide detailed information about the nature or extent of ownership.
- Beyond the technical hurdles mentioned above, the KYCEG found that national differences in the UBO determination process (e.g., accumulation approach versus domination approach) lead to situations where a natural person qualifies as UBO in one particular member state (the state which regulates the financial institution), whereas the same person is not deemed to be UBO in another member state which applies a different methodology (the state in which the legal entity customer is registered). In such cases, the UBO information held in the UBO register is not useful for the bank which serves the customer, again limiting the use of UBO registers for pan-European KYC due diligence purposes.
- To date, UBO registers are not reliable. On the contrary, the majority of national regulations stipulate that obliged institutions must consult the national UBO register when performing KYC due diligence and report any identified discrepancies between



information about a client's UBO that they have on file and the information set out in the UBO register extract back to the register in a timely manner.

In summary, KYCEG member institutions found that the absence of accessible and reliable UBO registers is the most relevant obstacle in their drive towards automated and efficient KYC processes. In domestic situations, they are unreliable and often incur direct cost due to paywalls, and indirect cost due to registration management and discrepancy reporting requirements. In cross-border KYC situations, they frequently lack accessibility, incur additional cost, and often contain data which is not aligned with the local regulatory requirements of the data consumer.

## 8. KYCEG Recommendations

In order to effectively manage AML risks and combat the financing of terrorism, obliged financial institutions must be able to identify risks in a consistent and timely manner. Cost related to KYC data collection and verification, which are ultimately borne by the customer, have to be minimised, and particularly so for low-risk scenarios. To achieve this, financial institutions must be able to automate certain elements of the KYC due diligence process and focus the employment of human experts on higher or high-risk due diligence situations which require deeper scrutiny and manual risk assessment. This can only be achieved if automated KYC data verification and monitoring processes can be employed consistently, both for domestic and for pan-European customer relationships.

In order to support the evolution towards reliable trigger event driven perpetual KYC processes, the KYCEG concludes that a number of adaptations are required at national levels, both in terms of national regulation and regarding the ease of access to national registers. The proposed alignments aim to enhance the quality of the KYC process in low-risk scenarios, increase the speed of onboarding new customers and thus increase pan-European competition, and improve the ongoing monitoring of customer data for adverse changes.

To achieve this, the KYCEG recommends:

1. Validity of data and documents: The KYCEG proposes a pan-European alignment in respect to the 'age' or 'freshness' of supporting documents and similar data which are provided by the legal entity customer for KYC onboarding and review purposes. This alignment has to include a clear definition of the 'end-date' of the period, ideally as "not older than [x] months at time of receipt by the bank", rather than "not older than [x] months at time of sign-off and completion of the review" to avoid the need to refresh data or documents during the ongoing KYC review process. A harmonised definition of age-limits will provide legal entity customers with certainty what to provide or update when they submit information to their banking partners and support the introduction and efficient management of KYC processes for institutions which serve a legal entity customer in a number of European countries. However, this requirement could be partly mitigated by free electronic access to data and documents held at continuously reliable business and UBO registers.

2. Reliability: All national primary sources, e.g., business registers and UBO registers, should be obliged to maintain current and accurate information so that financial institutions as data consumers can rely on its information at all times. The obligation to provide correct and accurate data to the respective register in a timely manner should be with the legal entity, and the obligation to reliably transpose corporate documentation data into digital data should rest with the register.
3. Definitions: All definitions and methodologies should be aligned at a pan-European level according to the entity's legal category. This includes definitions about who constitutes a senior management official, or who (and how many) of such senior managers qualify as nominated UBO. The information held in UBO registers should be aligned and include the entire ownership hierarchy of the legal entity and a consistent indication related to percentage of ownership, voting rights or control through other means. The objective of this requirement is to ensure that the UBO information captured in a national register is sufficient to fulfil regulatory requirements in all member states of the EU and EEA.
4. Discrepancy reporting: The approach to discrepancy reporting for UBO registers should be aligned with the reporting process applied to business registers. The current process, which puts the obligation to report incorrect data onto obliged financial institutions, adds to the complexity of the KYC due diligence process, incurs additional cost and thus hinders, rather than promotes, the evolution towards real-time trigger event driven KYC processes.
5. Access restrictions: The KYCEG recommends the introduction of a harmonised EU-wide access mechanism for obliged entities and their employees which would enable financial institutions to access any register, ideally through an interconnected portal, without any additional registration requirements at national level.
6. Paywalls: Paywalls should not restrict the continuous access to legal entity data or UBO information which is required by an obliged financial institution to fulfil its regulatory verification and/or monitoring obligations. CBCS legal entity data or, once passed into law, ALMR required legal entity data should be available for free or charged for based on a 'unlimited access' subscription model in all business registers. This would resolve any potential conflict between the desire to constantly monitor data for changes, thus enhancing the effectiveness of AML/CFT controls, and immediate direct cost which would otherwise incur for such repeated consultations.
7. Technology: All public primary sources should be set up consistently in terms of technology and should be accessible via standardised API. Digital data (not just documents) should be available and structured in a comparable manner to overcome language barriers and promote the introduction of automated verification processes. All data which includes special characters (e.g., diacritics) should be made available in its English language equivalent and/or a Unicode standard to support automation and cross-referencing. This suggestion is aligned and supports the intention of the EU to

interconnect all national commercial and UBO registers through a single-access portal<sup>8</sup> and would improve the current EU offering. This recommendation is in line with the EU Open Data Directive.<sup>9</sup>

8. **Monitoring:** Open-source data-files are offered by a small number of registers and enable a financial institution (or any other data consumer) to download the entire content of the respective register in one machine-readable digital file. The automated (and often AI enhanced) comparison of historic files with current files then enables the identification of gaps or changes in the data, which has proven to significantly enhance the efficient ongoing monitoring of customer data for adverse changes. Beyond their capability to enable event driven perpetual KYC processes, open source data files also prevent data leakages and address privacy concerns as they protect the confidentiality of corporate-to-bank customer relationships. Due to these advantages, the KYCEG strongly promotes the introduction of open source data files at all registers in addition to any existing API interfaces.

## 9. Politically Exposed Persons (PEP)

The KYCEG compared national regulations and best practices to determine if KYC processes could benefit from further harmonisation related to Politically Exposed Persons (PEP), their family member(s) and/or close associates. The comparison focused on the definition of a PEP (and their family / close associates), and the impact on the due diligence process an obliged institution has to follow if a PEP is identified as a stakeholder in a legal entity customer.

The KYCEG found that the current approach, which is based on the identification of a PEP via roles (i.e., important party officials or “high ranking” officers) and titles (i.e., heads of state, heads of government) does not provide sufficient guidance to identify such positions of influence uniformly and with certainty across jurisdictions where there are differences in titles and political systems. Furthermore, add-on regulations at national level in some member states have added complexity through the introduction of more extensive, but not harmonised, functional lists. As a result, it frequently happens that an individual with a certain role or function is treated as a PEP in one member state, whereas the same individual can engage in banking activity in a different member state and not trigger PEP-related higher risk due diligence measures. From a pan-European point of view, this enables PEPs to avoid scrutiny, creates loopholes which can be exploited if bad intentions exist, and as such contradict the intention of PEP-related regulation.

The definition of ‘family members’ is also not harmonised, and some member states include siblings of the PEP, thus going beyond the Financial Action Task Force (FATF) recommendations. This is yet another example where different definitions create fragmentation

---

<sup>8</sup> [https://e-justice.europa.eu/489/EN/business\\_registers\\_search\\_for\\_a\\_company\\_in\\_the\\_eu](https://e-justice.europa.eu/489/EN/business_registers_search_for_a_company_in_the_eu)

<sup>9</sup> Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024>

within the EU/EEA, which can be exploited if bad intentions exist by simply moving certain account activities into a different EU/EEA country.

If a PEP has been identified as a stakeholder of the legal entity customer, financial institutions have to apply additional risk measures. These include, uniformly, senior management approval before entering into a relationship with the respective customer, the collection of additional personal data of the PEP including the identification of source of funds and source of wealth, and enhanced screening and monitoring requirements. However, the KYCEG found that the requirements related to enhanced screening and monitoring are not harmonised within the EU, the major difference being the risk classification, which is applied in such cases, ranging from “higher risk” in some countries to a mandatory (and more expensive) “high risk” in others.

Finally, once a PEP leaves the PEP function or loses the PEP role, AMLD5 stipulates that PEP risk-measures have to continue for at least 12 months, or until such time as that person is deemed to pose no further risk specific to PEPs, after which the re-classification of the legal entity customer from an ALM risk perspective is potentially permitted. However, this risk-based approach has not been consistently adopted in all local regulations, leading to situations where the restrictive view of “once a PEP always a PEP” is still applied in some countries.

Overall, the KYCEG found that the current regulations related to PEPs are not consistent, provide loopholes in certain situations, and cause significant problems for institutions which operate throughout the EU as no single harmonised policy or procedure can be applied for customer relationships which involve a PEP (or their family / close associates) as stakeholder.

The KYCEG feels that a more detailed analysis of this topic is required before the KYCEG feels comfortable to suggest alternatives to current regulation and/or best practices and subsequently propose a suitable approach to harmonisation in this area.