Good Practices PEP Wwft BES

1 July 2025

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

2 International context

3 AML regulations: general framework

4 Good practices regarding sources to be used to determine PEP status

5 Red flags with respect to PEPs

6 Good practice: PEP measures

7 Good practice: independent testing

1 Introduction

The laws and regulations of the countries in the Kingdom of the Netherlands include provisions that service providers must comply with in their operational management to counter money laundering and terrorist financing through the services they provide (AML regulations). To assist service providers in complying with these requirements, this Good Practices document has been drafted. However, service providers are at all times fully responsible themselves for compliance with relevant statutory provisions. While this document uses terms that are defined in more detail in the laws and regulations of the countries in the Kingdom of the Netherlands, terms that differ from these definitions or any other provisions may also be used. In case of doubt, the legal texts prevail.

"Politically exposed persons" (PEPs) occupy a special position in AML regulations. A PEP is a person who holds or has held a prominent or high-ranking public position. Thus, the PEP concept is not only limited to politicians, but also covers, for example, individuals who hold prominent positions with an international organization. Because of the potential corruption risks associated with PEPs, international standards and rules and regulations require institutions to pay special attention to these individuals.

In the area of integrity supervision, Kingdom supervisors collaborate in the Working Group on Harmonisation of Integrity Supervision.[1] With this Good Practice document, the Kingdom supervisors aim to provide supervised institutions in Aruba, the BES islands, Curaçao and Sint Maarten with a common guideline for dealing with PEPs, taking into account the differences in laws and regulations.[2]

In addition, with this Good Practice document the supervisors aim to encourage service providers to take its contents into account in their considerations, as well as their own circumstances, without them being obliged to do so. This Good Practice provides insight into the policy practices observed or expected by supervisors. It is only indicative in nature and therefore does not rule out that some service providers must apply the underlying regulations differently, and possibly more strictly. Any considerations regarding the application rest with these service providers, who themselves remain fully responsible for compliance with laws and regulations.

1 The Kingdom supervisors are the partners referred to in the 2013 Memorandum of Understanding between the central banks in the Kingdom of the Netherlands and the Financial Markets Authority. They include the Financial Markets Authority (AFM), the Central Bank of Aruba (CBA), the Central Bank of Curaçao and Sint Maarten (CBCS) and De Nederlandsche Bank (DNB).
2 A complicating factor here is that there are differences between the AML regulations of Aruba, the BES islands, Curaçao and Sint Maarten, including with regard to PEPs. The Kingdom supervisors are currently exploring options for harmonisation with regards to this issue.

2 International context

The PEP regulations stem from the recommendations of the Financial Action Task Force (FATF).[3]

FATF Recommendation 12 - Politically exposed persons

Financial institutions should be required, in relation to foreign politically exposed persons (PEP's) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
b. obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
c. take reasonable measures to establish the source of wealth and source of funds; and
d. conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEP's.

The term PEP is closely related to corruption:

- In 2011, the FATF stressed that PEPs carry a high money laundering risk: because of their position, their access to large public funds, their control over public companies and contracts, and because of the opportunities they have "simply to create structures to siphon money from government coffers."[4]
- According to the FATF, money laundering is essential to corruption: "the stolen assets of a corrupt public official are useless unless they are placed, layered, and integrated into the global financial network in a manner that does not raise suspicion."[5]
- In 2001, the Basel Committee pointed out PEPs' corruption risks, stating: "There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her. Banks should gather sufficient information from a new customer (...) in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level."[6]

3 The FATF is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. The FATF recommendations are recognised as the global standard in countering money laundering and terrorist financing.
4 FATF, *FATF Report. Laundering the Proceeds of Corruption*, 2011, p. 9.
5 FATF, *FATF Report. Laundering the Proceeds of Corruption*, 2011, p. 6.
6 Basel Committee on Banking Supervision, *Customer due diligence for banks*, 2001, p. 11.

It's not about the PEPs - it's about risks

So, PEPs fundamentally represent a higher risk. Merely focusing on PEPs is insufficient; specific attention must be focused on the risks. In 2012, the FATF stated: "combating corruption-related money laundering must be more than simply ensuring that PEPs receive an appropriate level of scrutiny. Rather, an effective AML scheme requires an assessment of corruption-related risk (...), regardless of whether a FATF-defined PEP is involved."[7] In other words: the definition is not the starting point, but the risk - and in that case an official of an international football organization may be considered more at risk than a local politician. And in 2013, the FATF stated: "When considering whether to establish or continue a business relationship with a PEP, the focus should be on the level of ML/TF risk associated with the particular PEP, and whether the financial institution or DNFBP has adequate controls in place to mitigate that ML/TF risk (...)."[8]

7 FATF, *Specific Risk Factors in Laundering the Proceeds of Corruption. Assistance to Reporting Institutions*, 2012, p. 4.
8 FATF, *FATF Guidance. Polically Exposed Persons (Recommendations 12 and 22)*, 2013, p. 7.

3 AML regulations: general framework

Although there are differences between the AML regulations of Aruba, the BES islands, Curaçao and Sint Maarten, the main elements with regard to dealing with PEPs in these regulations are based on the relevant FATF standards. In the relevant AML regulations, a PEP is defined as a person who holds or has held a prominent or high-ranking public position. PEPs also include immediate family members or close associates of that person ("connected persons").

In addition, the following points apply generally:

- When entering into a business relationship or prior to executing an occasional transaction, service providers will check whether the customer, or the customer's ultimate beneficial owner (UBO), is a PEP. This check is repeated periodically, as well as in the event of alerts or changes.
- Service provision to PEPs requires additional measures, as it entails higher integrity and reputational risks. In particular, these measures concern:
  - Any decision to enter into a business relationship or execute an occasional transaction is to be taken or approved by senior management or individuals authorised to do so.
  - Adequate measures are in place to determine the source of wealth and the source of funds.
  - The service provider must monitor the business relationship on an ongoing basis.

Service providers can design their internal procedures in a risk-based manner, including with regard to PEPs.

4 Good practices regarding sources to be used to determine PEP status

There are several methods to determine the status of a PEP, including:

- Service providers use available PEP lists (see below, 'The use of PEP lists').
- In addition to using general PEP lists, service providers also use their own "local" PEP lists, running a check on names of local individuals in prominent positions.
- In the event of signals, service providers conduct research online, for example into the level of corruption in the customer's country of origin.
- To gather sufficient information to identify PEPs during the CDD process, and to find out if there are any connected persons involved, services providers use a targeted questionnaire.

Merely running a check against a PEP list does not suffice in every situation. It is a good practice for service providers to be aware that PEPs may hide behind another person (concealment or front-man risk). In case of a complex structure, the service provider will make additional efforts to understand this structure and identify the UBO. In doing so, service providers focus not only on "ownership" but also on "control".

A person holding any of the following prominent positions qualifies as a PEP in principle:

- head of state, head of government, minister, state secretary
- member of parliament (or a similar legislative body)
- party leader or member of any governing body of a political party
- member of a supreme court, constitutional court or other high court that issues rulings against which no further appeal is possible
- member of a court of auditors or of a central bank's board of directors
- ambassador or chargé d'affaires
- senior officer of the armed forces
- member of an administrative, management or supervisory body of a state-owned enterprise
- director, deputy director, associate director or member of the board or a similar position with an international organisation (e.g. (WHO, UNODC, IMF, IAEA, OPEC).

No public position referred to in the points above includes persons at middle or lower management levels.

Immediate family members and close associates of persons who are or were entrusted with the aforementioned prominent positions are also considered PEPs.

- Immediate family members are:
  - a PEP's spouse or a person considered equivalent to a PEP's spouse
  - a PEP's child, that child's spouse or a person considered equivalent to that child's spouse
  - a PEP's parent.
- Close associates include:
  - any natural person known to have joint ownership of a legal entity or legal arrangement, or any other close business relationship, with a PEP
  - any natural person who is the sole ultimate beneficial owner of a legal entity or legal arrangement known to have been set up for the benefit of a PEP.

The above (non-exhaustive) list should be considered as an aid. For the official lists, please refer to the AML regulations of each country.

The use of PEP lists

Some service providers hire an external service to assist them in PEP screening. This may involve, for example, outsourcing the screening to a third party or using commercial software for screening by the service provider itself. It is a good practice for a service provider using an external list provider to maintain its own, local PEP list in case the external list is insufficient. An in-house PEP list enables service providers to take into account local positions and individuals who qualify as PEPs but are not included in international lists.

It is a good practice that service providers periodically check whether all relevant lists are being used and are up to date. It is also a good practice that updates to the PEP lists used are made at least annually. It is furthermore a good practice that service providers also update their local PEP list after events such as elections or a change of board members.

Using an external service may improve PEP checks and the recording thereof, for example because a third party can perform the check more efficiently or more thoroughly. Of course, the rule here is that in the case of outsourcing, the service provider itself remains responsible – in this case also for the PEP check. It is important to make proper arrangements in this regard with the party to which work is being outsourced. It is a good practice to evaluate the outsourcing systematically to determine whether it is actually working as intended and whether it meets the legal requirements. It can therefore be useful to periodically test processes, systems and lists et cetera in practice.

A PEP check performed through a system can often be combined effectively with sanctions screening or the retrieval of adverse media coverage on a customer.

5 Red flags with respect to PEPs

In principle, a PEP carries a higher risk of involvement in corruption and money laundering. In any case, the risk is further increased when the following situations occur:

- The PEP is from a jurisdiction with a higher risk of money laundering and/or corruption, or from an EU- or UN-sanctioned country.
- There is negative news about the PEP (this includes case law).
- The customer/UBO refuses to provide relevant information or is unclear about the source of wealth and the source of funds.
- Available information on the customer (occupation, age, income) does not match the information on the source of wealth and the source of funds.
- The customer/UBO provides documents on the source of wealth and the source of funds that are inconsistent with those provided by comparable customers.
- The customer/UBO provides documents on the source of wealth and the source of funds originating from high-risk jurisdictions.
- The customer/UBO provides documents on the source of wealth and the source of funds that are inadequate or apparently forged or lack a rationale.
- The customer/UBO provides information on the source of wealth and the source of funds through complex, opaque structures (e.g. offshore structures, trusts, bank accounts in high-risk countries), and the information remains unclear.

It is a good practice for service providers to take additional control measures in these situations. Examples would be asking additional questions, setting limits on transaction amounts and explicitly pre-assessing transactions the PEP wishes to execute. In such cases, the service provider must also consider whether the risk is still acceptable. If not, the service provider should refuse, terminate or limit its services.

6 Good practice: PEP measures

Enhanced customer due diligence

Where there is a PEP, and a higher risk of involvement in money laundering or terrorist financing, the service provider should take additional measures. Enhanced customer due diligence includes at least an investigation into the source of wealth and the source of funds. The service provider will tailor the intensity of this investigation to the risk.[9]

In practice, the measures taken by service providers include:

- Service providers identify the sources of funds and wealth using multiple sources of information, such as:
  - publicly available information
  - information from the customer, combined with documentary evidence
  - financial data of a related foundation.
- Because of the potential burden on the customer and on the employee, it is a good practice for the service provider to consider how the enhanced customer due diligence can be organised, for example with regard to the style of communication, so as to reduce resistance from an employee or resistance from a customer to disclose fully.
- Through trigger-based or periodic reviews, the service provider determines whether the assigned risk profile is still appropriate and whether the risk is still acceptable.
- When carrying out these reviews, the service provider also considers the transactions carried out, including the identification of potential unusual transactions, taking into account the established transaction profile.
- The service provider tests the models and/or business rules used in transaction monitoring periodically to determine whether the transaction monitoring system adequately detects unusual transactions by PEPs and by foundations related to PEPs and/or political parties.

Senior executives taking responsibility

Any decision to enter into a relationship with, or execute an occasional transaction for, a PEP must be taken by senior management or by individuals authorised to do so. In the latter case, the following elements are important:

- Clarity regarding risk-based scenarios in which approval is delegated by senior management and regarding scenarios that must be submitted to senior management for deciding.
- Requirements regarding officers with decision-making power:
  - they must have sufficient knowledge of ML/TF risks
  - they must be at the right decision-making level
  - they must be sufficiently informed about the risks regarding PEPs.
- Accountability to senior management and reporting on exposure with regard to PEPs.
- Recording and audit trail.

9 It may be useful to be aware of the level of corruption in the country where the person holds the position. In practice, institutions often use Transparency International's Corruption Perception Index for this purpose.

It is a good practice that the role of senior management goes beyond approving a relationship or occasional transaction. Senior management has the responsibility to deal with PEPs appropriately, for example by applying the following points:

- Compliance has at least an advisory role when a customer involves a PEP. Compliance has the resources and is in the position to operate independently in these matters.
- Staff in charge of identifying PEPs, handling alerts from the screening and monitoring system or conducting enhanced customer due diligence receive high-quality training and instructions, as does the team conducting reviews. Senior management ensures that staff members have the appropriate knowledge and expertise as well as a sound level of critical thinking and working.
- More generally, management actively maintains a culture that encourages collaboration to achieve the goals of AML/CFT regulations.

7 Good practice: independent testing

Service providers ensure independent and systematic testing of compliance with PEP regulations. The following points could be taken into account here:

- It is a good practice for internal supervision, such as the compliance function, to conduct checks on the operation and effectiveness of procedures for identifying PEPs.
- It is a good practice for service providers to test their transaction monitoring systems to ensure their proper functioning, with regard to both generating alerts and handling them.
- Compliance periodically tests whether policies, procedures and measures are applied correctly and to this end also performs checks in e.g. transaction systems and customer files.
- The internal audit function has the appropriate AML/CFT knowledge and expertise to adequately determine proper compliance with AML/CFT regulations and puts these to use.
- The service provider periodically reviews whether Compliance's capacity and resources are sufficient, and whether Compliance's position is sufficiently independent in practice.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:
Instagram
LinkedIn
X

DeNederlandscheBank
EUROSYSTEEM