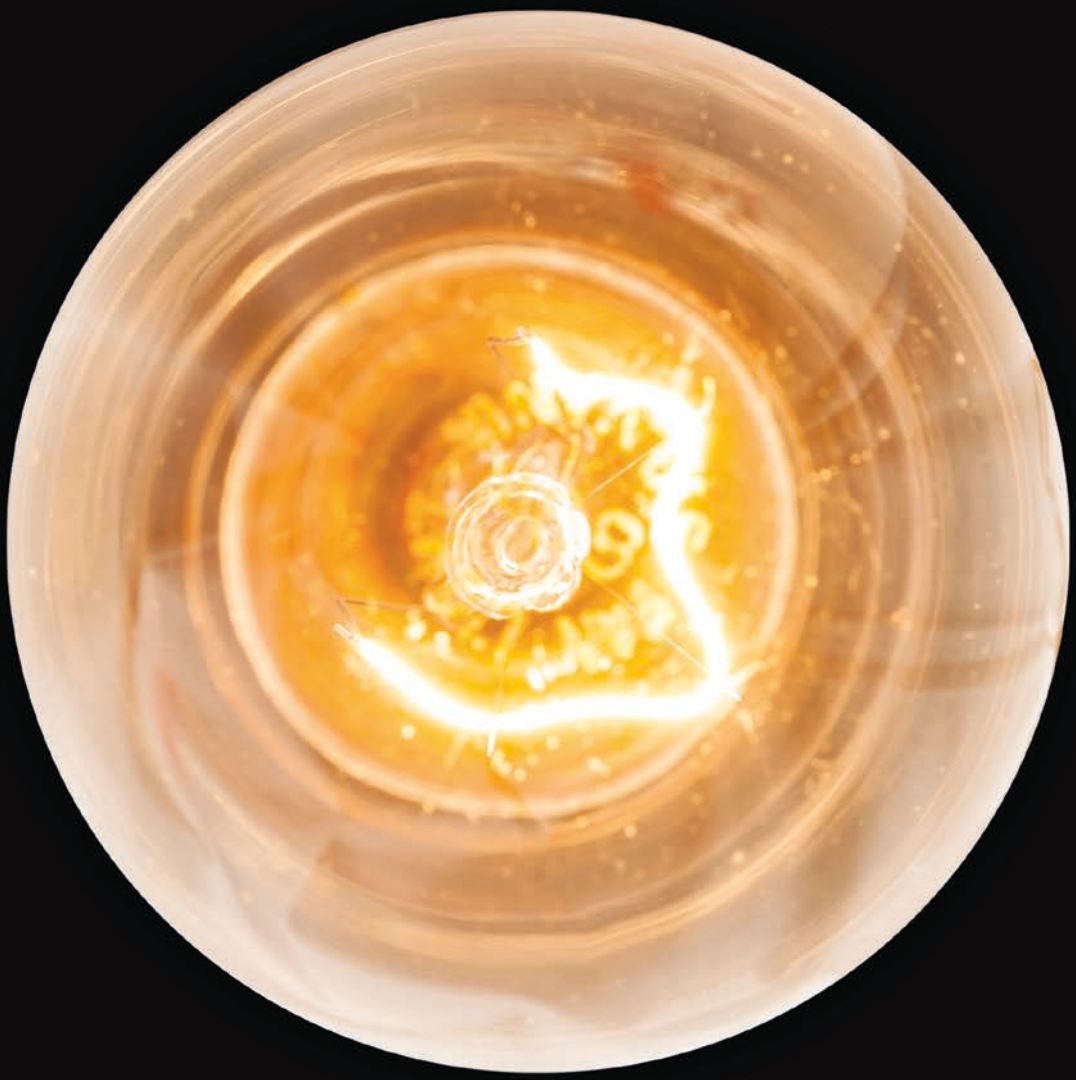
Deloitte.



PEPs in the age of GDPR

Regulatory change, risks and key considerations for Financial Institutions

Contents

Introduction

It is now over a decade since Politically Exposed Persons ("PEPs") were singled out as a unique category of customer in the 3rd Money Laundering Directive. Since that time, Financial Institutions ("FIs") have been at pains to both identify PEPs in their customer base, be they prospective or current customers, and to apply proportionate risk-based measures once a PEP has been identified. Following the changes brought about by the Money Laundering Regulations ("MLR17" or "Regulations") last year, whereby domestic holders of public positions qualifying for PEP status are now also to be categorised as PEPs, the issue of identification, categorisation and application of proportionate risk-based measures has once again come to the fore.

Our approach

This paper will explore the issues outlined above in the context of a host of recent regulatory change and industry guidance, examining the implications of the General Data Protection Regulation ("GDPR"), the Bank of England and Financial Services Act ("the Act") and MLR17 on the treatment of PEPs. In an age of GDPR, this paper seeks to present a unique holistic viewpoint, examining the treatment of PEPs from both an AML/CFT standpoint as well as through a data protection lens, along the way demonstrating their interconnected nature. To contextualise this, we will use the Information Commissioners Office ("ICO") response to MLR17 as our starting point, exploring how this response touches upon several salient themes, including de-risking, PEP acceptance, classification and declassification.

Once we have explored these themes we will lay out the main areas for consideration and provide suggestions on the next steps that FIs can pursue.

Why should this concern us?

Failing to give adequate consideration to these issues has a number of serious consequences for FIs including:

- Reputational damage as a result of being subject to a fine or other punitive measure(s) by a regulatory authority. FIs are at risk in this regard from multiple bodies, including the Financial Conduct Authority ("FCA"), Financial Ombudsman Service ("FOS") and the ICO, all of which have robust enforcement powers at their disposal. Firms also risk losing their clients' trust if they are seen to be subject to measures such as these;
- Disrupted customer experience and consequent decline in customer satisfaction in a competitive marketplace; and
- Increased regulatory oversight and scrutiny, bringing compliance and operational shortcomings into sharp focus.

In an age of GDPR, this paper seeks to present a unique holistic viewpoint, examining the treatment of PEPs from both an AML/CFT standpoint as well as through a data protection lens, along the way demonstrating their interconnected nature.

Key considerations summary

Our key considerations for FIs are summarised in the table below and will be based around the following overarching themes:

Theme	Key considerations
PEP acceptance and declassification	Ensure that the senior manager responsible for making the decision on whether to accept or continue a PEP relationship is of sufficient seniority to accept the risk. Firms should take note of the FCA PEP guidance in this regard, as it states that the senior manager responsible for the approval of PEP relationships should, *'as a minimum'*, be the person holding the Money Laundering Reporting Officer ("MLRO") role. For higher risk relationships, the guidance indicates that board of director level is the baseline[1].
	Firms must also ensure that this logic extends to the individual responsible for making the decision to cease enhanced measures on the family members or known close associates of a PEP, once the PEP in question has stepped down from their public function.
	Firms which apply a "PEP for life" blanket approach should consider if this is truly commensurate with a risk-based approach and whether it would stand up to regulatory scrutiny.
	When rejecting new PEP customers, firms should ensure that their decision is reflective of a properly functioning risk based approach. Without this documented, firms run the risk of falling foul of the compensation measures laid out in the Act.
Newly categorised (domestic) PEP customers	Firms should ensure that they adhere to the provisions of the first data protection principle when categorising existing customers as PEPs for the first time. To this end, firms should consider updating the privacy notices given to customers who are now encapsulated under the enhanced CDD requirements.
Data accuracy and relevance	Pay careful consideration to the provisions of GDPR with regard to the accuracy of customers' personal data in order to ensure that the potential for false attribution when screening customers, and hence their recourse to rectification, is diminished. To remedy this, firms should consider the potential limitations of any screening tools acquired from third party vendors.

1. FCA – The treatment of politically exposed persons for anti-money laundering purposes (2017)

ICO response to MLR17

The serious nature of the data protection implications of MLR17 were highlighted when the ICO felt compelled to issue a response to what was then a consultation on the draft Regulations.

The main focus of the response was the sudden upsurge in the number of customers who would be classified as PEPs without even being aware of their new classification and the consequent enhanced measures which FIs would apply to them. These individuals include the aforementioned domestic holders of PEP positions, their family members and known close associates, and the new mandatory category of PEPs (the members of the governing bodies of political parties, and directors, deputy directors and members of the board or equivalent function of an international organisation). Bringing these individuals within the scope of EDD for the first time means that FIs must give due consideration to the first data protection principle which states that personal data shall be *'processed lawfully, fairly and in a transparent manner in relation to the data subject'*. The importance of adhering to this principle is made clear by the fact that *'personal data'* has a broad definition, encompassing data which simply relates *'to a living individual'*. FIs acting in their capacity as data controllers (an organisation determining how personal data is held and processed) must therefore be cognisant of the numerous provisions attached to the first data protection principle.

These include ensuring that the data controller[2]:

- has legitimate grounds for collecting and using personal data;
- does not use personal data in ways that have unjustified adverse effects on the individuals to whom the data relates;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways those individuals would reasonably expect; and
- make sure they do not do anything unlawful with the data.

Re-categorising existing customers as PEPs and consequently obtaining additional information that the customer was not previously required to provide (e.g. obtaining information on the customer's source of wealth) will present new challenges to FIs. For example, FIs may need to consider updating the privacy notices of customers when they become classified as PEPs for the first time. Being both transparent and having *'legitimate grounds for collecting and using personal data'* go hand in hand when FIs collect the additional information (some mandatory and some not) as part of applying EDD. Indeed, obtaining extra information on a customer which is not required by law or regulation will warrant a more considered explanation when informing their customers about how they intend to process their data. This is especially pertinent with PEPs considering that the level of information that they are required to provide can often be considered excessive and invasive, a problem that is not unique to dealing with domestic PEPs as it has long been documented how certain overseas cultures view the request for personal information as an affront to their privacy rights.

Next steps:

- When managing the migration of domestic PEPs to EDD status, FIs will have to take into account the incoming changes of the GDPR which places an increased emphasis on making privacy notices both understandable and accessible.
- Firms should consider updating the privacy notices given to customers who are now encapsulated under the enhanced (PEP) CDD requirements for the first time. Such a notice should reflect the requirement for additional personal information.
- Under GDPR, privacy notices will now also need to specify the time period, or the criteria used to determine the time period, for holding personal data. A statement that any personal data received from the customer will be processed only for the purposes of preventing money laundering or terrorist financing will also need to be included as per MLR17.
- Ensure that any reclassification is handled in accordance with the ICO guidance on the first data protection principle.

2. ICO – The Information Commissioner's Office (ICO) response to HM Treasury's consultation on the Money Laundering Regulations 2017 ("the consultation") (2017)

Accuracy of personal data

When processing their customers' personal data it is incumbent on FIs to adhere to the fourth data protection principle, namely, ensuring that the personal data they hold is *'accurate and, where necessary, kept up to date'*.

This obligation is reinforced through MLR17 which stipulates that FIs must keep their customers' CDD documents/information up-to-date as part of the requirement to conduct ongoing monitoring. It is no coincidence that the ICO expands on principle 4 in its response to the consultation on MLR17, outlining how in practice data controllers must:

- take reasonable steps to ensure the accuracy of any personal data they obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

The ICO deliberately highlights these provisions due to the clear potential for misattribution, an issue which is of particular relevance to PEP customers as will become clear. In its response, the ICO drew attention to the fact that MLR17 states that when identifying if an individual is a *'known close associate'* of a PEP, the FI need *'only have regard to information which is in its possession, or to **credible** information which is **publicly available**'* [emphasis added]. The ICO stressed the fact that there is no consensus on how 'credible information' and *'publically available'* are to be defined[3]. Consequently, ostensible 'family members' and 'known close associates' may feel aggrieved if they have been erroneously categorised as a customer with a link to a PEP (and hence worthy of more intrusive EDD measures) using sources which are unknown to them and which they have not been able to challenge the accuracy or relevance of.

This is an acute concern bearing in mind that the primary tools used by FIs to identify 'family members' and 'known close associates' are screening applications provided by third party vendors. These tools amalgamate a wide range of sources, which has the benefit of extensive coverage but also the drawback of the inclusion of sources of questionable repute. So serious is the ICO's concern for misattribution that it called for greater clarity on both definitions, along with appropriate guidance on the use of such information[4].

FIs should take note of these concerns as the data obtained from screening tools is *Personal Data* after all, and hence there is the requirement to ensure that it is accurate, relevant and up-to-date. The issue of misattribution will undoubtedly assume greater relevance under GDPR as it places greater emphasis on the ease of the data subject's right to rectification. The fourth data protection principle has thus been amended to now include the addition of; *'.....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'*. Moreover, GDPR explicitly holds data controllers accountable for ensuring the accuracy of the personal data held and stipulates that they should be able to demonstrate compliance with this obligation.

'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'

GDPR (EU) 2016/679 – fourth data protection principle

Next steps:

- Firms should ensure that they are able to demonstrate compliance with the obligation under GDPR for ensuring the accuracy of the personal data held.
- Review and take into account the potential limitations of any screening tools acquired from third party vendors.

3. ICO response to MLR17
4. ICO response to MLR17

Financial exclusion and de-risking

Taking a step back for a moment, we can see that the potential for misattribution was also a key concern embedded in the first data protection principle; data controllers should '*not use personal data in ways that have unjustified adverse effects on the individuals to whom the data relates'.*

Clearly, the potential for spurious media sources providing 'evidence' of either links to PEPs or unsubstantiated negative news, could have *'unjustified adverse effects'* on customers. The ICO even acknowledges the financial exclusion of individuals solely on the basis of their PEP status or connections. Excluding customers purely based on their categorisation puts the issue firmly in the heart of the de-risking debate, and while de-risking pronouncements have mainly been focused on respondent banks, charities and MSBs located in high risk jurisdictions, it is noteworthy that the report commissioned by the FCA on the subject included evidence of the difficulty faced by Crown and civil servants, including members of the UK diplomatic service who had served aboard, who had problems obtaining bank accounts by virtue of their positons[5]. The measures laid out in Section 30 of the Act are a reflection of these concerns as they gave the Secretary of State the power to make provisions regarding the arrangements that be put in place for individuals who complain about their treatment by FIs. The circumstances in which the complaint will be adjudicated on mirror the scenarios previously discussed[6] :

- a person was treated as though he or she was a PEP (and he or she was not);
- a person who is a PEP was treated unreasonably in disregard of (the FCA) guidance; and
- a person was refused a business relationship solely on the basis that he or she is a PEP.

The PEP guidance issued by the FCA last year in response to the Act stressed that not all PEPs pose the same inherent risk and as such should be considered on a case-by-case basis, going on to state that:

'The FCA expects that a firm will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or of a family member or known close associate of a PEP). A firm may, after collecting appropriate information and completing its assessment, conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases will it be appropriate to decline or close that relationship'.

In terms of actual redress though, the FCA's guidance was limited, simply stating that:

'The Financial Ombudsman Service ("FOS") will consider complaints from PEPs, their family members or close associates – and will take the guidance into account when deciding what is fair and reasonable in all the circumstances of a complaint'[7]

FIs should nevertheless be wary of bringing any customers into the orbit of the FCA or the FOS, as the treatment of PEP customers and de-risking practices more widely are brought under increased scrutiny. The Explanatory Memorandum to MLR17 provides a prime example of such a pronouncement:

"Refusing to establish a business relationship or carry out a transaction with a person simply on the basis that they are a PEP is contrary to the letter and the spirit of the law"

MLR17 – Explanatory Memorandum

Next steps:

- Firms should first evaluate the effectiveness of their PEP risk assessment processes and then ensure that risk appetite thresholds determining the acceptance of PEPs is considered alongside and is given equal footing with those applicable to other high risk customers classes e.g. MSBs, charities and respondent banks.
- When rejecting new PEP customers, firms should ensure that their decision is reflective of a properly functioning risk-based approach. Without this documented, the firm runs the risk of falling foul of the compensation measures laid out in the Act.

5. John Howell & Co. Ltd. – Drivers & Impacts of de-risking: A study of representative views and data in the UK, by John Howell & Co. Ltd. for the Financial Conduct Authority (2016)
6. Bank of England and Financial Services Act (2016)
7. FCA PEP guidance

Cessation of PEP status

When considering data protection as part of the treatment of PEPs, FI's must also pay close attention to another salient provision of MLR17. Under the Regulations, family members and known close associates no longer need to be subject to EDD measures after the PEP in question (i.e. the PEP they are connected to) has ceased to hold their public function.

This applies even if the 12 month cooling off period has not yet elapsed, with the obvious caveat that all decisions on the cessation of EDD measures must be subject to a risk-based approach. The difficulty here is that if a decision has been made by senior management to cease EDD measures for a family member or close associate, then as they have deemed the relationship to no longer be high risk, then is there a legitimate reason to hold extra information provided by the customer which was obtained outside of the public domain? Such information could include detailed accounts of their business interests, their financial situation and how they acquired their wealth over time. Clearly, where there is evidence of a culture of nepotism or cronyism in a particular jurisdiction, then it will be necessary to continue EDD measures. The difficulty therefore lies in the treatment of family members and close associates of low risk domestic PEPs, as firms need to take account of the third data protection principle which states that personal data held shall be *'adequate, relevant and* ***limited to what is necessary*** *in relation to the purposes for which they are processed ('data minimisation')'* [emphasis added]. These data protection considerations should also be considered alongside the fact that regulators and global standard setters are taking a dim view of firms which adopt a *'PEP for life'* blanket approach. The Wolfsberg PEP Guidance issued last year emphasised the circumstances where it would **not** be appropriate to subject certain 'family members' and 'close associates' to the same control framework as PEPs.

The Guidance listed separation, estrangement or the end of a business relationship with a PEP as examples of such cases. Indeed, the Wolfsberg Guidance could not be more explicit in its disproval of the blanket approach adopted by many FIs; '*the principle of "once a PEP, always a PEP" runs counter to an appropriate RBA and should be considered very carefully before being applied*'[8]. The FCA's own PEP guidance was also equally clear on this point:

'*A PEP must be treated as a PEP after he or she leaves office for at least 12 months, depending on risk. This does not apply to family members, who should be treated as ordinary customers, subject to customer due diligence obligations from the point that the PEP leaves office. The FCA considers a family member of a former PEP should not be subject to enhanced due diligence measures unless this is justified by the firm's assessment of other risks posed by that customer*'[9]

Reconciling data protection and record-keeping obligations under MLR17 will therefore present a unique challenge for firms, especially considering that the timelines on holding the CDD documentation and information apply after the business relationship ends (this includes all additional information collected as part of EDD). It therefore seems that a grey area exists when holding supplementary information on a customer who is no longer deemed high-risk, but who is still a current, and now low or medium risk, customer.

'the principle of "once a PEP, always a PEP" runs counter to an appropriate RBA and should be considered very carefully before being applied'

The Wolfsberg Group – Guidance on Politically Exposed Persons

Next steps:

- Firms must ensure that the individual responsible for making the decision to cease enhanced measures (as well as accept/continue PEP relationships) on the family members or known close associates of a PEP is of sufficient seniority. Firms should consult the FCA PEP guidance when inferring the level of seniority for different risk levels.
- Firms which apply a "PEP for life" blanket approach should consider if this is truly commensurate with a risk-based approach and whether it would stand up to regulatory scrutiny.
- When making the decision on whether an individual qualifies for PEP status, firms should make use of the new lists, required to be published as part of the 5th Money Laundering Directive, of exact functions which qualify as prominent public functions. Each member state and any international organisations accredited to it will be required to keep an up-to-date list of exact functions which qualify as a 'prominent public function'.

8. The Wolfsberg Group – Wolfsberg Guidance on Politically Exposed Persons (PEPs) (2017)
9. FCA PEP Guidance

Closing remarks

As this paper has demonstrated, a firm's AML/CFT and data protection obligations are not always mutually aligned, leading to greater uncertainty with regards to the application and prioritisation of such measures, especially considering that the costs of non-compliance will be severe in both cases. Navigating their way through the raft of new legislation and industry guidance will therefore require a period of introspection when deciding how they treat their PEP customers in order to ensure that both AML/CFT and data protection obligations are given due consideration.

Glossary

Acronym or term	Definition
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
EDD	Enhanced Due Diligence
FCA	Financial Conduct Authority
FI	Financial Institution
FOS	Financial Ombudsman Service
GDPR	EU General Data Protection Regulation (2016/679)
ICO	Information Commissioners Office
MLRO	Money Laundering Reporting Officer
MLR17 or Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
PEP	Politically Exposed Person
RBA	Risk-based approach
the Act	Bank of England and Financial Services Act (2016)

Contacts

If you want to get in touch with us, please contact one of the Deloitte team listed below:

Katie Jackson
Partner
Tel: +44 (0) 20 7303 0586
Mob: +44 (0) 7748 931108
Email: kjackson@deloitte.co.uk

Biren Shah
Partner
Tel: +44 (0) 20 7303 2879
Mob: +44 (0) 7775 818286
Email: birenshah@deloitte.co.uk

Emma Hardaker
Director
Tel: +44 (0) 20 7007 0411
Mob: +44 (0) 7468 700296
Email: emhardaker@deloitte.co.uk

Alexander Hitch
Assistant Manager
Tel: +44 (0) 20 7303 0243
Mob: +44 (0) 7964 017460
Email: ahitch@deloitte.co.uk

Download more financial crime insights like this at **Deloitte.co.uk/FinancialCrime**

Deloitte.