GENERAL FEEDBACK for PUBLIC CONSULTATION on GUIDELINES for AML, CP128.

The Data Protection Commission is responsible for upholding the rights of individuals as set out in the GDPR and Data Protection Acts 1988-2018 and enforcing the obligations upon data controllers. The Commission is appointed by Government and is independent in the exercise of its functions. This Office does not approve any particular use of personal data but offers guidance as to the obligations and responsibilities of data controllers.

We welcome the opportunity to provide observations on the draft AML guidelines, which we believe, will provide valuable assistance to all entities required to comply with AML obligations, especially when balancing the requirements under the fourth & fifth Directives with the GDPR principles of Purpose limitation and Data Minimisation. One of the key elements in the 4th Directive is for Data protection rules to apply in any implementation of AML.

This is set out in the 4th AML **Directive 2015/849 in Recital 43**, which states …

It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of

complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

There is one potential ambiguity therefore in that the AML procedures have to work in tandem with the data protection principles of Purpose Limitation and Data Minimisation as set out in **Article 5 of GDPR**.

Therefore, the reasonable risk based approach should be done in a proportionate, relevant and as necessary, wherein the principles of data minimisation are also being complied with. If this does not occur, then the consequences are that the entity /data controller could be in breach of the GDPR and the Data Protection Act, 2018 and as a result face potential sanction pursuant to the corrective powers and administrative fines that the DPC has (Max potential fine of €20 million or 4% of total worldwide turnover.)[1]

It is therefore important that all entities when conducting AML procedures have a balanced approach when fulfilling the regulatory AML requirements together with the data protection requirements, that involve the methods of processing for Customer Due Diligence and other aml measures for PEPS, beneficial owners etc, are done in a proportionate manner. That it is consistent with GDPR the collection and processing of personal data.

The guidelines can also be used as a useful tool for financial entities to apply to their 'Transparency Notices', when informing the Public about aml requirements. In this regard **Article 13 of GDPR** states that Data Controllers need to provide information to the Individual when collecting personal data from him/her (for aml purposes) with the core provisions being :-

- The purposes of the processing.[2]
- The recipients of the personal data.[3]

[1] Article 83 of GDPR and Section 141 of the Data Protection Act, 2018
[2] Art 13.1 (c)
[3] Art 13.1 (e)

- The period for which the personal data will be stored.[4]
- The existence of the rights of the individual to request from a Data Controller / Financial entity access to and rectification or erasure of incorrect personal data.[5]
- Consequences of failure to produce personal data where it is a statutory requirement.[6]
- The existence of automated decision making, including profiling referred to in Article 22(1) and (4) and at least in those cases meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[7]
- The right to lodge a complaint with the DPC.[8]

Similar provisions apply under **Article 14 of GDPR**, when the personal data of an individual has not been collected or obtained directly from the individual but has been sourced from other sources such as publically available information or other third parties. Examples of such entities could be Credit reference agencies / Agencies that provide identity checking services / Sanction lists/ Information made available publically from State agencies such as CRO, Revenue Commissioners, and Court Services.

Specific Comments of the guidance document.

Beneficial Ownership & PEPs (Paragraphs 5.2.2 and 5.6)

1. This office has received many queries from data controllers over the years on how the entities can comply with their AML obligations as well as the Data protection implications for such collection and processing. One of the problem areas relates to where an individual is associated with other individuals such as a spouse, offspring, sibling, next of kin, etc, especially when the individual in question is a politically exposed person or a beneficial owner with other beneficial owners or a Joint account holder with

[4] Art 13.2 (a)
[5] Art 13.2 (b)
[6] Art 13.2 (e)
[7] Art 13.2 (f)
[8] Art 13.2 (d)

other parties. We note the guidance in the document on these specific areas, which is very general. Therefore, we would welcome more detailed guidance and possible case studies or examples as to what the defined obligations are for any entity when they have to comply with the requirements for PEPs, Beneficial ownership, connected persons and related parties. A consistent approach should be developed in these areas so that any reporting entity has the relevant information as to what is expected of it to comply with both the AML and data protection issues. This is important for any person that is associated with or related to a PEP and is being risk assessed for ML/FT , based on that connection. That person may not know that they are being made subject to an enhanced due diligence procedure because they are linked to a PEP. Similarly, it applies to "Connected persons" and "Related Parties".

Use of Innovative solutions (Paragraph 5.2.5)

2. Please note that where the "regtech" solution incorporated new technology that involves the profiling or automated processing of the personal data of a customer database then it will probably require a 'Data Protection Impact Assessment', to be done. Please see our guidance note for more information at the following link :- https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf

Ongoing Monitoring (Paragraph 5.3)

3. **Section 35(3) of CJA 2010** requires the monitoring to occur to … *the extent reasonably warranted by the risk of ML/TF .* This is consistent with the "reasonable risk based approach". However does this mean that an entire customer database has to be profiled and matched to a sanction list on a daily basis especially is the majority of these customers have already been assessed as a low AML risk and not engaged in criminal conduct?
   We understand that "periodic reviews" can be completed but more guidance would be appreciated as to what is commensurate with the level of ML/TF risk. In this regard, it would appear that any identified 'High', risk would warrant a daily review with a sanction list or other means of reviewing the High Risk. Also enhanced due diligence may warrant such actions. However, low level risks for which we assume that the

majority of the customer database are on, should not be treated similarly to a high risk or Advanced due diligence procedures unless it is specifically justified. From a data protection perspective, this is important to comply with the Principle of Purpose Limitation so that the personal data is not processed in a manner that is incompatible with the objective of identifying criminal behaviour under AML/FT to that of an ordinary law abiding customer.

Record Keeping (Paragraph 9)

4. **Article 30 of GDPR** requires that any data controller keeps a record of processing activities and this is compatible with the guidance in this paragraph. It is also very important for any data controller to have a proper record of processing activity as not only does it assist with regulatory audits and lawful requests for disclosure, it also assists with dealing with an Individual exercising any one of his or her fundamental rights under GDPR i.e. Right of Access, Rectification etc.

Screening Customers against Sanction lists (Paragraphs 10.3.3 and 10.3.4)

5. It would be beneficial if it could be outlined what sort of sanction lists exist and when they are used and how they are used. Again, this relates to the rights of individuals to be informed as to what is occurring with the processing of their personal data, whom it is being disclosed to, and what action can occur from it. It is especially important if the information on the customer is inaccurate or incorrect or has been contaminated by an identity impersonation or identity fraud. In such instance, an individual has the right to seek the correction or erasure of inaccurate personal data. In some justified cases, this might require an amendment to the Sanction list itself.

Should you require any clarifications on the above matters. Please contact the undersigned.

Garrett O'Neill

Head of Private & Financial Sector Consultation

Data Protection Commission

An Coimisiún um Chosaint Sonraí
Data Protection Commission

3rd April 2019

An Coimisiún um Chosaint Sonraí, 21 Cearnóg Mhic Liam, Bhaile Átha Cliath 2.
Data Protection Commission, 21 Fitzwilliam Square, Dublin 2.
www.cosantasonrai.ie | www.dataprotection.ie | eolas@cosantasonrai.ie | info@dataprotection.ie Tel: +353 (0)76 1104800