Finding the balance between data protection and AML requirements

*The Fourth Anti-Money Laundering Directive ("**4AMLD**") required transposition into national law by 26 June 2017. The new obligations imposed on obliged entities by means of the 4AMLD are significant and require investment in dedicated compliance resources. The changes brought about by the 4AMLD cannot however be seen in isolation but must be considered in the context of other important developments, including revisions to the 4AMLD itself (known as the 5AMLD), which are currently being negotiated at EU level and the General Data Protection Regulation ("**GDPR**"), which will come into force on the 25 May 2018.*

What has to change?

The balance between the data protection framework and the AML regime does not typically top the agenda of the people that matter in obliged entities. More often than not, AML obligations have tended to take precedence, even if this meant trumping on data protection principles. This is even true from a regulators' perspective, who appeared to promote the countering of money laundering as far more important than protecting an individual's privacy. Indeed, by setting high expectations on obliged entities under the AML regime both through their off-site and on-site communications, regulators have indirectly been delegating responsibilities for AML to such obliged entities. Regulators across all EU Member States tend to be under-resourced and generally lacking expertise, which has resulted in them pushing their AML responsibilities down the regulatory line and deputising obliged entities to perform the role of law enforcement offices. In turn, obliged entities have been left with little option but to do what they can to meet regulators' expectations, even if this meant throwing data protection principles out of the window, thus safeguarding themselves against the risk of reputational damage and other regulatory sanctions.

This will now have to change. The GDPR imposes harsher penalties and transparency requirements ,and, more importantly, introduces the concept of individual accountability. Collectively, these factors suggest that obliged entities must up their game when it comes to compliance with data protection requirements. To some extent, the 4AMLD aspires to transcend this by having the risk-based approach as the star of the show. It also imposes data retention limits and forces human intervention in automated alert systems, thereby impressing upon obliged entities the need to consider AML and data protection requirements as complementary to each other rather than being mutually exclusive.

Interplay between AML-related projects and data protection requirements

Many AML-related projects will overlap with data protection rules, particularly remediation and implementation measures that will follow the 4AMLD transposition. In connection with these initiatives, obliged entities might be considering the installation or upgrade of screening tools, the introduction of regulatory technology in KYC/CDD processes, the development of data mining of customer data for detection of suspicious activity, and a spate of other measures, which should not only be targeted at AML compliance but should also consider requirements under the GDPR. In addition, obliged entities may be looking into the outsourcing of AML-related activities involving personal information (such as sanction screening or KYC) and, in these cases, the outsourcing agreement should not focus exclusively on AML compliance but should also oblige the service provider to evidence compliance with key requirements under the GDPR. Compliance with the GDPR is even more crucial given that it places more onerous and direct obligations on data processors, in comparison with its predecessor.

The risk-based approach facilitates this interplay, particularly insofar as data collection and analysis are concerned. In terms of data collection, the focus should not be one of casting the net as widely as possible and grabbing every piece of data that comes your way. Rather, the spotlight should be on the quality and 'recency' of data. Using low quality data, including data from dodgy sources, is not only unhelpful by detracting the focus from other more important information, but can also have unintended adverse repercussions, for example in the event that an obliged entity decides to block a transaction on the basis of such data and causes damages to any third party as a result. Obliged entities must also be able to demonstrate that their policies and procedures for data collection are commensurate to the risk posed by the customer and hence vary depending on whether simplified, normal, or enhanced due diligence is being applied.

What should the next steps be?

The overriding advice is for obliged entities not to wait for the date of applicability of the GDPR to weave data protection policies and processes into day-to-day business activities. As changes to the AML regime are well-underway, data protection issues should be considered in parallel across all areas. This will require obliged entities to consider beefing-up their privacy expertise and conducting a privacy risk assessment but also embed privacy requirements in policy and procedures and train client-facing and compliance staff, as well as the MLRO in data protection. For this purpose, obliged entities should also consider conducting impact assessments of the processing of personal data to achieve a 'privacy by default and design' under the GDPR.

Clearly, it is not only obliged entities who must make this shift, but also regulators – as long as regulators will continue to overlook data privacy issues in their AML supervision activities, there is a high risk that obliged entities will follow suit. In fact, the perception remains that the objective of combatting money laundering should be considered superior to the respect to one's privacy as policymakers continue to debate the 5AMLD and the extent to which different parties should be granted access to the data contained in the beneficial owner register. Nevertheless, it is important for obliged entities to challenge the status quo by thoroughly documenting their risk assessments and rationale underpinning their data collection and analysis activities. This is because obliged entities are not exclusively accountable to law enforcers and regulators, but they must also be able to justify their actions to their data subjects, who may question whether the extensive personal data being demanded of them is really necessary in light of the risk level and nature of the service being provided.

Obliged entities are consistently being bombarded with new regulation and amendments to existing frameworks. Yet, the AML regime appeared to operate relatively in isolation, even in the wake of FATCA and CRS which, notwithstanding certain overlaps, did not really tie in with the pure AML compliance obligations. The GDPR will however force its way into the AML space and obliged entities should force themselves to understand its sheer significance. Headway can only be made if obliged entities consider the 4AMLD and the GDPR as a good opportunity to revisit the amount and extent of personal data being collected and retained for AML purposes, in order to assess whether the current *modus operandi* merits reconsideration and amendments to ensure that the data being processed is limited to that which is required at law and which adds value to the compliance process. This will not only entail a systems change but will require, more importantly, a cultural change that will force individuals to discard a tick-box approach to AML compliance.

Contact us

Camilleri Preziosi commands an outstanding reputation amongst clients and peers as a leading Maltese corporate law firm. We are regularly ranked as a top-tier firm by Chambers, IFLR1000 and Legal 500. We retain a strong commitment to deliver a quality service in the practice of law. We do this by combining technical excellence with a solution-driven approach.

We have substantial experience in advising and assisting clients with their AML and data protection compliance obligations. Please contact our regulatory and data privacy experts below for further information as to how we can help.

Diane Bugeja
Senior Associate, Corporate Finance
D (+356) 2567 8132
E diane.bugeja@camilleripreziosi.com

Sharon Xuereb
Associate, Regulatory, EU and Litigation
D (+356) 2567 8125
E sharon.xeureb@camilleripreziosi.com