Bloomberg Law

Privacy Law Watch™

Financial Data

A Compliance Conundrum for Financial Institutions: U.S. Anti-Money Laundering Initiatives and the Forthcoming EU General Data Protection Regulation

Money Laundering

The new European Union privacy regime, the General Data Protection Regulation, will have direct and important ramifications for current anti-money laundering and counter-terror finance compliance programs, many of which are inconsistent with the GDPR, the author writes, showing that GDPR-money laundering integration requires a multi-disciplinary approach involving a financial institution's legal, compliance, and information services functions.

By William P. Barry

Multinational financial institutions find themselves facing a compliance conundrum. The European Union General Data Protection Regulation (GDPR) is slated to go into effect on May 25, 2018. Financial institutions that provide services in the EU or use EU residents' personal data for marketing purposes may find themselves subject to its requirements. The GDPR will dramatically expand the rights, obligations and penalties associated with data privacy protection in the EU, and will affect companies operating in the EU as well as those located there. The GDPR will change the manner in which financial institutions may properly collect, process, use, share, and store data. This has direct and important ramifications for anti-money laundering and counter-terror finance (AML/CTF) compliance programs at those institutions, particularly for financial institutions subject to U.S. AML/CTF requirements and the EU's Fourth Anti-Money Laundering Directive. Many current AML/CTF compliance programs are inconsistent with the GDPR's requirements.

William Barry is an attorney at Miller & Chevalier LLP in Washington that advises financial institutions on a broad range of issues including compliance with Foreign Corrupt Practices Act and money laundering.

In this article, we discuss (a) areas of conflict between the GDPR and current U.S. AML/CTF compliance practices; (b) the challenges faced by multinational financial institutions that must comply with both regimes; and (c) steps financial institutions should take now to achieve GDPR compliance and avoid diluting their commitment to sound AML/CTF practices.

Areas of Conflict Between the GDPR and Current U.S. AML/CTF Compliance Practices The conflict between the GDPR and U.S. AML/CTF compliance practices stem from two sources. First, there is a fundamentally different interpretation of who owns personal data. Under the U.S. construct, the financial institution (or

 ISSN 0000-0000

other entity) that comes into possession of personal data is deemed to be the owner of that data. The EU views such data as belonging to the individual and has taken increasingly aggressive steps to protect its collection, processing, use, sharing, and storage. Second, since the enactment of the USAPatriot Act, the U.S. approach has been to view AML/CTF and data privacy as separate issues with AML/CTF taking priority due to its importance to national security. This approach is consistent with Financial Action Task Force (FATF) recommendations, which historically have prioritized AML/CTF concerns over data privacy, and typically do not incorporate EU data privacy considerations. As a result, entities subject to AML/CTF and data protection/data privacy requirements have prioritized the former over the latter. The GDPR clarifies the EU's expectation that AML/CTF compliance measures must fall within the data protection/data privacy framework, and establishes significant penalties for entities and for individuals in the event this expectation is not met.

For many financial institutions, AML/CTF processes such as Know Your Customer (KYC) and sanctions screening have included the collection of massive amounts of data that are then filtered, sorted, evaluated, and stored for current and future use. The GDPR will require a different approach. Personal data collection must be undertaken for specific, approved purposes. Such data may be maintained only as long as necessary and the collection cannot be excessive. There are limitations on how such data can be shared both within and without the organization, as well as responsibility for the oversight of third parties to whom AML/CTF roles may be delegated or who may be retained to process data.

In addition, data collected for an approved, legitimate purpose cannot be used or maintained for other usage unless such usage also qualifies as legitimate. For example, to the extent that customer or third-party personal data is collected and used for AML/CTF purposes and then imported into other systems within the institution for marketing purposes, that use must be evaluated and justified. This has the potential to require significant work by legal, compliance, and information services stakeholders to assess the manner in which information flows within the organization, how sensitive data is compartmentalized and how to make efficient and effective use of data within the requirements of the GDPR.

Challenges Faced by Multinational Financial Institutions The GDPR will come into effect at a time when financial institutions are being required to collect and maintain increasing amounts of information for AML/CTF and other regulatory purposes. The challenges posed by the GDPR for financial institutions are myriad, including identifying relevant, accurate data that can be used for AML/CTF purposes and assuring such data is protected from misuse within the organization or breach from without, to educating affected individuals regarding the intended use of personal data and obtaining the individual's consent required for collection and processing of personal data. In addition, an institution must be able to monitor the data it holds, delete data when it is no longer necessary and be in position to explain its process to regulators with competing agendas.

The issue of misuse within the organization is a potential minefield for financial institutions that may have collected personal data for legitimate AML/CTF purposes and then sought to monetize that information, for example by using KYC-related information for marketing purposes or to develop other business strategies. The European Data Protection Supervisor (EDPS) commented on access to beneficial ownership information and data protection implications in its February 2017 opinion on proposed amendments to EU money laundering directives. Among other issues, the EDPS noted that ''Processing personal data collected for one purpose for another, completely unrelated purpose infringes the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality.'' *Opinion 1/2017 of 2 February 2017 on the access to beneficial ownership information and data protection implications.* The EDPS questioned whether ''invasive personal data processing, acceptable in relation to anti-money laundering and [the] fight against terrorism, are necessary out of those contexts and . . . whether they are proportionate.'' *Id.*

The use of customer personal data for purposes of risk profiling and customer transaction monitoring poses additional challenges. While the utility of these methods is generally acknowledged, the GDPR requires increased transparency on the part of controllers of personal data to assure that individuals whose data is collected understand the use for which their data has been collected. It also provides opportunities for individuals to object to the use of personal data for these purposes. Accordingly, financial institutions must prepare for how such objections will be received and addressed.

Steps Financial Institutions Should Take Now to Achieve Compliance Integration of GDPR principles with AML/CTF compliance processes requires a multidisciplinary approach involving the legal, compliance, and information services functions. Just as importantly, it requires training to re-orient personnel with respect to the appropriate handling and usage of sensitive data. Steps financial institutions should consider include:

- develop a task force for implementation and establish clear lines for ongoing governance and accountability for addressing tensions between AML/CTF issues and data protection/data privacy requirements, including:
  - analyzing and remediating gaps or inconsistencies between the use of personal data under the AML/CTF program and GDPR requirements;
  - streamlining information sharing and record keeping processes;
  - evaluating third-party agreements and relationships relevant to the collection, processing, filtering and storage of personal data, including outsourced AML/CTF functions; and
  - enhancing notice, consent, and documentation procedures as well as processes for addressing objections from individuals regarding the use of sensitive data;
- inventory regulatory risk stemming from data protection/data privacy in the EU and elsewhere, including jurisdictions in which the institution has operations, maintains data servers or is otherwise exposed;
- identify the type and content of personal data under the institution's control and analyze the purpose for which such data is held, the location at which it is held, the length of time it is stored, whether and how it is

  PRA ISSN 0000-0000

shared or transferred, and what safeguards are in place to prevent leak or theft of the data;

■ evaluate the current segregation of data within the organization's systems, including whether functions outside of the AML/CTF process have access to sensitive KYC, CDD, or similar data;

■ implement group-wide policies and procedures regarding the interplay of data privacy and AML/CTF, particularly with respect to the sharing of information collected in the AML/CTF process. This approach should include, but not be limited to, sharing such data within the organization and also pursuant to information-sharing provisions under in U.S. law that are part of the AML/CTF process. Policies and procedures should be implemented more broadly if the financial institution uses such data outside of the AML/CTF process, e.g. for commercial purposes;

■ review and update as necessary any codes of conduct and employee consent provisions relevant to the collection, retention, and transfer of personal data;

■ develop a process for assuring AML/CTF program compliance with prohibitions on the transfer of sensitive data outside of the European Economic Area, and potential exceptions thereto;

■ conduct enhanced training for AML/CTF professionals to better incorporate data protection/data privacy concerns in their day to day responsibilities.

AML/CTF compliance and data protection/data privacy do not have to operate with competing agendas. Indeed, incorporating the AML/CTF compliance process into a data protection/data privacy framework can provide important advantages to financial institutions. The challenge for financial institutions is to proactively develop a clear, defensible process to achieve GDPR compliance without diluting AML/CTF compliance. This will require a coordinated effort to understand existing tensions within the financial institution's current processes and reorient company personnel in a manner that promotes the GDPR objectives of established rights to personal data protection and privacy.

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberlaw.com