ACHIEVING AML, PRIVACY & DATA COMPLIANCE MANAGEMENT CONVERGENCE IN THE AGE OF GDPR

By: Robert Merrick & Suzanne Ryan

In the age of the European Union's expansive requirements for the protection of personal information under GDPR, organizations large and small need to be mindful of the converging obligations of AML, Privacy and Data Management when delivering products and services to customers.

Below is an outline of the critical Governance, Risk and Compliance Management (GRCM) steps needed to manage the risks associated with regulatory regimes that address the collection, use and storage of data belonging to or about customers, employees and other individuals.

TEN STEPS TO ACHIEVING INFORMATION COMPLIANCE READINESS

1) Enable GRCM Relative to Business Size

GRCM should be handled internally, externally through third-parties, or a combination of both by delegating responsibility but not accountability (i.e. at least one person internally must be accountable for compliance).

2) Identify Compliance Requirements and Assess Risk Scope and Tolerance

Determine what regulations apply to your business, the risk of non-compliance, and your organization's risk tolerance. Monitor changes in regulation and resulting changes in risk.

3) Assign Compliance Accountability and Authority throughout the Organization

Identify responsibility for, and governance of, compliance and risk management obligations throughout your organization and assign accountability in policies and job mandates.

4) Develop Program Policies & Procedures Across Business Lines and Functions

Establish written policies and procedures for managing, assessing and reporting on employee, customer and third-party compliance obligations and related risks.

Cont'd ...

... Cont'd

5) Create and Manage Processes and Systems for Protection & Retention of Data

Define and document control processes and systems that gather, process or store personal information of, or by, customers, employees and third-parties collected across business lines based on business accountabilities and legislative responsibilities.

6) Institute Customer, Employee and Third-Party Relationship Controls Consistent with AML, Privacy and Data Management Program Objectives

Put in place controls to manage customer and employee rights and your obligations for the collection, use and storage of their information, including that which is collected and/or distributed by third parties.

7) Activate a Process for Complaint and Incident Response Handling and Reporting

Define roles and responsibilities for processes for managing AML, privacy and data management complaints and breaches including those relating to complaint escalation and reporting.

8) Integrate GRCM within Operational Systems and Processes

Since there are many operational areas that touch personal information (e.g. technology operations, legal, marketing, payroll, human resources), develop a strategy and plan to design and implement a GRCM program that integrates fully with all relevant systems and processes.

9) Adopt a GRCM Stakeholder Communications Strategy

Implement GRCM-approved strategies to communicate with customers, employees, vendors, shareholders, regulators, media, and any other stakeholders who need information about compliance matters (e.g. data breaches).

10) Implement a Compliance Monitoring and Reporting System

Put in place processes and system to monitor 1st line controls in coordination with the 3rd line and to assess the effectiveness of compliance controls.

For GRCM information or assistance, please contact:

Robert Merrick, Principal
GRC MANAGEMENT ADVISORY SERVICES
D: 416-727-5525
E: robert.merrick@grcmanagement.ca

Suzanne Ryan, Strategic Advisor
GRC MANAGEMENT ADVISORY SERVICES
D: 647-980-1300
E: suzanne.ryancousto@gmail.com