Checklist for M&A's – Data Management Practices

Data production is forecasted to be 44 times greater, or a 4300% increase in annual data generation in 2020 verses 2009.[i] This data growth produces a massive undertaking for the Privacy Office to maintain organizational compliance related to the collection, transfer, use, storage and timely destruction of personal data.

This document is an aid for privacy officers and staff to define data protection and management procedures for personal data using a standards and controls [ii]approach that enables compliance with domestic and international privacy regulations and laws. In conjunction with this effort, the privacy office should include a metrics program, which can provide evidence of compliance to management, regulators and internal audit. Specific details of the measurements and metrics that can be employed are outlined in Monitor Data Handling Practices - Measurement and Metrics.pdf.

Identify the Disciplines, Practices and Partners

The monitoring and reporting program will need to identify and agree upon the disciplines that apply. Define the following; monitoring procedures, measurement processes, and secure agreement from the business functions for resources to manage the data handling practice. The activities are key to an overall a data governance process. The table below provides an outline to identify the disciplines, data management practices and business partners for the program.

Discipline	Standard	Control	Business Partner
Notice	Consistent notification that defines the purposes of use	Assessment of the systems or processes operated to collect personal data	Legal, Marketing
Collection	Practice to limit personal data only necessary	Audit of the systems or processes to validate data types	IT, Operations
Use	Defined application of business practices or intentions	Audit of the systems or processes to validate practices	IT, Marketing, Operations, Compliance
Choice	Consistent application of individual rights	Assessment of online systems, call center operations, email requests	IT, Operations
Integrity or Accuracy	Defined system requirements that limit inaccurate or fraudulent input, documented operational processes	Audit of the systems or processes to validate practices	IT, Marketing, Operations, Security
Transfer	Document requirements for international data transfers	Assessment and overlay of regulatory obligations, routine process checks of origin of collection and data types	IT, InfoSec

Discipline	Standard	Control	Business Partner
Access and Correction	Defined system requirements and business practices that enable individual capabilities or operational practices	Assessment of online systems, call center operations, email requests	IT, Operations
Accountability	Defined organizational roles and responsibilities and required privacy registrations/filings	Audit of functional roles, systems or processes to validate regulatory compliance	Marketing, Compliance
Data Protection or Safeguards	Defined data protection requirements by data type, vulnerability and external risks	Assessment of online systems, internal applications/databases, email platforms, ingress and egress points	IT, InfoSec

A comprehensive monitoring and reporting program assists the Privacy Office in understanding the level of regulatory compliance, costs, potential harm and risks to the individual and business.

Monitoring and Reporting

A comprehensive monitoring and reporting program are critical components of the privacy program, they enable the privacy office to identify and document the overall level of compliance and areas of non-compliance. In addition a remediation process for non-compliance gaps should be incorporated and should; assign gap ownership, track remediation activity, implement changes and follow up testing of the changes.

The Privacy Office should document the program's objective, frequency and identify who will receive the results of the monitoring and reporting efforts. These reports in conjunction with the metrics recorded can provide evidence of compliance and protect or reduce the organization risk of fines, civil actions or loss of personal data use in the event of a data breach, regulatory audit or legal action. Specific details of the measurements and metrics that can be employed are outlined in [name document].

Conclusions

It is critical that management understands the scope, funding and risks of the monitoring and reporting program. In the event the privacy office has recorded non-compliant findings and the organization has not remedied in a reasonable period of time, a data protection authority or enforcement arm of the authority can review reports and determine that the organization is in violation of applicable law. This may create additional financial, civil or criminal risks to the organization and the executives.

[i] Sources: IDC/EMC 2011 Digital Universe Study, 2010 Digital Universe Decade Study, Data Evolution, Sept. 2011, CSC's Leading Edge Forum

[ii] Standards are defined as documented technical specifications or other criteria to be used consistently as guidelines, or definitions of characteristics to ensure that processes and services utilize the data for the defined purpose(s). Controls are defined as technical or administrative safeguards or counter measures to avoid, counteract or minimize loss or unavailability due to threats, vulnerabilities or security risks.