Monitor Data Handling Practices: Measurement and Metrics

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. To aid privacy officers and staff in defining and maintaining a measurement and metrics program, this document provides specific details that can be utilized.

Identification of Measurements

The privacy office will need to identify the measurement practices, metrics will vary and based on risk tolerance of the business, the tables below are broken into two levels. Table A includes activities that require minimal staffing and considered low hanging fruit. Table B includes activities that require higher level of staffing and additional effort.

Table A

Discipline	Measurement	Frequency	Comments
Consent (Online)	Number of consent clicks recorded vs records updated in the data warehouse	2x/month for small to medium, weekly for large	Privacy included in the development and approval of the privacy notice
Consent (Mobile)	Number of consent clicks recorded vs records updated in the data warehouse	2x/month for small to medium, weekly for large	Privacy included in the development and approval of the privacy notice
Access (Manual)	Number of calls generated by customers/consumers requesting access to their records	Quarterly for small to medium, monthly for large	Track and record by online vs. retail vs. mobile (option to access records is not online)
Access (Online)	Number of requests generated by customers/consumers requesting access to their records	Quarterly for small to medium, monthly for large	Track and record by online vs. retail vs. mobile (option to access records is online)
Choice	Number of calls generated by customers/consumers requesting to opt-out	2x/month for small to medium, weekly for large	Track and record by online vs. retail vs. mobile

Discipline	Measurement	Frequency	Comments
Data Protection or Safeguards	Validation of encryption of personal data at point collection and transfer	Launch or updates to online or mobile applications	Coordinate with development team to include privacy as part of product/service launch. Partner with InfoSec to test and report findings.
Training	Recording of number of employees, contractors and vendors that have completed privacy training	Annual	Organizations that have fundamental and role based training should measure and record separately
Governance	Executive Briefings	Quarterly	Review the privacy metrics, secure support for future activity and raise awareness on areas of concern
Governance	Number of regulator inquiries and individual complaints	Quarterly	Individual privacy complaints received via email, calls and post; inquires by regulators by country of type (choice, access, correction, breach)
Privacy Impact Assessment (PIAs)	Number of planned vs actual PIAs	Quarterly	Prioritize by systems or databases that contain sensitive personal data (financial, medical, criminal) and highest volume of records

Table B

Discipline	Measurement	Frequency	Comments
System Access	Validation of number and role (if feasible) of users by employee and contractor	Semi-annual	Partner with Procurement and HR to provide the number of employees and contractors, work with IT to pull access rights
Retention	Validation that records and data are in compliance with the retention schedule	Semi-annual	Start with highest risk areas, such the unstructured environment and expand to structured systems (usually greater security controls)
Encryption	Assessment of the percentage of data that is encrypted in motion, at rest, number of laptops	Quarterly	Partner with InfoSec for validation of encryption at Ingress and Egress points, random sampling (5-10%) of systems encryption, IT provide number of laptops encrypted vs unencrypted

Discipline	Measurement	Frequency	Comments
Breach	Number of records that have been lost, unauthorized access or stolen, rolling 24 months, tracking of reduction or increase from previous quarters	Quarterly for small to medium, monthly for large	Track and record by online vs. retail vs. mobile (option to access records is online)
Compliance	Number of calls generated by customers/consumers requesting to opt-out	Recommended 2x/month for small to medium, weekly for large	Track and record by online vs. retail vs. mobile
Awareness	Validation of call center and/or front line associate (if applicable) privacy knowledge (assessment of choice, access and correction)	Quarterly	Scheduled monthly calls to agents or associates, roll up monthly findings to a quarterly report
Privacy Impact Assessment (PIAs)	Validation of privacy functionality for high risk systems, number of gaps identified, include number open vs. closed	Annually	Supplement resource effort by using 3rd party privacy consultants or Internal Audit to measure and record findings
Accuracy	Number of emails or SMS communications bounced back or send failure (invalid email address or non- functional mobile number)	Quarterly	Work with IT or procurement to define process and secure reports
Regulatory	Number of applicable regulations, changes and additions	Quarterly	Original effort identify number of applicable regulations, then tracking regulatory changes and additions on a rolling 24 month period
Governance	Number of partners or clients requiring a documented and measured privacy program	Quarterly	Work with procurement and the business to track the number of companies that request evidence of a privacy program

Conclusions

A measurement and metrics program assists the Privacy Office in understanding the level of regulatory compliance, costs, potential harm and risks to the individual and business. The program should be documented to include the objective, frequency and identify who will receive the results.

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. This may create additional financial, civil or criminal risks to the organization and the executives.