UPDATED FEBRUARY 2014

Nymity Privacy Management Accountability Framework™

NYMITY

1. Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities

- Maintain job descriptions for individuals responsible for data privacy (e.g. data protection officers)
- Assign accountability for data privacy at a senior level
- Allocate resources to adequately implement and support the privacy program (e.g. budget, personnel)
- Appoint a representative in member states where the organization does not maintain a physical presence
- Conduct regular communication between individuals accountable and responsible for data privacy
- Consult with stakeholders throughout the organization on data privacy matters
- Maintain a Code of Conduct
- Report, on a scheduled basis, on the status of the privacy program (e.g. board of directors, management board)
- Integrate data privacy into business risk assessments/reporting
- Conduct a Privacy Risk Assessment
- Assign responsibility for data privacy
- Maintain a privacy program charter/mission statement
- Maintain ethics guidelines
- Maintain a strategy to align activities with legal requirements (e.g., address conflicts, differences in standards, creating rationalized rule sets)
- Require employees to acknowledge and agree to adhere to the data privacy policies
- Report periodically on the status of the privacy program to external stakeholders, as appropriate (e.g. annual reports, third-parties, clients)
- Maintain a Privacy Strategy

2. Maintain Personal Data Inventory

Maintain an inventory of the location of key personal data storage or personal data flows with defined classes of personal data

Privacy Management Activities

- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain approval for data processing (where prior approval is required)
- Register databases with data protection authority (where registration is required)
- Maintain documentation for all cross-border data flows (e.g. country, mechanism used as a basis for the transfer such as Safe Harbor, model clauses, binding corporate rules, or approvals from data protection authorities)
- Maintain an inventory of key personal data holdings (what personal data is held and where)
- Maintain flow charts for key data flows (e.g. between systems, between processes, between countries)
- Use Binding Corporate Rules as a data transfer mechanism
- Use Standard Contractual Clauses as a data transfer mechanism
- Use Cross-Border Privacy Rules as a data transfer mechanism
- Use the Safe Harbor framework as a data transfer mechanism
- Use Data Protection Authority approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

3. Maintain Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk

Privacy Management Activities

- Maintain a data privacy policy
- Maintain a separate employee data privacy policy
- Obtain board approval for data privacy policy
- Document legal basis for processing personal data
- Document guiding principles for consent

4. Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for pseudonymization/anonymization of personal data
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for collecting and honouring consent preferences
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into behavioural advertising practices
- Integrate data privacy into hiring practices
- Integrate data privacy into employee background check practices
- Integrate data privacy into social media practices
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into e-mail monitoring practices
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into delegate access to employees' company e-mail accounts (e.g. vacation, LOA, termination)
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into customer/patient/citizen facing practices (e.g. retail sales, provision of healthcare, tax processing)
- Integrate data privacy into back office/administrative procedures (e.g. facilities management)
- Integrate data privacy into financial operations (e.g. credit, billing, processing transactions)
- Integrate data privacy into research practices
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures

5. Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities

- Conduct training for newly appointed employees upon assignment to privacy-sensitive positions
- Maintain a core training program for all employees
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Conduct regular refresher training to reflect new developments
- Maintain a second level training program reflecting job specific content
- Integrate data privacy into other training programs, such as HR, security, call centre, retail operations training
- Provide ongoing education and training for the privacy office (e.g. conferences, webinars, guest speakers)
- Conduct data privacy training needs analysis by position/job responsibilities
- Conduct one-off, one-time tactical training and communication dealing with specific, highly-relevant issues/topics
- Maintain an internal data privacy intranet, privacy blog, or repository of privacy FAQs and information
- Maintain ongoing awareness material (e.g. posters, intranet, and videos)
- Hold an annual data privacy day/week
- Measure comprehension of data privacy concepts using exams
- Measure participation in data privacy training activities (e.g. numbers of participants, scoring)
- Require completion of data privacy training as part of performance reviews
- Provide data privacy information on system logon screens
- Maintain certification for individuals responsible for data privacy, including continuing professional education

6. Manage Information Security Risk

Maintain an information security program based on legal requirements and ongoing risk assessments

Privacy Management Activities

- Maintain an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain administrative and technical measures to encrypt personal data in transmission and at rest, including removable media
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal information (e.g. role-based access, segregation of duties)
- Conduct a security risk assessment which considers data privacy risk
- Maintain a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Maintain backup and business continuity plans
- Maintain a data-loss prevention strategy
- Maintain procedures to update security profile based on system updates and bug fixes
- Conduct regular testing of data security posture
- Maintain a security verification

7. Manage Third-Party Risk

Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain data privacy requirements for vendors
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Maintain a vendor data privacy risk assessment process
- Use standard contractual clauses for disclosures to third-parties
- Maintain a policy governing use of cloud providers
- Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors based on a risk assessment
- Review long-term contracts for new or evolving data protection risks

8. Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain a data privacy notice that details the organization's personal data handling policies
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in all forms, contracts, and terms
- Maintain scripts for use by employees to provide the data privacy notice
- Maintain a data privacy notice for employees (processing of employee personal data)
- Maintain a privacy Seal or Trustmark to increase customer trust
- Provide data privacy education to individuals (e.g. preventing identity theft)

9. Maintain Procedures for Inquiries and Complaints

Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities

- Maintain procedures to address complaints
- Maintain procedures to respond to access requests
- Maintain procedures to respond to requests to update or revise personal data
- Maintain procedures to respond to requests to opt-out
- Maintain procedures to respond to requests for information
- Maintain customer Frequently Asked Questions
- Maintain escalation procedures for serious complaints or complex access requests
- Maintain procedures to investigate root causes of data protection complaints
- Maintain metrics for data protection complaints (e.g. number, root cause)

10. Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities

- Maintain a Privacy by Design framework for all system and product development
- Maintain PIA guidelines and templates
- Conduct PIAs for new programs, systems, processes
- Maintain a procedure to address data protection issues identified during PIAs
- Maintain a product sign-off procedure that involves the privacy office
- Maintain a product life cycle process to address privacy impacts of changes to existing programs, systems, or processes
- Maintain metrics for PIAs (e.g. number completed, turnaround time)

11. Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

Privacy Management Activities

- Maintain a documented data privacy incident/breach response protocol
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) and protocol
- Maintain a breach incident log to track nature/type of all breaches
- Maintain data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of breach protocol and document findings and changes made
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage
- Maintain a record preservation protocol to protect relevant log history

12. Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures

Privacy Management Activities

- Conduct self-assessments managed by the privacy office
- Conduct ad-hoc audits/assessments based on complaints/inquiries/breaches
- Conduct audits/assessments of the privacy program outside of the privacy office (e.g. Internal Audit)
- Benchmark results of audits/assessments (e.g. comparison to previous audit, comparison to other business units)
- Conduct ad-hoc walk-throughs
- Conduct assessments through use of an accountability agent or third-party verification
- Maintain privacy program metrics

13. Track External Criteria

Track new compliance requirements, expectations, and best practices

Privacy Management Activities

- Conduct ongoing research on developments in law
- Maintain subscription to compliance reporting service/law firm updates to stay informed on new developments
- Attend/participate in privacy conferences, industry associations, or think-tank events
- Record/report on the tracking of new Rule Sources or amendments to Rule Sources
- Seek legal opinions regarding recent developments in law
- Document that new requirements have been implemented (also document where a decision is made to not implement any changes, including reason)
- Maintain records or evidence that alerts are read and actions are taken (e.g. read daily and forwarded to key individuals as required)
- Review or participate in studies related to best practices in data privacy management

The Privacy Management Accountability Framework™ was developed based on Nymity's global research on data privacy accountability.
The Privacy Management Activities™ are common to organizations across jurisdictions, industries, and sectors.