UPDATED SEPT 2023

# PRIVACY MANAGEMENT ACCOUNTABILITY FRAMEWORK™

*A Practical and Operational Structure for Complying with the World's Privacy Requirements*

NYMITY POWERED BY TrustArc

## 1 Maintain Governance Structure

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

### PRIVACY MANAGEMENT ACTIVITIES

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network, and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Integrate privacy into the Data Ethics/Stewardship program
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Manage enterprise privacy risk consistent with organizational objectives
- Integrate data privacy into business risk assessments/reporting
- Align privacy strategy with organizational objectives
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

## 2 Maintain Personal Data Inventory and Data Transfer Mechanisms

Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

### PRIVACY MANAGEMENT ACTIVITIES

- Maintain an inventory of personal data and/or processing activities
- Classify personal data by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain documentation of data flows (e.g. between systems, between processes, between countries)
- Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approvals)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use the Data Privacy Framework as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

## 3 Maintain Internal Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

### PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

## 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 collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for algorithmic accountability
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- 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 digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- 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 use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate privacy into the System Development Life Cycle
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- 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 research practices (e.g. scientific and historical research)

## 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 privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training (e.g. HR, marketing, call center)
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain qualifications for individuals responsible for data privacy, including certifications

## 6 Manage Information Security Risk

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

### PRIVACY MANAGEMENT ACTIVITIES

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into the information security program
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO, NIST, SOC)

## 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 defined roles and responsibilities for third parties (e.g. partners, vendors, processors, customers)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a third party data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct due diligence around the data privacy and security posture of existing vendors/processors
- Review long-term contracts for new or evolving data privacy 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
- 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 contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust

## 9 Respond to Requests and Complaints from Individuals

Maintain effective procedures for interactions with individuals about their personal data

### PRIVACY MANAGEMENT ACTIVITIES

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for accounting for disclosures, transfers and sharing of data
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Obtain feedback from individuals about privacy
- Monitor and report metrics for data privacy 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

- Integrate Privacy by Design into data processing operations
- Maintain PIA/DPIA guidelines and templates
- Conduct Impact Assessments for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

## 11 Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

### PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

## 12 Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

### PRIVACY MANAGEMENT ACTIVITIES

- Conduct self-assessments of privacy management
- Monitor effectiveness of privacy controls
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Use interoperable frameworks to monitor and report on privacy risks
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

## 13 Track External Criteria

Track new compliance requirements, expectations, and best practices

### PRIVACY MANAGEMENT ACTIVITIES

- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

*The Privacy Management Accountability Framework(™) was developed based on Nymity's global research on data privacy accountability.*
*The Framework is a comprehensive listing of over 130 Privacy Management Activities (PMAs) categorized into 13 Privacy Management Categories (PMCs).*

TrustArc

# Data Privacy Management Expertise & Automation

TrustArc's all-in-one data privacy management solution makes it easy for your company to access and manage data while ensuring you remain compliant with global privacy regulations. By combining the right advice, governance, operations, and technology, TrustArc helps you scale your compliance using automation to maximize customer trust.

***Find out more at TrustArc.com***

***Download and share this guide***