PRIVACY MANAGEMENT ACTIVITIES

1. Maintain Governance Structure
   - Ensure that there is an individual responsible for data privacy, accountable management, and management reporting procedures.

2. Maintain Personal Data Inventory and Data Transfer Mechanisms
   - Collect personal data by type (e.g., sensitive, confidential, public).
   - Obtain or register approval for data processing (where prior approval is required).
   - Regularly update data schedules with regulated data (where regulation is required).
   - Maintain documentation of data transfer mechanisms (across businesses, between countries).
   - Maintain documentation of the mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approval).

3. Maintain Internal Data Privacy Policy
   - Maintain a data privacy policy.
   - Maintain an employee data privacy policy.
   - Maintain an organizational code of conduct that includes privacy.

4. Embed Data Privacy Into Operations
   - Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives.

5. Maintain Training and Awareness Program
   - Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks.

6. Manage Information Security Risk
   - Maintain an information security risk program based on legal requirements and ongoing risk assessments.

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.

8. Maintain Notices
   - Provide notice at all points where personal data is collected.
   - Provide notice in marketing communications (e.g., emails, flyers, offers).

9. Respond to Requests and Complaints from Individuals
   - Maintain effective procedures for interactions with individuals about their personal data.

10. Monitor for New Operational Practices
    - Integrate Privacy by Design into data processing operations.
    - Maintain PIAs/DPIAs to address new programs, systems, processes.

11. Data Privacy Incident/Breach Response Plan
    - Conduct periodic testing of data privacy incident/breach plan.
    - Engage a breach response remediation provider.

12. Data Privacy Breach Management Program
    - Maintain an effective data privacy incident and breach management program.

13. Track External Criteria
    - Track compliance requirements, expectations, and best practices.

LEGEND: Activities mapped to GDPR to demonstrate compliance

---

The Nymity Privacy Management Accountability Framework (™) was developed based on Nymity’s global research on data privacy accountability.

Copyright © 2018 by Nymity Inc. All rights reserved. All text, images, logos, trademarks and information contained in this document are the intellectual property of Nymity Inc. unless otherwise indicated. Reproduction, modification, transmission, use, or quotation of any content, including text, images, photographs etc., requires the prior written permission of Nymity Inc. Requests may be sent to info@nymity.com.