Working Towards Data Privacy Resilience in Government

NATIONAL PRIVACY COMMISSION
MARCH 14, 2018
Data Privacy Act Checklist - Signs of Compliance

Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

Appoint an individual accountable for compliance

- Notarized designation of a DPO/COP, filed with the NPC
- Evidence that DPO/COP recommendations are taken into consideration when making decisions
- Contact details are easy to find (e.g. on website)
- Continuing education program for the DPO/COP
Data Privacy Act Checklist – Possible Signs of Negligence

Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

- Ineffective data protection governance
- No DPO or COP (in which case CEO or HoA is the default DPO)
- Lack of interaction between DPO/COP and top management
- Lack of interaction between DPO/COP and functional units
- Communication from the DPO/COP is largely ignored

No continuing education program for the DPO/COP
THE NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

I. Establishing Data Privacy Governance

1. Appointment of your Data Privacy Officer (DPO)

II. Risk Assessment

2. Register

3. Records of processing activities

4. Conduct of a Privacy Impact Assessment (PIA)

III. Preparing Your Organization’s Data Privacy Rules

5. Formulate your organization’s privacy management program (PMP)

6. Craft your agency’s privacy manual

IV. Privacy in Day-to-Day Information Life Cycle Operations (To Be Included in the Privacy Manual)

7. Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)

8. Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them

9. Policies for limiting data processing according to its declared, specified and legitimate purpose

10. Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)

11. Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures to keep the same up to date

12. Policies/procedures that allow a data subject to suspend withdraw or order the blocking, removal or destruction of their personal information

13. Policies/procedures for accepting and addressing complaints from data subjects

14. Policies/procedures that allow data subjects to get indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false and unlawfully obtained or unauthorized use of personal information.

15. Policies/procedures that allow data subjects to obtain from the personal information controller a copy of his or her personal data processed by electronic means and in a structured and commonly used format

16. Policies/procedures for creation and collection, storage, transmission, use and distribution, retaining personal data for only a limited period or until the purpose of the processing has been achieved, and ensuring that data is securely destroyed or disposed of

V. Managing Personal Data Security Risks

17. Implement appropriate and sufficient organizational security measures (Policies and procedures in place)

18. Implement appropriate and sufficient physical security measures (Physical Access and Security, Design and Infrastructure)

19. Implement appropriate and sufficient technical security measures (Firewalls, Encryption, Access Control Policy, Security of Data Storage, and Other Information Security Tools)

VI. Data Breach Management

20. Compliance with the DPA’s Data Breach and Data Breach Management Requirements (e.g. Security Policy, Data Breach Response Team, Incident Response Procedure, Document, Breach Notification)

VII. Managing Third Party Risks

21. Maintaining data privacy requirements (Legal Basis for Disclosure, Data Sharing Agreements, Cross Border Security of Transfers for third parties e.g. clients, vendors, processors, affiliates)

VIII. Managing Human Resources (HR)

22. Periodic and mandatory personnel training on privacy and data protection in general and in areas reflecting job-specific content

23. Issuance of Security Clearance for those handling personal data

IX. Continuing Assessment and Development

24. Scheduling of Regular PIA for new and existing programs, systems, processes and projects

25. Review of Forms, Contracts, Policies and Procedures on a regular basis

26. Scheduling of Regular Compliance Monitoring, Internal Assessments and Security Audits

27. Review, validation and update of Privacy Manual

28. Regular evaluation of Privacy Management Program

29. Establishing a culture of privacy by obtaining certifications or accreditations vis-à-vis existing international standards

X. Managing Privacy Ecosystem

30. Monitoring of emerging technologies, new risks of data processing, and the Privacy Ecosystem

31. Keeping track of data privacy best practices, sector specific standards, and international data protection standards

32. Seeking guidance and legal opinion on new National Privacy Commission (NPC) issuances or requirements
DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE
A. Choose a DPO

II. RISK ASSESSMENT
B. Register
C. Records of processing activities
D. Conduct PIA

III. ORGANIZATION
E. Privacy Management Program
F. Privacy Manual

IV. DAY TO DAY
G. Privacy Notice
H. O. Data Subject Rights
P. Data Life Cycle

V. DATA SECURITY
Q. Organizational
R. Physical
S. Technical
   ▶ Data Center
   ▶ Encryption
   ▶ Access Control Policy

VI. BREACHES
T. Data Breach Management:
   ▶ Security Policy
   ▶ Data Breach Response Team
   ▶ Incident Response Procedure
   ▶ Document
   ▶ Breach Notification

VII. THIRD PARTIES
U. Third Parties;
   ▶ Legal Basis for Disclosure
   ▶ Data Sharing Agreements
   ▶ Cross Border Transfer Agreement

VIII. MANAGE HR
V. Trainings and Certifications
   w. Security Clearance

IX. CONTINUITY
X. Continuing Assessment and Development
   ▶ Regular PIA
   ▶ Review Contracts
   ▶ Internal Assessments
   ▶ Review PMP
   ▶ Accreditations

X. PRIVACY ECOSYSTEM
Y. New technologies and standards
Z. New legal requirements
THE 90 DAY PLAN
30 DAYS
I. GOVERNANCE

Choose a DPO
Register
# I. GOVERNANCE

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointment of your Data Privacy Officer (DPO)</td>
<td>Designation / Appointment Papers / Contract of the DPO and / or DPO team</td>
</tr>
<tr>
<td>Register Data Processing Systems (Phase I &amp; Phase 2)</td>
<td>Website or other visible announcement showing contact details of DPO</td>
</tr>
<tr>
<td></td>
<td>NPC Notification of completing Registration</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
II. RISK ASSESSMENT

Conduct PIA
## II. RISK ASSESSMENT

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain records of processing activities, including inventory of personal data, data flow and transfers outside country</td>
<td>Records of Processing Activities</td>
</tr>
<tr>
<td>Conduct a Privacy Impact Assessment (PIA) including baselining (Personal Data Inventory)</td>
<td>PIA Report</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
III. ORGANIZATION

Privacy Management Program
Privacy Manual
<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement and Maintain a Privacy Management Program (PMP)</td>
<td>Privacy Manual</td>
</tr>
<tr>
<td>Develop a Privacy Manual</td>
<td>List of activities on privacy and data protection</td>
</tr>
<tr>
<td></td>
<td>List of key personnel assigned responsibilities for privacy and data protection within The organization</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
60 DAYS
IV. DAY TO DAY OPERATIONS

Privacy Notice
Data Subject Rights
Retention
Disposal
## IV. DAY TO DAY OPERATIONS

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have visible and accessible Privacy Notices with contact details of DPO</td>
<td>Privacy Notice in Website and/or within organization (where collection of personal data occurs)</td>
</tr>
<tr>
<td>Develop, Review or Maintain Policies and Procedures for processing of</td>
<td>Consent forms for collection and use of personal data</td>
</tr>
<tr>
<td>personal data from collection to retention or disposal (procedure for</td>
<td>List of Policies and Procedures in place that relate to privacy and data protection (may be in</td>
</tr>
<tr>
<td>obtaining consent)</td>
<td>privacy manual)</td>
</tr>
<tr>
<td>Establish procedures or platform for data subjects to exercise their</td>
<td>Policies and Procedures in dealing with requests for information from parties other than the data</td>
</tr>
<tr>
<td>rights (access, correction erasure, data portability)</td>
<td>subjects (media, law enforcement, representatives)</td>
</tr>
<tr>
<td>Comply with notification and reporting requirements</td>
<td>Retention and Disposal Schedules</td>
</tr>
</tbody>
</table>
### IV. DAY TO DAY OPERATIONS

**Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)**

**Formulation of policies/procedures that allow data subjects to object to subsequent processing or changes to the information supplied to them**

**Policies for limiting data processing according to its declared, specified and legitimate purpose?**

**Policies/procedures for providing data subjects with access to their personal information including its sources, recipients, method of collection, purpose of disclosure to third parties, automated processes, date of last access, and identity of the controller (Data Subject Access Request)**

**Policies/procedures that allow data subjects to dispute inaccuracy or error of their personal information including policies/procedures the same up to date**

**Policies/procedures that allow a data subject to suspend, withdraw or order the blocking, removal or destruction of their personal information**

**Policies/procedures for accepting and addressing complaints from data subjects**

**Policies/procedures for retaining personal data for only a limited period or until the purpose of the processing has been achieved**

**Policies/procedures for ensuring that data is securely destroyed or disposed of**

---

**CREATION AND COLLECTION**

**STORAGE, TRANSMISSION, USE AND DISTRIBUTION**

**RETENTION**

**DESTRUCTION/DISPOSITION**
V. DATA SECURITY

Data Center
Encryption
Access Policy
Transfers
### V. DATA SECURITY

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain Organizational Security Measures (Policies and procedures in place)</td>
<td>Data Center and Storage area with limited physical access</td>
</tr>
<tr>
<td>Maintain Physical Security Measures (Physical Access and Security, Design and Infrastructure)</td>
<td>Report on technical security measures and information security tools in place</td>
</tr>
<tr>
<td>Maintain Technical Security Measures (Firewalls, Encryption, Access Policy, Security of Transfers and Storage of Data, other Information security tools)</td>
<td>Firewalls used</td>
</tr>
<tr>
<td></td>
<td>Encryption used for transmission</td>
</tr>
<tr>
<td></td>
<td>Encryption used for storage</td>
</tr>
<tr>
<td></td>
<td>Access Policy for onsite, remote, and online access</td>
</tr>
<tr>
<td></td>
<td>Audit logs</td>
</tr>
<tr>
<td></td>
<td>Back-up solutions</td>
</tr>
<tr>
<td></td>
<td>Report of Internal Security Audit or other internal assessments</td>
</tr>
<tr>
<td></td>
<td>Certifications or accreditations maintained</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
VI. BREACHES

Breach Management
Assessment
Monitoring
Response Team
Review
Notification
## VI. BREACHES

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement safeguards to prevent or minimize personal data breach (Breach drills, security policy)</td>
<td>Schedule of breach drills</td>
</tr>
<tr>
<td>Constitute Data Breach Response Team</td>
<td>Number of Trainings conducted for internal personnel on breach management</td>
</tr>
<tr>
<td>Maintain and Review Incident Response Policy and Procedure</td>
<td>Personnel Order constituting the Data Breach Response Team</td>
</tr>
<tr>
<td>Document Security Incidents and personal data breaches</td>
<td>Incident Response Policy and Procedure (may be in Privacy Manual)</td>
</tr>
<tr>
<td>Comply with Breach Notification requirements</td>
<td>Record of Security incidents and personal data breaches, including notification for personal data breaches</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
90 DAYS
VII. THIRD PARTIES

Due Diligence
Agreements
Notification
Access Policy
## VII. THIRD PARTIES

### Framework

<table>
<thead>
<tr>
<th>Execute Data Sharing Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review or Enter into contracts and other agreements for transfers of personal data, including cross border transfers, to ensure comparable level of data protection and DPA compliance</td>
</tr>
<tr>
<td>Review or enter into outsourcing contracts with PIPs, to ensure comparable level of data protection and DPA compliance</td>
</tr>
<tr>
<td>Establish and document legal basis for disclosures of personal data made to third parties</td>
</tr>
</tbody>
</table>

### Demonstrate Compliance (Output/Evidence)

<table>
<thead>
<tr>
<th>Data Sharing Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of recipients of personal data (PIPs, other PICs, service providers, government agencies)</td>
</tr>
<tr>
<td>Review of Contracts with PIPs</td>
</tr>
<tr>
<td>Review of Contracts for cross-border transfers</td>
</tr>
<tr>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
Training
## VIII. MANAGE HR

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regularly train personnel regarding privacy or security policies</td>
<td>Number of employees who attended trainings on privacy and data protection</td>
</tr>
<tr>
<td>Ongoing training and capacity building for Data Protection Officer</td>
<td>Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files</td>
</tr>
<tr>
<td>DPOs work towards certifications and applies for membership in DPO organizations</td>
<td>Certificate of Training of DPO</td>
</tr>
<tr>
<td>Non-Disclosure Agreements for personnel handling Data</td>
<td>Certifications of DPOs</td>
</tr>
<tr>
<td>Security Clearance issued for those handling personal data</td>
<td>NDAs or confidentiality agreements</td>
</tr>
<tr>
<td></td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
IX. PROJECTS

Conduct and Update PIA
## IX. PROJECTS

<table>
<thead>
<tr>
<th>Framework</th>
<th>Demonstrate Compliance (Output/Evidence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Regular PIA</td>
<td>Policy for Conduct of PIA (may be in manual)</td>
</tr>
<tr>
<td>Review Forms, Contracts, Policies and Procedures on a regular basis</td>
<td>Policy on conduct of Internal Assessments and Security Audits</td>
</tr>
<tr>
<td>Schedule Regular Compliance monitoring, internal assessments, and security audits</td>
<td>Privacy Manual contains policy for regular review</td>
</tr>
<tr>
<td>Review, Validate and Revise Privacy Manual</td>
<td>List of activities to evaluate Privacy Management Program (survey of customer, personnel assessment)</td>
</tr>
<tr>
<td>Regularly evaluate Privacy Management Program</td>
<td>Other means to demonstrate compliance</td>
</tr>
</tbody>
</table>
X. MANAGE LEGAL COMPLIANCE

Monitor Legal Compliance

Contract Review
## X. MANAGE LEGAL COMPLIANCE

### Framework
- Monitor emerging technologies, new risks of data processing, and the legal and ICT Environment
- Keep track of data privacy best practices, sector specific standards, and international data protection standards
- Attend trainings and conferences
- Seek guidance and legal opinion on new NPC Issuances or requirements

### Demonstrate Compliance (Output/Evidence)
- Number of trainings and conferences attended on privacy and data protection
- Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards
- Number of management meetings which included privacy and data protection in the agenda
- Other means to demonstrate compliance