Working Towards Data Privacy Resilience in Government

NATIONAL PRIVACY COMMISSION

MARCH 14, 2018

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 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	CREATION AND COLLECTION, STORAGE, TRANSMISSION, USE AND DISTRIBUTION, RETENTION, AND DESTRUCTION/ DISPOSAL
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	

THE NPC'S 32-Pt. DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE CHECKLIST

20. Compliance with the DPA's 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

A. Choose a DPO

B. Register
C. Records of processing activities
D. Conduct PIA

E. Privacy Management Program
F. Privacy Manual

G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy

T. Data Breach Management;
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Document
- Breach Notification

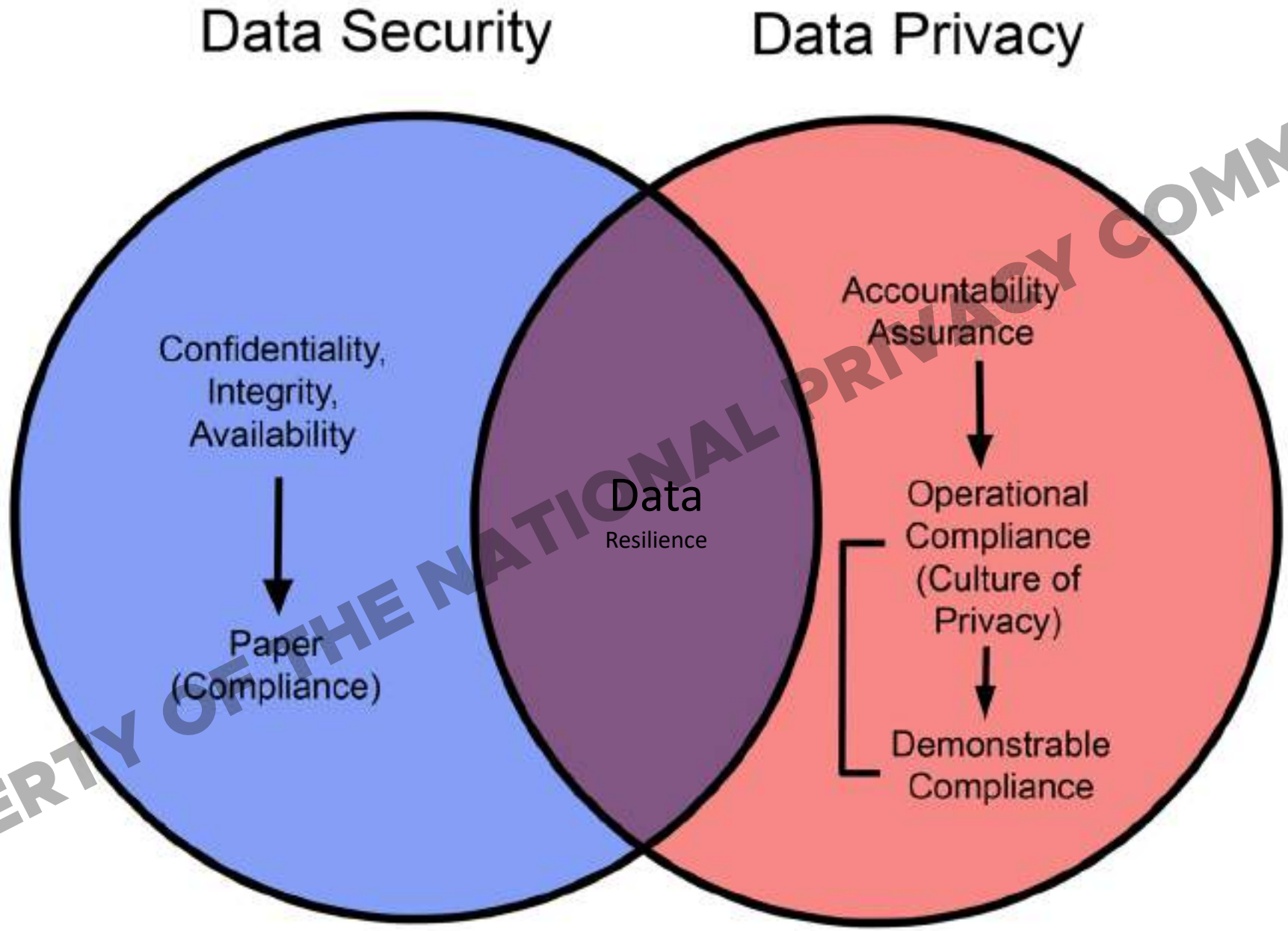
U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

V. Trainings and Certifications
W. Security Clearance

X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

Y. New technologies and standards
Z. New legal requirements

NATIONAL PRIVACY COMMISSION



THE 90 DAY PLAN

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

30 DAYS

I. GOVERNANCE

Choose a DPO Register

I. GOVERNANCE

Framework	Demonstrate Compliance (Output/Evidence)
Appointment of your Data Privacy Officer (DPO)	Designation / Appointment Papers / Contract of the DPO and / or DPO team
Register Data Processing Systems (Phase I & Phase 2)	Website or other visible announcement showing contact details of DPO
	NPC Notification of completing Registration
	Other means to demonstrate compliance

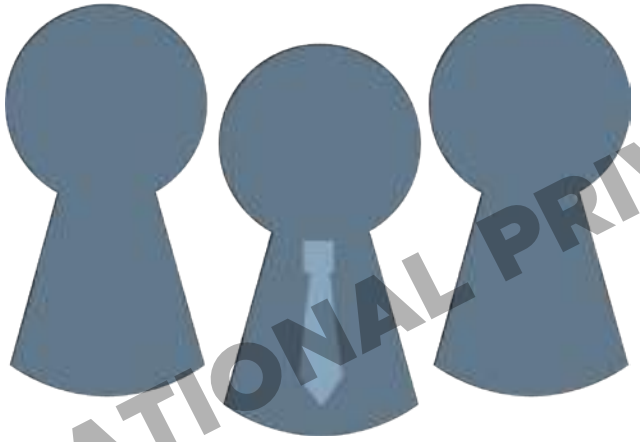
II. RISK ASSESSMENT

Conduct PIA

II. RISK ASSESSMENT

Framework	Demonstrate Compliance (Output/Evidence)
Maintain records of processing activities, including inventory of personal data, data flow and transfers outside country	Records of Processing Activities
Conduct a Privacy Impact Assessment (PIA) including baselining (Personal Data Inventory)	PIA Report
	Other means to demonstrate compliance

III. ORGANIZATION



Privacy Management Program
Privacy Manual

III. ORGANIZATION

Framework
Implement and Maintain a Privacy Management Program (PMP)
Develop a Privacy Manual

Demonstrate Compliance (Output/Evidence)
Privacy Manual
List of activities on privacy and data protection
List of key personnel assigned responsibilities for privacy and data protection within The organization
Other means to demonstrate compliance

60 DAYS

IV. DAY TO DAY OPERATIONS

Privacy Notice
Data Subject Rights
Retention
Disposal

IV. DAY TO DAY OPERATIONS

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

IV. DAY TO DAY OPERATIONS

Informing data subjects of your personal information processing activities and obtain their consent, when necessary. (Privacy Notice)	**CREATION AND COLLECTION**
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?	**STORAGE, TRANSMISSION, USE AND DISTRIBUTION**
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	**RETENTION**
Policies/procedures for ensuring that data is securely destroyed or disposed of	**DESTRUCTION/DISPOSAL**

V. DATA SECURITY

Data Center
Encryption
Access Policy
Transfers

V. DATA SECURITY

Framework
Maintain Organizational Security Measures (Policies and procedures in place)
Maintain Physical Security Measures (Physical Access and Security, Design and Infrastructure)
Maintain Technical Security Measures (Firewalls, Encryption, Access Policy, Security of Transfers and Storage of Data, other Information security tools)

Demonstrate Compliance (Output/Evidence)
Data Center and Storage area with limited physical access
Report on technical security measures and information security tools in place
Firewalls used
Encryption used for transmission
Encryption used for storage
Access Policy for onsite, remote, and online access
Audit logs
Back-up solutions
Report of Internal Security Audit or other internal assessments
Certifications or accreditations maintained
Other means to demonstrate compliance

VI. BREACHES

Breach Management

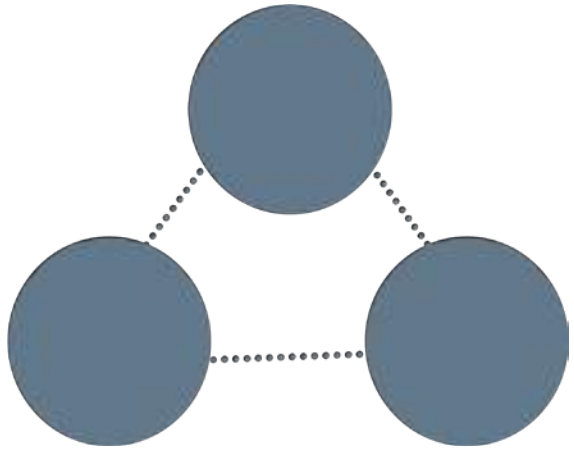
- Assessment
- Monitoring
- Response Team
- Review
- Notification

VI. BREACHES

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

90 DAYS

VII. THIRD PARTIES



Due Diligence
Agreements
Notification
Access Policy

VII. THIRD PARTIES

Framework
Execute Data Sharing Agreements
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
Review or enter into outsourcing contracts with PIPs, to ensure comparable level of data protection and DPA compliance
Establish and document legal basis for disclosures of personal data made to third parties

Demonstrate Compliance (Output/Evidence)
Data Sharing Agreements
List of recipients of personal data (PIPs, other PICs, service providers, government agencies)
Review of Contracts with PIPs
Review of Contracts for cross-border transfers
Other means to demonstrate compliance

VIII. MANAGE HR

Training

VIII. MANAGE HR

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

IX. PROJECTS

Conduct and Update PIA

IX. PROJECTS

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

X. MANAGE LEGAL COMPLIANCE

Monitor Legal Compliance

Contract Review

X. MANAGE LEGAL COMPLIANCE

Framework	Demonstrate Compliance (Output/Evidence)
Monitor emerging technologies, new risks of data processing, and the legal and ICT Environment	Number of trainings and conferences attended on privacy and data protection
Keep track of data privacy best practices, sector specific standards, and international data protection standards	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
Attend trainings and conferences	Number of management meetings which included privacy and data protection in the agenda
Seek guidance and legal opinion on new NPC Issuances or requirements	Other means to demonstrate compliance