Data Protection Starter Kit Checklist

This checklist provides a guide for organisations in the *implementation of accountable data protection practices* in the management of personal data under its possession or control. It references the following PDPC guides

- Guide to Developing a Data Protection Management Programme (DPMP) (www.pdpc.gov.sg/DPMP)
- Guide to Managing Data Breaches 2.0 (www.pdpc.gov.sg/Managing-Data-Breaches)
- Guide to Data Protection Impact Assessments (www.pdpc.gov.sg/DPIA)

Organisations may also consider Data Protection-as-a-Service for SMEs (DPaaS@SMEs) Providers registered with IMDA to implement the DPaaS@SMEs Package in Section 1 and Section 2.

SECTION 1: DPAAS@SMES PACKAGE (ONE-TIME SETUP)		
A. Data Protection Management		
Step	**Description**	**Resources/ References**
1.	Appoint a DPO and business contact information is made available to the public ☐	For ACRA-registered entities, organisations may register in ACRA BizFile⁺ (www.bizfile.gov.sg). For non ACRA-registered entities, organisations may register the DPO with PDPC (www.pdpc.gov.sg/dpo-registration). Refer to *Appendix I* for instructions to register DPO on ACRA BizFile⁺ and sample website notice on making available the business contact information of DPOs.
2.	Identify risks and gaps using PDPA Assessment Tool for Organisations (PATO) ☐	Refer to the PDPA Assessment Tool for Organisations (PATO) (www.pdpc.gov.sg/PATO) to identify, evaluate, rectify and improved current gaps with regards to the management of personal data.
3.	Develop a Data Protection (DP) Policy ☐	Refer to *Appendix II* for the DP Policy (Sample). For Steps 4 to 10, references will be made to the relevant annexes in the sample DP Policy (Sample).
4.	Embed data protection as part of corporate governance and establish a reporting structure for data protection matters ☐	Refer to *ANNEX A-1* of the DP Policy (Sample) for a sample corporate reporting structure. Additional references can be found under "**Policy**" section in the DPMP.

Data Protection Starter Kit Checklist

5.	Embed regular monitoring and reporting mechanisms within Enterprise Risk Management (ERM) Framework	☐	Refer to *ANNEX A-2* of the DP Policy (Sample) for the Enterprise Risk Management Framework. Additional references can be found under **"Good DP Practices"** section in the DPMP.
6.	Document data assets and flows using a Data Inventory Map	☐	Refer to *ANNEX B* of the DP Policy for Data Inventory Map Templates. Additional references can be found under **"Process"** section in the DPMP.
B. Data Breach Management			
7.	Establish a data breach management team	☐	Refer to *ANNEX G* of the DP Policy (Sample) for the Data Breach Management Plan (Sample) which will include
8.	Develop a complaint handling procedure	☐	• Data breach management team composition template; • Complaint Handling Procedure (Sample); and
9.	Develop a 4-step action plan for data breach response (using C.A.R.E model)	☐	• Breach Incident Response Plan. Additional references can be found in the Guide to Managing Data Breaches 2.0.
C. Training and Communications			
10.	Develop a staff training and communications plan	☐	Refer to *ANNEX H* of the DP Policy (Sample) for the Training and Communications plan (Sample).
11.	Mandate all staff to complete the PDPA E-Learning Programme	☐	Refer to the PDPA E-Learning Programme for all staff (www.pdpc.gov.sg/elearning)
12.	Identify key personnel to attend the 2 PDPC courses if they do not possess any prior data protection certifications listed in the DPO Competency Framework and Training Roadmap	☐	The 2 PDPC courses are: • Fundamentals of Personal Data Protection Act (www.pdpc.gov.sg/fundamentals-of-pdpa) • Practitioner Certificate in Personal Data Protection (www.pdpc.gov.sg/practitioner-certificate) For more information on the DPO Competency Framework and Training Roadmap (www.pdpc.gov.sg/dp-competency)

Data Protection Starter Kit Checklist

SECTION 2: DPAAS@SMES PACKAGE (ANNUAL RETAINER)
1.   Carry out annual review of data protection policies.
2.   Conduct a table-top exercise to test the data breach response plan.
3.   Provide one refresher training for key employees on handling personal data.

SECTION 3: GOOD ACCOUNTABILITY PRACTICES
1.   Conduct a Data Protection Impact Assessment (DPIA) for ***new or existing systems and processes undergoing changes*** to identify, assess and address risks. Refer to ANNEX E of the DP Policy (Sample) for the DPIA Report (Template).
2.   Adopt the Data Protection-by-Design (DPbD) principles when developing ICT systems. Refer to Guide to Data Protection by Design for ICT Systems (www.pdpc.gov.sg/DPBD) for more information.
3.   Independent validation of established policies, processes and practices. Organisations are encouraged to apply for the Data Protection Trustmark (www.imda.gov.sg/dpcertifications) certification for an independent review on its policies and processes.

APPENDICES

Appendix I	Registration of DPO on ACRA BizFile+ and Sample Website DPO Notice	Appendix I - Registration of DPO a
Appendix II	Data Protection Policy (Sample)	To be published at a later date