

Data Protection by Design and Accountability

Koh Suat Hong, Deputy Director, Tech Engineering
Personal Data Protection Commission

28 Aug 2020

Accountability and the PDPA

From compliance to accountability



PDPA Amendments

- Integrate accountability into the Act
- Enhance consent regime and provide options for deemed consent through notification-and-opt-out & legitimate interest exception



Data Protection Trust Mark

- Recognising organisations with accountable practices through certification systems
- Piloted in 2018 and formally launched in 2019



Accountability Tools

- **Guide on Data Protection by Design (DPbD)**
- Guide to Developing a Data Protection Management Programme (DPMP)
- Guide to Data Protection Impact Assessments (DPIA)



GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY



ISACA
Singapore Chapter

Data Protection by Design and Accountability

Guide on Data Protection by Design (DPbD)



Launched in partnership
with Hong Kong PCPD



Key principle of embedding data
protection considerations into the
design and development of IT
systems



Provides practical guidance on
design considerations at each
stage of the software development
life cycle (SDLC) to meet data
protection obligations



GTACS 2020
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA
Singapore Chapter

Seven Principles of DPbD



Proactive and Preventive

Assess, identify, manage and prevent any data protection risks before any data breach occurs



Data Protection as the Default

Integrate data protection measures into processes and features of the systems



End-to-End Security

Security measures to be built into in the entire Software Development Lifecycle (“SDLC”)



Data Minimisation

Collect, store and use personal data that is relevant and necessary for the intended purpose



User-Centric

Develop and implement ICT systems with individuals in mind while protecting their personal data



Transparency

Take an active role in informing individuals on what data is collected from them and how it is being used



Risk Management

Systematically identify and mitigate risks through design and implementation



GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA
Singapore Chapter

Data Protection Impact Assessment as a Tool to Support DPbD

Key tasks in Data Protection Impact Assessment (DPIA)

Identify personal data handled by system or process, and the reasons for collecting personal data

Identify personal data flows through system or process

Identify data protection risks by analysing personal data handled and its data flows

Address identified risks by amending system or process design, or introducing new policies

Check to ensure identified risks are adequately addressed before deployment





GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY



ISACA®

Singapore Chapter