DATA PROTECTION BY DESIGN FOR SOFTWARE, SYSTEMS & WEBSITES

FOR ORGANISATIONS

Build systems to better safeguard your customers' personal data by considering data protection principles right from the start. It will help to reduce unnecessary delays and contain cost, compared to retrofitting data protection features afterwards.

More than 60 good practices, such as the following, are elaborated in the Guide to Data Protection by Design for ICT Systems:

- Requiring explicit action for the user to indicate consent.
- Keeping a record of what users consented to.
- Segregating personal data by sensitivity and according appropriate security measures.

DATA PROTECTION BY DESIGN PRINCIPLES

1 PROACTIVE AND PREVENTIVE

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

2 DATA PROTECTION AS THE DEFAULT

Organisations should be responsible for protecting Individuals' personal data and provide for it in default settings.

3 END-TO-END SECURITY

Incorporate good security features and practices from the point that personal data is collected till it is purged from the system.

4 DATA MINIMISATION

Only collect, store and use personal data that is relevant and necessary.

5 USER-CENTRIC

Develop and implement ICT systems with individuals in mind and make the systems user-friendly.

6 TRANSPARENCY

Inform customers what personal data is collected from them and how it is being used.

7 RISK MINIMISATION

Design and implement the right processes and relevant ICT security measures when processing personal data to reduce risks.

To find out how to design data protection into your ICT systems, visit www.pdpc.gov.sg/og or www.pcpd.org.hk.

Developed by:

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

PCPD HK 香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong