MLS / Company Secretary Limited

BE COMPLIANT WITH THE PERSONAL DATA PROTECTION ACT (PDPA): HOW YOU CAN ADOPT AN ACCOUNTABILITY-BASED APPROACH?

The PDPA requires every organisation to designate one or more individuals to be responsible for ensuring that it complies with the PDPA. The approach of an organisation to appoint a DPO depends on the size of the structure and the extent which it collects, uses, discloses and stores personal Data.
The key role of a DPO is as follows:

- Ensure compliance with the PDPA when developing and implementing policies and processes for handling personal data.
- Foster a data protection culture among employees and communicate personal data policies to stakeholders.
- Manage personal data protection-related queries and complaints
- Alert management to any risks that might arise with regard to personal data and
- Liaise with the PDPC on data protection matters if necessary.

The contacts details of a DPO needs to be available to the public.

Organisations should not view data protection as a mere compliance exercise but as a responsibility given to them by their customers and fully integrated into the organisational culture.

Accountability is a way of demonstrating compliance, and adopting an accountability-based approach to Personal data management helps to:

- Demonstrate responsible use of personal data in the organisations
- Demonstrate that the organisation is proactive and systematic an adept in implementing relevant personal data protection
- Strengthen trust with the public, enhance business competitiveness.

An effective data protection policy is one that can be operationalised into business processes.
One way to translate data protection policies to business processes is by adopting a data protection policy by design approach in which organisations consider the protection of personal data from the earliest possible design stage of any project.
A key component of the wider data protection by Design approach could be conducting a data protection impact assessment for each project.

In order for organisations to demonstrate responsibility and accountability the PDPC has issued some tools and guides:

- Develop a DPMP (data protection management program)
- DPIA (data protection impact assessment)
- PDPA assessment tool for organisation (PATO)

<u>Data protection management programme (DPMP)</u>

A DPMP is a systematic framework that can be used to help organisations establish a robust data protection infrastructure. It covers management policies and processes for handling personal data.
To demonstrate accountability each organisation needs to implement accountability framework that are suited to their business needs.
The DPMP is a framework that provides the foundation for organisations building a robust personal data infrastructure and demonstrate accountability.

The three Components of a DPMP are: Policy, People, Process

- Policy: develop and manage policies for handling personal data
- People: Establish a proper governance structure and define the data protection roles and responsibilities of each officer identified in the organisation. This helps to provide clarity.
- Process: Design manage and review processes for the handling of personal data (collect, storage, use and disclose.)

There is no one size fits all for a DPMP, but here are a few common considerations an organisation would need to look into:

- Ensure that it has a management sponsor

- Identify the stakeholders and to consider when they need to be brought inside the DPMP process
- To leverage key functions and involve all departments that collect, use disclose and store
- To develop an enterprise risk management framework which includes the conduct of risk assessments.
- To develop controls (technical, physical and administrative)
- To conduct data protection training to educate the staff.

Organisations may consider these **4 steps to help them formulate the DPMP**:

1- Identify Personal data handling
2- Identify assess and manage risks
3- Develop DPMP- policy, people process
4- Maintain the DPMP

- The first step is to identify Personal data handling,

one method is to develop a data inventory map or a data flow diagram.
A data inventory map is easy to develop maintain and update and does not require high level of software. A data flow diagram is handy for quick reference and can be easily understood.

- The second step is to identify assess and manage risks.

Risk management is the identification, assessments and prioritisation of risks followed by actions to minimise monitor and control the probability of the risky event occurring or/and its impact if it does occur.
A risk is the potential for loss harm or negative effect on a situation. For example, in the case of compliance with the PDPA the risk is the potential for a failure to comply with the PDPA.

A good way to assess risks in an organisation is to do a data classification.
We can categorise 4 types of risks:

- Risks relating to data protection act and Do not call provisions. It could be for example an unsecured handling of personal data as a breach of the protection obligation one of the 9 obligations in the DP provisions.
- Risk relating to business processes, the first step in developing the DPMP is to build a data inventory map, the second step is to identify the potential data protection risks in the business processes that handle the personal data, organisations need to identify whether there are exposure or gaps in each department's specifics business processes (collect, store, use and disclose)
- Risks relating to data intermediaries (when third parties are involved or concerned) Organisations have the same obligations under the PDPA in respect of personal data processed on their behalf by a data intermediary as it would have if they process the data themselves.
- Risks relating to electronic processing of personal data.

Each organisation should use a risk assessment framework that it considers to be appropriate for its objectives and needs.
An organisation can do the rating/scoring under a risk assessment framework by using either a quantitative approach or a qualitative approach.
Then the organisation can compare and prioritise the risks from the most to the least severe.
Another way is by simply assigning a number to indicate the magnitude of the potential impact of a risk and another number for its likelihood, multiply the two numbers and then rank the risk in term of the resulting number.

- Likelihood criteria- probability of occurring 1 is rare and 5 almost certain
- Impact criteria – indicate the magnitude of potential impact.1 is insignificant and 5 is severe.

After ranking risks, the DPO should present it to the PDPA project team for feedback, approval budget.

- Managing the risks

Once an organisation has identified the risks associated with the collection use storage and disclosure of Personal data, it can put controls in place to manage them.

The organisation can implement a combination of phase controls (technical, administrative and physical)

There are four common ways in which an organisation can respond to a risk namely:

- Risk modification/reduction by action and controls
- Risk retention the organisation accepts the risk
- Risk avoidance by removing the source of the risk, stop an existing activity
- Risk sharing

➢ The third step is to develop DPMP policy

The policy lifecycle has four steps:

- Drafting
- Getting management approval
- Communicating with stakeholders
- Training and enforcing the policy.

Again, there is no one size fits all. But some items as the consent clauses, confidentiality obligations and acceptable use policy, BYOD, due diligence, an IT policy should generally be included in a personal data policy.

An internal policy is a policy made for the organisation's employees as users of personal data.
An external policy is often made available externally, this is usually called a policy but it's a notice.
For both of them, please do be clear and informative, do be easy to understand do not assume that everyone has the same level of understanding, do use a simple style and do not use terminology that might confuse the general public.

The policy lifecycle is continuous and an organisation should review its personal data regularly and has to structure the team their roles and responsibilities, who's the DPO and what are they doing in the company. It's important for the on-boarding and all the employees to have a briefing on the fundamentals, and refresher trainings.

Policies need to be communicated to relevant stakeholders and the organisation must ensure that the personal data protection policy is implemented.

When developing a policy, an organisation may implement a DPIA.

Data Protection Impact Assessment (DPIA's)

A data protection impact assessment involves identifying assessing and addressing personal data protection risk based on an organisation's functions, needs and processes. In doing so, an organisation would be better positioned to assess if their handling of personal data complies with the PDPA and implement appropriate technical measures to safeguard against data protection risk to individuals.

An organisation could conclude a DPIA on its IT system on its processes, when there is a new IT system or process or when the existing system or process are undergoing changes.

How to do a DPIA:

The DPIA involves the following life cycle:

Phase 1: Assess the need for a DPIA (A new IT system is introducing for example)
Phase 2: Plan the DPIA (decide who should be involved, the scope, parties involved, the timeline)
Phase 3: Identify the personal data and personal data flows (identify the data inventory map, or flows)

Phase 4: Identify and assess personal data protection risks (create a DPA checklist questionnaire analyse the impact
Phase 5: Create an action plan (indicate the action owners responsible for the implementation of specific recommendation such as technical measures)
Phase 6: Implement the action plan and monitor its results.

An organisation may also develop and implement a data breach management plan:

Contain the Breach
Assessing risks and impact
Reporting the incident
Evaluating the response and recovery to prevent future breaches

This is the CARE activities in the breach response plan.

- The fourth step is to maintain the DPMP and keep it relevant.
- Monitor and review, revise and notify
- Validate
- Audit plan

Organisations are encouraged to routinely review their data protection policies and practices to enable them to identify data protection gaps and the appropriate remedies> in Singapore's evolving digital economy, this will provide the assurance that the organisation's data protection practice are in line with regulatory and technological developments and that data protection risks are being managed effectively. A key part of sustaining an organisation's DPMP is to educate and communicate to all staff the organisation's personal data protection policies and practices.
It's good to have the DPMP reviewed and validated by a third party.

To conclude, there is no one size fits all and each organisation has to choose the right format when deciding to implement a DPMP or a DPIA, but in order to be compliant with the PDPA, The Data protection officer in each organisation needs to follow the rules and to update policies.

Please contact: Helene Canard-Duchene (Singapore)
hcd@mlscompanysecretary.com
+65 93969193

Maëva Slotine (Hong Kong)
ms@mlscompanysecretary.com
+852 2639 3680

The material contained in this article is provided for general purposes only and does not constitute legal or other professional advice.