INTRODUCTION TO THE PDPA

WHAT EVERY COMPANY NEEDS TO KNOW

The Personal Data Protection Act 2012 ("PDPA") is Singapore's primary legislation for data protection, ensuring that individuals' personal data is safeguarded while allowing organisations to use it for legitimate business purposes. All companies operating in Singapore, regardless of size, are required to comply with the PDPA.

This overview highlights the key obligations under the PDPA, and outlines the practical steps for compliance, including appointing a Data Protection Officer ("DPO"), implementing basic anonymisation techniques, and developing a Data Protection Management Programme ("DPMP").

KEY OBLIGATIONS UNDER THE PDPA

Collection, Use and Disclosure of Personal Data

- **Consent**: Obtain clear and informed consent before collecting, using or disclosing personal data. Individuals should also be allowed to withdraw their consent.
- **Purpose Limitation**: Use personal data only for specific, legitimate purposes that a reasonable person would consider appropriate.
- **Notification:** Notify individuals of the purpose and reasons for collecting, using and disclosing their personal data, and obtain fresh consent before using it for new purposes.

Care of Personal Data

- **Accuracy:** Ensure collected personal data collected is accurate and complete, especially when used to make decisions affecting the individual or disclosed to third parties.
- **Protection of personal data:** Implement reasonable safeguards to protect personal data from unauthorised access, loss or misuse.
- **Retention of personal data:** Ensure that personal data is not retained for longer than necessary for legal, business or operational purposes.
- **Transfer of personal data out of Singapore**: Ensure that personal data is transferred overseas according to the Personal Data Protection Regulations 2021 to maintain a standard of protection is comparable to that under the PDPA.
- **Accountability:** Upon an individual's request, provide information about the organisation's data protection practices, policies, and complaint processes.

Autonomy over Personal Data

- **Access and Correction:** Upon an individual's request, provide them with access to their personal data and correct any errors upon request.
- **Notification of data breaches:** Evaluate breaches and notify affected individuals and the PDPC if the breach causes significant harm to individuals or is of a significant scale.
- **Data Portability:** Upon an individual's request, enable individuals to request for the transfer of their personal data in a machine-readable format to another organisation.

PRACTICAL STEPS FOR COMPLIANCE

1. Appoint a Data Protection Officer (DPO)

Every organisation must designate a DPO responsible for overseeing data protection compliance and managing data protection risks.

Key Requirements

- **Appoint a DPO**: This can be an internal party or external party, depending on the organisation's needs.
- **Register the DPO with Bizfile / PDPC**: The DPO's business contact and information must be made publicly accessible, and DPOs should be registered with the Personal Data Protection Commission.

Why this is important
Appointing a DPO is not just a legal requirement. It is a crucial step in embedding privacy practices within the organisation. A designated DPO enables proactive monitoring, reduces risks of a data breach, and strengths trust with customers.

2. Implement Basic Anonymisation Practices

Anonymisation helps organisations retain useful personal data while protecting individuals' privacy by ensuring that the data cannot be traced back to them.

Key Requirements

Step 1: **Identify Data Elements to Anonymise**

- Identify and remove direct identifiers (e.g., name/NRIC number/email address).

Step 2: **Apply Anonymisation Techniques**

- Use techniques such as character masking, record suppression, and generalisation of indirect identifiers (e.g., occupation / date of birth / postal code etc.).
- Anonymisation should be irreversible for high-risk data or data to be shared with third parties to prevent re-identification.

Step 3: **Monitor and Update**

Regularly review anonymisation practices to address new risks.

- Where reversible anonymisation is applied (e.g. for internal purposes), access to means of re- identification should be restricted to authorised personnel only.

Why this is important
Proper anonymisation minimises PDPA risks and simplifies risk assessments by reducing the likelihood of notifiable data breaches.

3. Develop a Data Protection Management Programme (DPMP)

A DPMP ensures that data protection is integrated into daily business operations.

Key considerations for a Good DPMP

Governance and Risk Assessment

- Establish a governance structure for compliance across departments.
- Identify data protection risks.

Policy and Practices

- Develop data protection policies that are embedded in every step of the organisation's operations.
- Implement data protection practices.
- Communicate policies to staff members and stakeholders.

Processes

- Design processes to operationalise policies.
- Conduct risk identification, remediation and monitoring.

Maintenance

- Regularly review and update data protection policies.
- Conduct audits and keep policies relevant.

Why this is important

A structured DPMP enhances regulatory compliance throughout the organisation, improves operational efficiency, ensures transparency and builds stakeholder and customer confidence.

CONCLUSION

A strong data protection framework is not just a legal obligation but a competitive advantage. Compliance with the PDPA mitigates risks, prevents penalties, and fosters trust with customers and business partners. By taking proactive steps, organisations can ensure they meet PDPA requirements while maintaining operational efficiency and business integrity.

If you or your organisation would like to know how we can assist, please do not hesitate to contact Daniel Chia at 9799 5122 or daniel.chia@colemanstreetchambers.com.