New PDPC guidance on data management practices in Singapore

29 July 2016

The Personal Data Protection Commission of Singapore ("PDPC") continues to be active in issuing advisory guidelines and practical guidance to assist businesses in complying with the Personal Data Protection Act 2012 (the "Act"). Last week, the PDPC issued several new guides to assist businesses in devising and reviewing their data management practices (the "Guides", available here):

- The Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data;
- The Guide to Disposal of Personal Data on Physical Medium;
- The Guide on Building Websites for SMEs; and
- The Guide to Securing Personal Data in Electronic Medium (updated).

The Guides are not legally binding, but represent the PDPC's view of best practices in complying with the Act. While the Guides cover a variety of data protection issues, the following common themes are clear throughout the Guides and are indicative of the approach to data management being encouraged:-

- Governance: organisation-wide data handling policies and procedures are critical. Prevention is better than a cure, and businesses are expected to ensure that data handling roles and responsibilities are communicated effectively to employees. Human error tends to be a cause or contributory factor in the majority of data breach events.
- Accountability for vendors: organisations remain responsible for personal data even when it is processed by a third party vendor. Organisations are expected to conduct appropriate due diligence and impose contractual obligations on their vendors to ensure outsourced data is adequately protected.
- Full data life cycle approach: data protection considerations apply at all stages of the data life cycle, from collection to processing, storage and disposal, and a data management strategy should address the organisation's practices at each stage.

A summary of each Guide is set out below.

Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data (published 20 July 2016)

Singapore law distinguishes between an entity that controls the collection and processing of personal data (referred to as the "organisation") and an entity that is engaged solely to process personal data on behalf of an organisation (the "data intermediary"). The distinction is similar to that between a "data controller" and a "data processor" under European law or that between a "data user" and a "data processor" under Hong Kong law.

An organisation that engages a contractor for data processing activities will generally remain primarily liable under the Act for those processing activities, even if a breach is caused by the contractor. Because of this, the terms of the service agreement under which the organisation engages the contractor are extremely important.

The new *Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data* provides sample clauses for including in service agreements that involve the processing of personal data ("Sample Clauses"). The Sample Clauses are not mandatory, nor does their use guarantee compliance with the Act, but they do provide a starting point in determining the obligations to include in a vendor agreement that involves data processing activities.

Among other obligations, the Sample Clauses require contractors to use personal data only for the purposes of providing the services or to comply with the law; to implement specific agreed-upon security measures; to process personal data only in Singapore unless consent is otherwise given; to restrict access to personal data to particular individuals only; to return or destroy personal data upon termination or expiry of the agreement; to take adequate steps to ensure the accuracy of personal data; and to notify the organisation of any breaches.

While much of the content of the Sample Clauses is in line with general commercial good practice in relation to data processing agreements, there are a few points to note:

- Contractors are obliged to put in place adequate measures to ensure that personal data entrusted to it by the organisation remain accurate and complete, which may be difficult for the contractor to commit to in practice given that in many situations contractors will not have any means of assessing the accuracy of the personal data they are entrusted with and will not be expected to "second guess" the accuracy as part of the services they are providing; and

- Contractors are obliged to indemnify the organisation and all of its officers, employees and agents against all actions, claims, demands, losses, damages, penalties, costs and expenses arising from the data intermediary's breach of its obligations or any act, omission or negligence that causes the organisation to be in breach of the Act, which imposes a risk allocation that may not be consistent with the commercial risk allocation agreed by the parties under any particular service agreement.

As noted at the outset, the Guide in which the Sample Clauses are presented is not binding and states that the Sample Clauses should be adapted to suit organisations' particular circumstances and needs. These statements suggest that organisations will retain some flexibility to negotiate alternatives to the specific Sample Clauses set out in the Guide.

We recommend businesses with operations in Singapore review their standard service agreements and existing arrangements with suppliers to ensure that they align with the Sample Clauses.

Guide to Disposal of Personal Data on Physical Medium (published on 20 July 2016)

The *Guide to Disposal of Personal Data on Physical Medium* follows recent reports in Singapore of disposals of unshredded documents containing personal data with other rubbish – a practice which enables "dumpster diving", where documents are stolen from bins giving rise to the risk of identity theft.

The disposal of documents containing personal data engages two key principles under the Act: the protection obligation, which requires reasonable security arrangements to be made to protect personal data; and the retention limitation obligation, which requires an organisation to delete, destroy or anonymise records that contains personal data when there is no longer a legal or business purpose for retaining them.

The Guide is a reminder that obligations under the Act do not end by discarding of personal data; personal data must be irretrievable upon its disposal. The Guide also provides the means by which organisations should dispose of paper containing personal data – by shredding, pulping or burning – and requires organisations to implement employee policies on data disposal and execute appropriate contracts with vendors that handle disposal. Similar to the Hong Kong Privacy Commissioner for Personal Data's Guidance on Personal Data Erasure and Anonymisation, the Guide provides a helpful level of technical guidance on the topic (download here).

It is important to note that while the Guide appears to be a response to certain incidents relating to paper documents, it has wider application to read-only digital storage media, such as CD-ROMs. The Guide does not, however, apply to re-writeable discs, USB memory sticks and other storage media that allow for overwriting of data on the basis that personal data may be disposed of without the need to dispose of the media itself.

Guide on Building Websites for SMEs (published on 20 July 2016)

Due to the rising volumes of data stored electronically by businesses coupled with the evolving and increasingly sophisticated cyber threats faced by them, electronic data management is considered one of the key components of any risk management and compliance strategy. *The Guide to Securing Personal Data in Electronic Medium* was first published in May 2015, and described a number of "good practices" and "enhanced practices" for protecting electronically stored personal data.

Though the Guide has been updated, its key themes have not changed substantially. The Guide contains a checklist which is a useful starting point for an organisation to review its existing practices and identify areas of weaknesses. The Guide is structured into sections based on the key areas of data management including Governance; Awareness; Testing; Authentication; Authorisation; Destruction; Network security; PC security; Portable device security; Multi-function printers; Database security; Email security; Website and application security; Patching; and Outsourcing.

The sum total of the various elements of the Guide suggest a continued move by the PDPC towards accountability as a critical aspect of achieving compliance under the Act. 'Accountability' here means a holistic approach to compliance, with effective management ownership of data protection issues, adequate resourcing and effective internal policy-making that ensures that all aspect of data processing within the organisation are subject to adequate oversight and risk assessment.

The Guides are available in full at: https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/other-guides

If you would like further information please refer to the 'Contacts' section in the sidebar or the person with whom you usually deal.

Contacts

Mark Parsons

Partner

Louise
Crawford

Counsel

> Read the full article online