The Personal Data Protection Standards 2015

by Adlin Abdul Majid and Kelly Yeo Chei Jun

The Malaysian Personal Data Protection Act 2010 (“the PDPA”), which came into effect in November 2013, was enacted with the aim of regulating the processing of personal data in commercial transactions. The PDPA provides that in processing personal data, data users are to observe the seven data protection principles: namely, the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Security Principle, the Retention Principle, the Data Integrity Principle and the Access Principle. However, these principles are set out in a general manner in the PDPA and, as such, guidance in the form of guidelines or guidance notes is required, to ensure that data users are on the right track in taking steps to comply with their obligations under the PDPA.

It is for this reason that, together with the enforcement of the PDPA, several orders and regulations, which provided further clarification on compliance with the personal data protection principles, were also enforced. Specifically, the Personal Data Protection Regulations 2013 (“the Regulations”) impose, among others, obligations in relation to compliance with the Security, Retention and Data Integrity Standards, as may be set out by the Personal Data Protection Commissioner (“the Commissioner”) from time to time. Consistent with these provisions, in July 2015, the Commissioner issued a public consultation paper proposing minimum standards to be adopted by data users to comply with the Security, Retention and Data Integrity Principles (“the Proposed Standards”).

The standards were finalised and came into effect on 23 December 2015 (“the Standards”).

Proposed Standards and the Standards

Although the Proposed Standards were merely a draft used for the purposes of consultation, the Proposed Standards and the final Standards do not differ significantly. The main differences relate to the imposition of specific obligations, including those with regard to timelines. These obligations are notably drafted in a more general manner in the Standards. For instance, the Proposed Standards require the cancellation of a staff member’s unique ID or the right of access to personal data within three working days if he is no longer processing personal data. In the Standards, this three working days’ requirement has been replaced with a more subjective term, “immediately”.

In the Proposed Standards, the transfer of personal data processed electronically was prohibited, unless it was done with the permission of an authorised officer of the data user. This could cover a wide range of modes of transfer, and could even include emails, thus potentially limiting the issuance of emails that contain personal data. The Standards have narrowed the reference to “electronic transfer” by only focusing on the use of removable media devices and cloud computing services for the purposes of transfer. Transfers by removable media devices and cloud computing services will only be allowed with the written permission of an officer authorised by the data user’s senior management. All such transfers would also have to be recorded and transfers via cloud computing services, in particular, would have to abide by the data protection principles of the PDPA and, if applicable, data protection laws in other countries.

1 This article was first published in DataGuidance, January 2016 (Volume 13, Issue 1)
Obligations under the Standards
The key obligations under the Security Standards relate to the provision of a secure environment in the processing of personal data. This is to be done by, for example, maintaining and limiting the right of access to personal data, setting limits upon the power of staff to access personal data and maintaining personal data access records. Further, risks of potential leaks of personal data can be reduced by ensuring that security procedures are in place and by controlling and recording incidences of data transfers. Obligations under the Security Standards also cover the physical security of data — for instance, by monitoring access to data repositories, putting in place closed-circuit cameras and storing hard copies of personal data in locked cupboards.

Under the Retention Standards, steps must be taken to ensure that personal data is disposed of permanently once no longer required. These steps include disposing of data collection forms within 14 days of collection, unless the forms are subject to other legal requirements. Data users must also ensure that personal data no longer in use is removed from the organisation’s database. Data users are further prohibited from storing personal data in removable media devices without the written permission of senior management.

The obligations under the Data Integrity Standards relate to ensuring that personal data is accurate, complete, not misleading and up-to-date. Requirements imposed include making available (online and physical) forms for data subjects to update personal data and data users updating personal data immediately after receiving a data correction notice.

Clarification of the Principles
The word “standard” is defined in the Regulations as a minimum requirement which is issued by the Commissioner, aimed at repeated use and acting as a guide to achieve uniformity in the given context, which in this case would be compliance with the data protection principles. No doubt the Standards have clarified certain obligations under the PDPA. For instance, s 9(1)(c) of the PDPA provides that regard is to be given to any security measures incorporated into any equipment in which the personal data is stored. The Standards take this a step further by providing that the back-up or recovery system and the anti-virus software installed for the protection and prevention of intrusion of the personal data stored must be updated.

In some respects, however, the Standards have not clarified certain positions under the PDPA. The Retention Standards still echo the Retention Principle, which requires that personal data is not to be retained for “longer than is necessary”. This is a subjective element that has yet to be clarified, although the Standards do provide that consideration is to be given for any other legal provision which requires the personal data to be retained for a longer period. It is further observed that the 14-day period stated in the Standards for data users to dispose of data collection forms would be too short for data users to comply with.
In relation to Data Integrity, the Standards envision that data users are to “immediately” update the personal data of a requestor although under s 35 of the PDPA, this requirement is “not later than 21 days from the date of receipt of the data correction request”. Thus it is unclear whether the 21 days serve as a statutory maximum while the requirement of “immediately” merely means any time before this maximum.

Enforcement
Pursuant to s 101 of the PDPA, the Commissioner may carry out inspection of any personal data system and for the purposes of this inspection, regulation 14 of the Regulations provides that the Commissioner may require the production of records of compliance in accordance with the Standards.

Several instances in the Standards make reference to the requirement for data users to maintain records, be they records of access to personal data by staff or records of regular disposal of unused personal data. These are to be maintained properly and regularly, and presented for the inspection of the Commissioner when requested to do so. This requirement was not present in the Proposed Standards, and its inclusion appears to point towards the fact that the Commissioner is serious about supervising data users in the implementation of the Standards within their organisations. Thus, it is expected that with the issuance of the Standards, the Commissioner will commence enforcement actions.

At present, it is likely that many companies would not have adequate systems or procedures in place to immediately implement the requirements set out in the Standards. As explained above, certain obligations under the Standards are rather specific in nature, and thus suitable planning is required before data users are able to effectively implement the Standards.

Nonetheless, the Standards are mandatory for all data users. As they are already in force, data users are urged to take proactive steps in complying with the requirements under the Standards, as any contravention could lead to a fine not exceeding RM300,000 or a term of imprisonment not exceeding two years, or both.

About the authors
Adlin Abdul Majid (aam@lh-ag.com) is a partner, and Kelly Yeo Chei Jun (ycj@lh-ag.com) an associate, with the Regulatory & Compliance team at Lee Hishammuddin Allen & Gledhill. Adlin also heads the firm’s Regulatory & Compliance team.