Luther.

Malaysia News:

Personal Data Protection

November 2019

Table of Contents

Over recent years, a trend towards greater awareness of data privacy and the security of personal data has been gaining momentum around the world. Fuelled by the rapidly growing importance of data for the global economy and the simultaneously rising number of data related scandals, citizens as well as authorities are becoming more conscious about data protection.

Given the importance of the matter, it is to be expected that the attention on personal data will grow in Malaysia as well, leading to generally greater awareness and stricter enforcement of the Personal Data Protection Act (the "**PDPA**").

Hence, the following newsletter will outline the current data protection regime in Malaysia and its core principles. It will then explain the obligations for businesses and finally it will suggest measures that ensure compliance with the PDPA.

A. What is Personal Data

Before measures to protect personal data can be discussed, it must be first established what qualifies as such. The term personal data is often seen as very abstract and as a consequence, in some more complex instances, businessmen and businesswomen might be unsure whether or not they actually collected any personal data or which collection of data requires further measures for compliance.

The PDPA defines personal data as any information that directly or indirectly relates to any individual who is identified or identifiable from that information or from that data in combination with any other information held by the same data user.

In more general terms, whatever can be used to identify a person is considered to be personal data. For example, this includes names, email addresses, date or place of birth, name of the spouse, residential addresses, initials, IP addresses, account numbers, bank accounts, passport or ID numbers, telephone numbers, social security numbers, pictures, membership details and the list goes on.

As a consequence, the scope of the PDPA is broad and concerns nearly all businesses.

B. Obligations under the PDPA

The PDPA centres around seven core principles that must be complied with.

In practice it is often difficult to interpret these principles and apply them correctly for the individual business and transaction. Hence, the principles will be shortly introduced in the following section to provide an overview of what needs to be covered.

I. General Principles

As a first and foremost rule, personal data can only be collected and processed with the consent of the so called data subject, the individual who is the subject of the personal data in question. Furthermore, the consent can later be withdrawn at the data subjects discretion.

Yet, there is no rule without exception: In certain very specific situations data may be collected and processed without express consent. This, for example, applies when the data is strictly required for the performance of a contract with the data subject or to comply with court orders.

However, it must always be carefully examined if an exception applies. In case of doubt, it is better to request consent.

II. Notice and Choice Principle

The second principle requires informing the data subject of the reasons for the collection and processing of their data, as well as of their rights.

Whenever personal data is collected notice must be given to the data subject outlining: what data is collected and for what purpose, to whom it might be disclosed during the processing, the consequences if the consent is withheld and the data subject's rights, in particular, how the data subject can limit the processing or access the personal data.

After notice has been given, the data may only be used as expressly described in the notice. Hence, if the personal data should be processed for another purpose or additional personal data is collected, a new notice would be necessary.

III. Disclosure Principle

The third principle is a logical consequence of the notice requirement: Personal data collected may only be disclosed to other parties with the consent of the data subject and as described in the notice.

Additional provisions apply if the personal data is transferred to a place outside of Malaysia. Currently, this is only allowed if it can be ensured that the data is kept protected to a level at least equal to the protection granted under the PDPA. This can be achieved by contractual obligations with the data processor to secure the personal data and protect it against loss, abuse and disclosure. Of course, the data subject needs to also consent to the transfer abroad and must be notified of the possibility that the data might be processed by certain entities in a specific country.

IV. Security Principle

Further, personal data must be kept secured and confidential. Thus, depending on the circumstances in the individual case it must be diligently examined how the personal data can be protected not only from a legal perspective but from a technical one as well. This requires carefully implemented security measures to prevent any loss, misuse, modification or unauthorised access.

Technical measures may include firewalls, encrypted databases, or locked and additionally secured data stores. Legal measures include proper guidelines on how to handle personal data for the staff and clearly defined processes. It is crucial that the staff are aware of the potential consequences and the importance of keeping personal data safe.

V. Retention Principle

Under the retention principle the personal data may strictly only be retained as long as it is required for the purpose it was collected.

Once retention is no longer necessary, the personal data must be deleted, returned or destroyed.

As outlined above, if the personal data should be kept after it is no longer necessary for the purpose it was collected for, new consent and notice are required.

This principle is easily overlooked particularly when personal data is kept after the performance of a contract for future

marketing. Therefore, all the purposes for processing should be carefully listed in the notice when initially collecting the data.

VI. Data Integrity Principle

Reasonable steps need to be taken to ensure that the personal data is accurate, complete and up-to-date.

In practice, it is especially challenging to make sure that the personal data remains up-to-date since this requires the cooperation of the data subject. Therefore, to meet this principle, the data should be regularly reviewed and if possible the data subject should be contractually obliged to inform of any updates regarding the collected personal data.

VII. Access Principle

The access principle provides the data subject with more practical control over his or her personal data.

At the data subject's request, access to the collected personal data of the data subject must be granted. Hence, the data subject can review if the data is still correct and required for the purpose. As a consequence, the data subject can take an informed decision if he or she wants to fully or partially withdraw the consent or just update incorrect data. In case of a violation of the principles, the data subject could also file a complaint to the authorities.

Consequently, access to the collected personal data needs to be granted at the request of the data subject within a short deadline.

To keep this deadline and to comply with all requests, it is important to establish internal structures on how to process such requests and to appoint a specific employee as a data protection officer, even though this position is not mandatory under the PDPA.

C. How to comply with the PDPA

With a very broad range of possible forms of collection, processing and purposes of businesses, it remains challenging to implement the necessary measures for full compliance. Furthermore, there are often no clear definitions or rules and final interpretation remains at the discretion of authorities.

However, the following steps may be helpful to minimise the compliance risks:

- Checking if registration with the Personal Data Protection Commission is required;
- Implementing data protection policies both externally, including the notice and collecting consent from data users, and internally by offering guidelines for the staff on how to handle personal data;
- Keeping records of collected, processed and disclosed personal data as well as of notices and expressions of consent ready for inspection.

I. Registration and Code of Practice

As a first step, it should be clarified whether or not a business belongs to a class of data users that is required to register with the Personal Data Protection Commissioner. It is at the discretion of the authorities to define these classes and decide if registration is required. Currently, the classes include among others certain businesses in the following sectors: Communications, banking and finance, insurance, real estate, health, tourism and hospitalities, education, direct selling and services like auditing, accountancy, architecture, engineering and legal advice.

Those businesses are only allowed to collect and process personal data after having received a certificate of registration and only as long as the certificate is valid.

Additionally, certain classes may form their own data user forums and prepare codes of practice regulating the collection and the processing of personal data by their members.

II. Data Protection Policies

Tailored data protection policies may be used to cover a range of very different situations. They may be used as standard

notice to data subjects but they may also be used to internally outline guidelines on how personal data is handled.

II.1. External Data Protection Policies

In order to ensure that a business is in full compliance with the PDPA all data subjects must be notified and consent to collection and processing where required. This may not only include customers and clients but also include employees, contractors, service providers and other business partners as well.

An external data protection policy can take the function of a notice to all or to a particular group of data subjects, depending on the business model.

Hence, such policy should include all information necessary for notice. It can be drafted broadly to be applicable for different situations by listing all purposes for collection, all sources of personal data and all instances when data is collected.

Furthermore, the policy should outline to whom the personal data may be disclosed. Typically, this includes other group companies, potential delivery partners, professional advisors or subcontractors.

It can then be served to the data subjects, for example, by publishing it on a website and linking it to the order process of an online shop by requiring the customer to click “I agree”. It could also be attached to a contract which directly refers to it, added in copy to a package for delivery if no prior consent is required, or published by displaying it clearly visible on a counter.

How exactly the policy should be implemented and published depends on the individual circumstances and in particular on whether consent is required or not.

Notice, consent and collection should always be recorded.

II.2. Internal Data Protection Policies

An internal data policy is one of the possible measures used to ensure the security of the personal data and compliance with the PDPA.

It does not take the role of a notice like an external policy but provides guidelines on how the staff handle personal data.

It explains the obligations under the PDPA to the staff and outlines their daily application in the business. An internal policy also details specific processes that must be applied to ensure compliance with the PDPA and tailors those processes to the individual business.

Additionally, an internal data protection policy can provide for the appointment of a data protection officer

This officer could receive a greater level of training on data protection and may assist other employees in more complex situations.

Furthermore, requests from data subjects may be addressed by the data protection officer to ensure professional and timely compliance with all requests.

An internal data protection policy can be implemented to be binding for the staff, triggering disciplinary actions if the guidelines are violated. Thereby, the awareness of the staff on data protection issues will be raised and violations of the PDPA prevented.

III. Records

In general, records of all collection of personal data, consent, notification, disclosure and access to personal data should be ready for inspection at any time.

The records can be requested by the authorities during an investigation or after a complaint by a data subject.

D. Our PDPA Related Services

Luther is able to assist in ensuring full compliance with the PDPA.

It is our goal to facilitate your daily work and minimise your compliance risks.

I. Policy Drafting

We offer to individually tailor the above mentioned policies for the specific needs and circumstances of a business. As a result all activities should be covered and we advise on how to implement the policies into the daily business.

II. Audits

Furthermore, we can screen businesses in a comprehensive data protection audit.

Here we would establish what personal data is collected and how it is processed to provide us with a detailed picture of the personal data portfolio.

In a second step we would then locate any gaps or lapses in the data handling.

Afterwards, we would assess the specific needs and what is required for compliance with the PDPA.

III. Training

Additionally, we offer training sessions for employees. This may be for both general staff members or specifically for data protection officers. The aim of the training is to raise awareness of the matter and provide guidelines and basic rules on how to handle personal data.

E. Your Contact

Lukas Kirchhof
LL.M. (Chinese University of Hong Kong)
Legal Counsel
Luther Corporate Services Sdn Bhd
Unit 17-2, Level 17, Wisma UOA II,
No. 21, Jalan Pinang,
50450 Kuala Lumpur
Malaysia
Phone +60 3 2166 0085
lukas.kirchhof@luther-services.com

Imprint

Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22, 50678 Cologne, Phone +49 221 9937 0, Fax +49 221 9937 110, contact@luther-lawfirm.com

Editor: Pascal Brinkmann, LL.M. (Stellenbosch), Managing Director, Unit 17-2, Level 17, Wisma UOA II, No. 21, Jalan Pinang, Phone: +60 (0)3-21660085, pascal.brinkmann@luther-services.com

Luther Corporate Services, the Corporate Services arm of Luther lawfirm enables us to offer our clients a “one-stop” solution for all their business needs. Our accountants, company secretaries and tax consultants provide the whole range services, which our clients expect from such a one-stop concept, from corporate secretarial services, outsourced administration, payroll and accounting to tax compliance. We assist our clients comprehensively in all stages of a business lifecycle, from the formation of a business vehicle, to ongoing support and statutory compliance matters and to the dissolution of a company.

Delhi-Gurugram, Kuala Lumpur, Shanghai, Singapore, Yangon

Luther Corporate Services Sdn Bhd (200901028935) | Unit 17-2, Level 17 | Wisma UOA II | No. 21, Jalan Pinang | 50450 Kuala Lumpur | Malaysia Phone +60 3 2166 0085 | Fax +60 3 2166 0087

Your contact:
Pascal Brinkmann, pascal.brinkmann@luther-services.com

Further contacts can be found on our website www.luther-services.com.

Hits the mark. Luther.