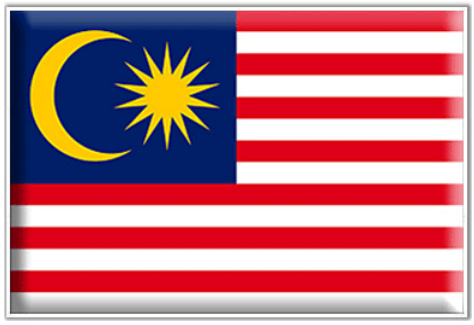
Data Protection Disease…

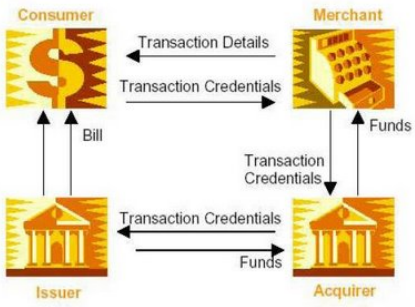


Malaysia has adopted the Personal Data Protection Act 2010, which regulates the processing of personal data concerning individuals. While this sounds like the European Data Protection Directive, chapter XYZ, this data protection act only applies to personal data which is involved *in commercial transactions*.

The act will not come into force until the responsible Minister inserts a notification in the official government *Gazette.* As is common in many parliamentary systems, different sections may come into effect at different times.

Commercial transactions.

As noted, in a significant limitation of protection for personal information, it is only information "in respect of commercial transactions"… "that relates directly or indirectly to a data subject, who is identified or identifiable from that information…".



A "commercial transaction" is one "of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency…". (It is always interesting to us to see how quickly and deeply the credit reporting industry becomes involved in lobbying proposed legislation in this subject area.)

Consequently, it would appear that if my banker asks for my address and phone number, this information would be protected by the statute, but when my university, sports club, doctor, Congressman or police officer asks for the same information, it would not be protected by the statute.

It is also unclear whether this law applies to an employer-employee relationship. It clearly does not apply to any data gathered by government agencies. It would also not seem to apply to educational institutions and medical institutions. The act specifically states that it is not applicable to personal data processed outside Malaysia unless it will be further processed in Malaysia. It also does not apply to federal and state governments, and any personal data collected for noncommercial transactions.

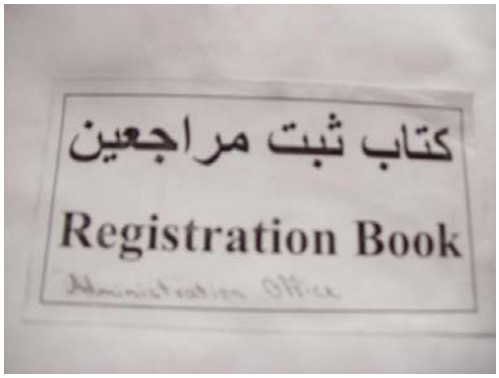
The OECD principles.

The statute sets out seven principles with which a data user must comply, principles which are derived directly from the OECD privacy principles. These include the notice and choice, disclosure, security, retention, data integrity access and the "general principle", which states the principle of consent to processing.

Data Protection Authority and Registration

Unfortunately, the act provides that one of more classes of data users may have to register with the

Continued on next page



Personal Data Protection Commissioner, "who may register the applicant and issue a certificate of registration, or refuse the application." It is not clear that the statute puts out the grounds on which an application may be refused. This is one of the most common complaints of business in Europe. There is no conceivable privacy-related purpose for this.

Consent.

Under the general principle, personal data can only be processed once the data subject has given his consent to such processing. The subcategory of sensitive personal data needs either consent or other validation for processing, discussed below.

And consent is?

The statute does not define "consent", which is extremely unfortunate. There are exceptions for processing of personal data apparently without consent which will be familiar to those familiar with European law: performance of the contract, steps preliminary to a contract taken at the request of the data subject, compliance with legal obligation to which the data user is subject, and the category of "protection of the vital interests of the data subject", which has been so severely limited by the Article 29 Committee. Under the practice of many other countries consent can be express or implied, but this statute is silent on this distinction although it sets out in some detail the circumstances in which consent is assumed, as in Europe. Unfortunately an assumption of consent is a different form of legal construct than "implied" consent.

Notices and clarity.

For marketers, including website operators, judicious use of notices and very clear privacy statements in terms of use would seem to be much in order.

In any event the notice and choice principle that requires that data users inform people in both English and the national language that personal data is being processed, the purpose of that processing, the individual's right to access and correct the data, to whom the data will be disclosed, the recourse to limiting such use, whether this collection is obligatory or voluntary, and consequences on refusal.

Data sharing.

In terms of data sharing, the law requires consent thereto but one assumes that the notice given at collection, provided it is robust enough, will satisfy this requirement. Interestingly, the statute has two exceptions to the requirement of consent to disclosure in addition to the usual prevention of crime exception. One is that the data user acted in the "reasonable belief" that he would've received the consent of the data subject if he had been told of the sharing, or the data user had a "reasonable belief" that he had the right to disclose the data.

Sensitive data.

The statute distinguishes between "sensitive personal data" and "personal data". The former is "personal data consisting of information as to the physical or mental health or condition of the data

subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission of an offense, or "any other personal data as the Minister may determine..."

It is a truism that what is sensitive depends on the culture. Labeling political opinions as sensitive information strikes a reader raised in a democratic tradi-

Continued on next page

tion of open political debate as unusual. For an American, not calling financial information sensitive is noteworthy. Finally, we note that sexual preference is not considered to be sensitive information, this in a country which has aggressively prosecuted one of its most important political leaders for alleged sexual misbehavior.

It is also interesting that the entire question of what else might be considered sensitive data is left to the judgment of a minister, who is a political appointee. This seems a dangerous power to provide to a political appointee, who could wield this against the press or a political opponent in an electoral environment.

Consent

The consent required for processing of personal data is "explicit", which is not defined. This also forebodes the extension of the European debate of whether or not an individual must do something to acknowledge consent in order for it to be “affirmative” or “explicit”.

Transfer of personal data abroad.

There is an absolute prohibition on the transfer of personal data outside Malaysia to places not specified in a notification published in the *Gazette* “by the Minister on the recommendation of the Commissioner.”. The statute does not seem to set a standard which the Commissioner use to make such recommendations, such as a destination country providing “adequate protection”.

There are exceptions, fortunately, including the consent of the data subject, necessity for contractual performance, for legal proceedings, "in the interest of the data subject”, and a few other grounds. A violation of this prohibition may be punished by a fine up to RM 300,000 ($100,000) or imprisonment for up to two years.

It is worthwhile recalling that the Article 29 Committee in Europe, and many Data Protection Commissioners, have severely restricted the scope of the “interest of the data subject” exception, limiting it in many instances to “life-and-death” circumstances.

Compliance.

The act will apply to data collected prior to the law's coming into force, although there is a grace period of three months to come into compliance. Because uses of personal data for commercial purposes will require consent, lawyers in Malaysia are advising their clients to carefully review and revise data intake forms used with customers in order to avoid collecting sensitive information. They also recommend delegating authority to a company officer to be responsible for privacy-related issues, implementing procedures to protect personal data from abuse, and establishing customer complaint procedures.

Conclusion.

Any company marketing or doing business in Malaysia would do well to review all business procedures relating to capturing and employing personal data in the business.

It will also be interesting to see if there is any intention of the Malaysian government or the to- be- named Personal Data Protection Commissioner to seek to have the statute adjudged "adequate" under the European Data Protection Directive. Given that this statute provides data protection only to information collected in the commercial context, we would expect that European officials would be somewhat reluctant to judge it "adequate".

Editor.

