RHTLaw TaylorWessing

Dated 30 April 2012

RHTLAW TAYLOR WESSING LLP

FEEDBACK ON
PROPOSED PERSONAL DATA PROTECTION BILL

Contact person:

Rizwi WUN

Partner

Intellectual Property and Technology Practice (Co-Head)

DID +65 6381 6818

rizwi.wun@rhtlawtaylorwessing.com

Six Battery Road
#09-01 & #10-01
Singapore 049909

Tel +65 6381 6868
Fax +65 6381 6869

www.rhtlawtaylorwessing.com

TABLE OF CONTENTS

Contents **Page**

1. Summary of Major Points

1.1 We are pleased to submit our views and comments on the proposed Personal Data Protection Bill issued on 19 March 2012 ("**the PDP Bill**"), as accompanied by the Second Consultation Paper dated 19 March 2012 ("**the Second Consultation Paper**") issued by the Ministry of Information, Communications and the Arts ("**MICA**").

1.2 Our submission will focus only on the following specific areas in the PDP Bill:-

(a) We believe there should be sufficient clarity on the standards of reasonableness expected in respect of the collection, use, disclosure, transfer and security of personal data.

We suggest that the factors to be taken into account in deciding these standards of reasonableness should be set out.

(b) We believe there should be additional measures imposed to safeguard the outflow of personal data overseas, especially to countries that do not have the equivalent regulatory protection of personal data.

(c) We would like to see some clarity on exceptions relating to the conduct of certain legal proceedings whether in Singapore or elsewhere that concerns the disclosure of personal data.

1.3 Our areas of concern will also set out proposals for consideration. It will be obvious that some aspects of our proposals will be intertwined amongst the above issues and the proposals should be considered from a macro perspective of these selected issues within the context of the intended Personal Data Protection Law.

2. Comments and Proposals

We set out below our detailed comments on the areas of concerns, together with our proposals for consideration.

2.1 Standards of Reasonableness

(a) We understand that the concept of "reasonableness" underpins the standards with which a Data Processor is expected to carry out its obligations under the PDP Bill. We note in particular clauses 3, 13, 20 and 26 of the PDP Bill.

(b) We are therefore pleased to note in Second Consultation Paper [1] that the Data Protection Commission ("DPC") will consider issuing guidelines in respect of the concept of "reasonableness" and "necessity".

(c) In view of the different stages of treatment of personal data, we believe that different expectations of reasonableness should apply at different stages.

(i) Collection

We believe that the standards of reasonableness at the point of collection should correspond to what is necessary for the purposes for which the personal data was collected in the first place.

In order to ascertain necessity, it would therefore be useful and essential for the Data Subject to know the specific purposes for which his or her personal data is collected. Therefore the key aspect is whether there is adequate communication from the Data Processor that enables the Data Subject to know and understand the purpose and intended use of the personal data that has been collected.

(ii) Use and Disclosure

The main concern is whether the personal data so collected has been used and or disclosed in accordance with the purposes communicated to the Data Subject at the time of collection. So long as the initial communication is clear, there should be little room for doubt or uncertainty. One important issue is whether there are collateral purposes that can be implied into collection of such personal data. *For*

[1] Paragraph 2.39

example would the personal data of a subscriber of an Internet e-mail account held by an Internet Service Provider be disclosable to a third party who wanted to take civil proceedings against the subscriber, assuming the third party has a valid case, or would this third party be compelled to find out the same information from other sources.

(iii) *Transfer*

The concerns regarding the transfer of personal data overseas have been well documented. We are of the view that minimum requirements regarding any such transfer should be imposed onto the Data Processor, and the degree of compliance with such minimum requirements should be taken into account. Please also refer to our comments in Section 2.2 below as well.

(iv) *Security*

Clause 26 of the PDP Bill states that protection of personal data should be by "*reasonable security arrangements*".

We note that MICA intends to issue guidelines on suitable means of protecting personal data.[2] However we note that MICA is considering not imposing mandatory data breach notifications but will instead be taken into account as a mitigating factor.

However, we feel that an efficient system of notification is useful as it enables data subjects to take remedial action in case there are other consequences that may arise from any unauthorised access of their personal data. The recent incidents concerning the millions of users affected by the unauthorised access to the database of Sony Playstation in 2011, and of Singapore Airlines' Krisflyer program last year and in Feb 2012 highlight this concern. We feel that having a system of notification should be taken into account in deciding whether or not reasonable security arrangements have been made.

In our view, there are three ways to address this. One alternative is once a breach of the security measures provided by the Data Processor or Data Intermediary has occurred, this is by itself an automatic breach of the provisions of Clause 26 of the PDP Bill when it becomes law, regardless of the effort put in by the Data

[2] Paragraph 2.111 of the Second Consultation Paper

Processor or Data Intermediary; the second alternative is to look at the endeavours of the parties to decide whether or not a breach of the provisions of Clause 26 has occurred, regardless of whether an actual breach of the security measures has occurred.

The third alternative would be a combination of both alternatives.

(d) In addition to the each of the different stages, we also believe that it should be clarified whether the concept of reasonableness should be from the point of view of the Data Subjects or from Data Processors.

(e) We note the difficulties associated with setting out the factors to be taken into account in deciding what is reasonable. However we believe that some effort in setting out such factors would enable Data Processors and or Data Intermediaries to know limits and boundaries as to expected standard of their conduct.

(f) <u>Proposal for Standards of Reasonableness</u>

We propose that:-

(i) it would be helpful to decide from whose perspective the concept of reasonableness should be determined, although this can be mitigated depending on the factors to be set out;

(ii) the concept of reasonableness should be approached in a manner not unlike the concept of reasonableness in the Second Schedule of the Unfair Contract Terms Act (Cap 396); and

(iii) the factors to be taken into account, for <u>each aspect</u> of collection, use and disclosure, transfer and security should be separately set out.

2.2 Minimum standards imposed on the outflow of data to other countries

(a) We share the concerns raised in the Second Consultation Paper[3] regarding the enforcement of the provisions of the Personal Data Protection Law in respect of personal data transferred outside of Singapore.

Taking a lead from the position in Europe, we suggest considering imposing an equivalent condition that where any personal data is to be transferred to another country where adequate data protection is not available, then the Data Processor responsible for transferring this personal data must include minimum standard contractual clauses in their contracts with the recipients of such personal data.

This could apply to transfers to Data Intermediaries that are located overseas, including for intra-group company transfers.

(b) We agree that data subjects should be notified of, and consent to, their personal data being transferred overseas. If the Data Processor only subsequently decides to transfer the personal data later, then the consent should nonetheless be obtained prior to the transfer.

(c) We recognise this is not a panacea for all possible concerns but nonetheless may provide a partial solution.

(d) Even if MICA is not minded to impose this minimum standard contractual clause requirement, we believe such a measure could be a factor to be taken into account to ascertain whether the conduct of any Data Processor is reasonable in the circumstances.

(e) Assuming this proposal is taken up, MICA might need to consider a consequential amendment to the Contracts (Rights of Third Parties) Act 2001 of Singapore, to allow Data Subjects the right to legal action against the Data Processors and or the receiving party in their home country under such contracts.

We note that there is already a provision to allow a private action in respect of contravention against a Data Processor after decision made by Data Protection Commission that there has been contravention, and the decision becomes final because of no further right of appeal.[4]

[3] Paragraphs 2.17 to 2.20 and 2.89 to 2.90
[4] Para 2.109 Second Consultation Paper cross referred with Part VII PDP Bill.

At the very least, this will give some assurance to Data Subjects of a minimum expectation that Data Processors who transfer Personal Data are liable under the Act if they fail to ensure such clauses are set out in contracts between them and recipients of personal data.

(f) Proposal

We propose that

(i) Data Subjects should be notified of, and should consent to, their personal data being transferred overseas if that is decided by the Data Processor;

(ii) these minimum standard contractual clauses should be imposed onto Data Processors be set out in the form of Subsidiary Legislation, not unlike the manner currently set out in Europe.

(iii) In the alternative, where a Data Processor has in place such contractual restrictions, then this would be a factor to consider when considering whether it is behaving reasonably in the circumstances.

2.3 Exceptions for Certain Legal Proceedings

Legal proceedings commenced outside of Singapore

Our concern is with regard to two possible scenarios concerning legal proceedings. The first is in respect of legal proceedings commenced outside of Singapore that involve a Data Processor or Data Intermediary disclosing Personal Data collected under Singapore Personal Data Protection Law. The other is where proceedings are commenced against a Data Processor or a Data Intermediary for the disclosure of Personal Data of a Data Subject, where the Data Subject is envisaged to be the defendant in legal proceedings.

(a) Under the doctrine of international comity, it would be assumed that where legal proceedings are commenced outside Singapore, and should there be included in such proceedings any application or order to disclose personal data collected by a Data Processor or Data Intermediary under Personal Data Protection Law in Singapore, then the foreign court or tribunal would recognise and respect Singapore Personal Data Protection Law.

(b) Clause 19(3) of the PDP Bill read together with paragraph 1(g) and or (h) of the Fifth Schedule to the PDP Bill creates an exception to disclosure without consent where:-

Disclosure is "necessary" for any investigation or proceedings
Disclosure is "required" or authorised by law

(c) Clause 4(7) of the PDP Bill also specifies that to the extent any provision of the PDP Bill is inconsistent with any provision of other written law, the provision of the other written law shall prevail.

(d) It is assumed that Clause 4(7) applies only to other provisions of Singapore Law, and that the inference from the relevant provision of the Second Consultation Paper [5] is that the exception under the Fifth Schedule only contemplates proceedings in Singapore.

(e) The concern is therefore the current wording does not contemplate legal proceedings commenced outside of Singapore that are based on provisions that are inconsistent with Singapore Personal Data Protection Law.

[5] Para 2.75 of the Second Consultation

Further, there is no clarity as to whether the party seeking disclosure what is the standard required to establish the concept of "necessity" or "requirement".

This concern becomes more acute in the case of a Data Processor and or Data Intermediary that is situated overseas.

(f) Applications for disclosure of Personal Data against a non-party

Increasingly, there have been instances where Data Processors in possession of personal data of their customers have been asked to disclose such personal data so that other parties may pursue legal proceedings against such customers. Such a concept has been recognised in the courts as applying for a "*Norwich Pharmacal*" order. This involves seeking pre-action discovery against a non-party to proceedings. It was most recently highlighted in the litigation involving *Odex Pte Ltd*, in which a Singapore distributor of Japanese anime in which personal data held by Internet Service Providers of their customers was disclosed in order for Odex to pursue copyright infringement claims against such customers.

The concern was also raised in the UK case of *Totalise v. Motley Fool* in which a refusal to disclose under the UK Data Protection Act was raised but decided as inapplicable because of a statutory exception.

(g) In our view, such a situation especially requires balancing of competing interests. On the one hand, the wronged party should not be denied access to such information simply on the basis of protecting the rights of Data Subjects, on the other hand, the Data Subjects should not be exposed to unwarranted or unjustified disclosure of their personal information simply because the complainant believes that such disclosure is necessary. The second concern is whether there should be a different standard under paragraphs 1(g) and (h) of the Fifth Schedule of the PDP Bill where the Data Processor is a defendant to proceedings, or where disclosure is sought against the Data Processor in order to take action against the Data Subject. Please refer to our concerns set out in paragraph 2.1(c)(ii) above.

(h) Proposal

We propose that:-

(i) there should be some clarification whether or not provisions of foreign law applies to:-

Clause 4(7) of the PDP Bill; and or
Paragraphs 1(g) and (h) of the Fifth Schedule of the PDP Bill.

(ii) It may be preferable to set limits or exceptions to disclosure of such personal data under both these paragraphs in the Fifth Schedule in respect of proceedings commenced overseas; and

(iii) there should be a higher standard to prove the concept of necessity and or requirement where the Data Processor and or Data Intermediary is required to disclose information in order for a complainant to bring an action against a Data Subject, as compared to a comparatively lower standard where the Data Processor is itself the defendant to the proceedings.

3. Conclusion

We are reassured that most aspects of the Proposed Personal Data Protection Bill give a certain level of certainty and clarity on how the law will treat personal data collected in Singapore.

Our intention in submitting our views and comments is to seek clarity on specific areas and to provide a balance between two possibly competing interests. It would be unrealistic to anticipate all eventualities but we would like to contribute towards reducing as much of the uncertainty as possible.

Should you have any further queries, please contact Mr Rizwi Wun, Co-Head of Intellectual Property and Technology Practice at RHTLaw Taylor Wessing LLP via the channels below:

E-mail: rizwi.wun@rhtlawtaylorwessing.com
Direct Line: +65 6381 6818
Mobile: +65 9756 2251