LLOYDS BANK CORPORATE MARKETS PLC, SINGAPORE BRANCH

RESPONSE TO PERSONAL DATA PROTECTION ACT (AMENDMENT) BILL CONSULTATION

28 MAY 2020

For any queries, please contact:

[Redacted]

SUMMARY OF MAJOR POINTS

We have set out below some queries and clarifications requested on the following points:

- Deemed Consent by Notification;
- Protection of Personal Data; and
- the Duty to Notify Breaches.

STATEMENT OF INTEREST

Lloyds Bank Corporate Markets plc, Singapore Branch ("LBCM") provides banking services to Large Corporates and Financial Institutions in Singapore and the Asia Pacific region. It has created policies and procedures to ensure compliance with the requirements of the Personal Data Protection Act in Singapore (the "Act"). As a result, we would like to assess what changes may be required to ensure continued compliance with the expectations of the Personal Data Protection Commission in Singapore. We are therefore keen to clarify expectations arising out of the proposed changes to the Act arising from the Bill.

COMMENTS

1. Deemed consent by notification

Clause 15A.—(1) Subject to subsection (2), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if —

(a) the organisation satisfies the requirements in subsection (3); and

(b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (3)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation.

(2) Subsection (1) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose.

(3) For the purposes of subsection (1)(a), the organisation must, before collecting, using or disclosing any personal data about the individual —

(a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; and

(b) take reasonable steps to bring the following information to the attention of the individual:

(i) the organisation's intention to collect, use or disclose the personal data;

(ii) the purpose for which the personal data will be collected, used or disclosed;

(iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data.

(4) The organisation must, in respect of the assessment mentioned in subsection (3)(a) —

(a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the relevant purpose is likely to have on the individual;

(b) identify and implement reasonable measures —

(i) to eliminate the adverse effect;

(ii) to reduce the likelihood that the adverse effect will occur; or

(ii) to mitigate the adverse effect; and

(c) comply with any other prescribed requirements."

LBCM Comment

- **Undefined terms of 'adverse effect' or 'likelihood' may require further clarity by the courts, or time for specific market practices to develop. We would appreciate if the Commission could provide further clarity on these two undefined terms, using examples, so that companies can better understand how to achieve compliance.**

2. Protection of personal data

"Clause 24: An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored."

LBCM Comment

- **The Bill offers no definition of what constitutes "reasonable security arrangements" in relation to clause 24 above for personal data. We would appreciate the authority providing some examples of what would constitute reasonable security arrangements to guide the company.**

3. Duty to notify occurrence of notifiable data breach

"Clause 26D:

Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 days after the day the organisation makes that assessment.

Subject to subsections (4), (6) and (7), the organisation must also notify, on or after notifying the Commission under subsection (1), each affected individual to whom significant harm results or is likely to result from a notifiable data breach in any manner that is reasonable in the circumstances.

(3) The notification under subsection (1) or (2) must

(a) contain all the information that is prescribed for this purpose; and

(b) be made in the form and submitted in the manner required by the Commission."

LBCM Comments

- **We would request if 3 days could be clarified as meaning business days or calendar days. Business days would seem more appropriate in these circumstances.**

- **Under Clause 26D (3) (b), reference is also made to the form and manner of submission of a notification to the Commission. We would appreciate if the Commission could provide the new template to be used, along with instructions as to the manner of submission, so this can be incorporated into company procedures where required.**

CONCLUSION

We would appreciate some additional guidance and clarification on the points raised above, with examples of the expectations being particularly helpful**.**