RESPONSE TO CONSULTATION PAPER

Consultation topic:	Consultation Paper on Draft Personal Data Protection (Amendment) Bill, including related amendments to the Spam Control Act
Organisation:	United Overseas Bank Ltd
Contact number for any clarifications:	Redacted
Email address for any clarifications:	Redacted
Confidentiality	
I wish to keep the following confidential:	Redacted

SUMMARY

Further guidance from MCI/PDPC is crucial to ensuring consistent interpretation and application of the amendments. It will make the difference between transforming how we use data and exceptions being left unused because the conditions are too burdensome or the lines are not clear enough for us to apply the exceptions with confidence. The huge increase in potential fines increases astronomically the risks of non-compliance, and acts as a strong deterrent if we do not have greater certainty.

CONCLUSION

We thank MCI/PDPC for your hard work on the Bill, and the effort made to strike the right balance between an organization's legitimate business interests and protection of individual privacy rights. We also appreciate the many opportunities given for feedback, and the open communication by your officers. We are supportive of these changes, and look forward to working with you on regulations and guidelines which will be critical in shaping implementation and compliance.

COMMENTS

Clause No. in Bill	Draft amendment	Comments
2	Definition of "user-provided data"	In some cases, the personal data of an individual is provided by another person, for example, a customer gives the organisation the personal data of his children for insurance purposes, or a company gives a bank the personal data of its officers for account opening purposes. Suggested amendment: "user-provided data" in relation to an organisation, means personal data provided by or with the consent of an individual to the organisation."
7	Conditions for the deemed consent by notification	1. We understand that organizations are not required to make the assessment available to the individuals, and ask that this be stated in the new provisions. 2. Given that the right to opt out is one of the conditions, please confirm that where the new purpose (eg. integrated app feature or use of a third party solution) is a necessary purpose, and the only way to "opt out" is to discontinue use of the product or service, this exception may still be applied. 3. We look forward to guidance being issued on: (a) How granular the description of purpose should be. For example, would it be acceptable to seek consent for "sharing your transactional data with third party organisations for the purposes of personalising product offerings from these third parties"? Or is the expectation that the purpose be specific , for example, "sharing the types of products you typically buy every month with suppliers of such products for the purposes of personalising offers to you in collaboration with these suppliers"? Or must the organisations with whom data is shared be identified by name? (b) Clarify that the consent sought may be ongoing rather than valid for a specified period or one time activity. The appropriate validity period of the consent may be included as part of the risk and impact assessment, to ensure that it is reasonable in the context of the intended purpose and impact.

		(c) Withdrawal of consent – please allow for circumstances where this may not be possible, for example, (i) consent was collected for a specific activity which has already been completed or which is already in progress, or where the data has been incorporated into a solution from which it cannot be extracted. Discontinuing use should be to the extent reasonably possible, taking into consideration the purpose for which consent was given. There can still be accountability, by the organization explaining to the individual how his data may continue to be used (similar to the current requirement to explain the consequences of a withdrawal of consent). For example, a person was featured in a book. It would not be reasonable to expect the company to withdraw the book from circulation, but it would be reasonable to remove that individual from future editions. (d) Examples of what would constitute adverse effect.
7	Deemed consent by notification – [Redacted]	[Redacted]

8 31	Use of personal data for "business improvement" purposes in Part 2, para 2 of the First Schedule	For business improvement purposes, an organisation may disclose personal data to a related corporation, for example a subsidiary that performs data analytics for the group, or other subsidiaries which may benefit from the findings. Please include a right of disclosure to related corporations in Part 3. We would be grateful if you could also permit disclosure to a third party service provider, as many organisations may not have the expertise themselves and have to rely on third parties such as consultants for data analytics, process engineering and other tools.
8 31	"Legitimate interests" in Part 3, para 1 of the First Schedule	1. We are happy to see that prevention of fraud is recognised as a legitimate interest which is beneficial to the public. Being able to exchange information of fraudsters to related corporations and even other banks will be instrumental in enhancing fraud prevention/anti-money laundering abilities. 2. Risk management, encompassing operational, credit, liquidity and other risks, is vital to ensuring an organisation's survival, and augurs to the benefit of its employees and customers, and in the case of a financial institution, to the economy and industry. We would be grateful if risk management could also be accepted as an example of legitimate interests.

8 31	"Business asset transactions" in Part 3, para 11 of the First Schedule	1. In sub-para 11(2)(a), it is provided that the personal data disclosed must be "about an employee, a contractor, a customer, a director, an officer or a shareholder of Y". In a transaction where X is transacting with Y to purchase Y's shares in target company T, the personal data would be of the individuals related to T not Y. Please amend sub-para 11(2)(a) to extend to T. 2. Sub-para 11(2)(b) requires a confidentiality agreement to be entered into between X and Y. This should be the responsibility of the disclosing party Y. If not required by Y, X would not insist on a confidentiality agreement. In a scenario where Y is not incorporated in Singapore and does not require a confidentiality agreement to be signed, the agreement should not be made mandatory on X. We propose that instead, there is an obligation on X to use and disclose the personal data received solely for purposes related to the business asset transaction, regardless of whether a confidentiality agreement has been signed. 3. We respectfully submit that sub-para 11(4)(a) may be deleted. X would already have to comply with PDPA in respect of the personal data that it has collected from Y, and this already includes ensuring that it has consent for use and disclosure. Referring to "purposes for which Y would have been permitted to use or disclose the personal data" implies that X must comply with laws in the jurisdiction of Y, and that X cannot use the personal data in the manner permitted by PDPA if inconsistent with foreign law applicable to Y. No doubt X should comply with foreign laws applicable to X, but not those applicable to Y. 4. We note that sub-paras 11(4)(a) and 11(5) do not specify when the personal data collected from Y must be returned or destroyed. Following a business asset transaction, organizations may need to retain transaction data for recordkeeping, audit or reporting purposes. Certain relevant personal data, for example, may be retained in minutes of Board meetings, which must be preserved by law. In any case, organizations must already comply with the Retention Obligation, and cease to retain the data if no longer required for the purposes collected or for other legal or business reasons. In view of this, we respectfully submit that sub-paras 11(4)(a) and 11(5) may be deleted. 5. Regarding the requirement to notify the data subjects that the transaction has taken place and that personal data about them has been disclosed, we seek your consideration to dispense with this requirement in cases where consent of the data subjects had been obtained for the

		disclosure. We would also be grateful if you would allow notification by way of newspaper advertisement or website notice or other public announcement (for example, via SGX).
10	Access to personal data	The new section 21(4) states " An organisation must not inform any individual under subsection (1)(b) that the organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made without the consent of the individual under this Act or any other written law". In many cases, customers/employees have given their general consent to disclosure for law enforcement purposes. To preserve the intent of section 21(4), we propose for your consideration amending the words underlined above to "without requiring the consent of the individual".
12	Notification of Data Breaches	1. The new provisions provide that a data breach is notifiable if it results in or is likely to result in significant harm to the affected individual. Notification must be made to PDPC and the affected individual. 2. However, the individual need not be notified if the organisation has taken measures that render it unlikely to result in significant harm to the affected individual. 3. We respectfully submit that if actions taken render the breach unlikely to result in significant harm, the breach would no longer be a notifiable breach by definition. Hence, we seek your consideration to remove the requirement to notify the PDPC in such cases. The PDPC could issue guidelines as to the acceptable measures, to ensure that it is still notified if the measures taken do not meet the expected standards. 4. We note that categories of data will be prescribed, which if compromised in a data breach will be considered to result in significant harm. Significance and likelihood of harm may depend on other factors at play, such as the number of persons to whom disclosure was made or whether there was malicious intent. We respectfully submit that falling into a specified category should not be the sole criterion for determining whether significant harm is likely to be caused.
13	Porting of applicable data	1. Please prescribe that data porting requests must be made in writing, and please consider

		allowing requests to be refused if the data relates to legal proceedings, as the usual discovery proceedings should apply instead. 2. Please clarify examples of circumstances where a request would not be considered to be made in P's "personal or domestic" capacity. Does this imply an obligation on the organization to check why the request is being made, and would obtaining a declaration from P be sufficient?
34	Amendment to the Eighth Schedule to include the "ongoing relationship" exemption	We note that the new sub-para 1(e) does not say that the message must be related to the subject of the ongoing relationship. Please clarify if this is still a condition for organizations to send messages when in an ongoing relationship with the recipient.