Data Protection Act (DPA) – Banks' Feedback

	Questions in relation to objectives and principles of proposed DP framework: ***Question 1: Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?*** ***Question 2: With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations?***
Bank A	Qn 1 & Qn 2: No concerns with proposed concurrent application of general and sectoral DP frameworks.
Bank B	Qn 1 & Qn 2: We recognize the need for a general data protection (DP) law to cater to sectors that are unregulated currently. However, the banking industry is already subjected to stringent banking secrecy requirements under the Banking Act which provide sufficient safeguards to protect customers' personal data. Thus, we would seek to exempt the banking industry from the proposed DP law.
Bank C	As a bank in Singapore, we are subject to stringent banking secrecy obligations under the Banking Act. Under section 47 of the Banking Act, a bank in Singapore is prohibited from disclosing customer information to any other person except as expressly provided in the Banking Act. In addition, a bank is required to collect customer information to provide the banking services mandated by the customer, and to comply with know-your-customer (KYC) and anti-money laundering requirements. An overlap is foreseeable if there is concurrent application of the DP law and banking regulations applicable to banks. The DP law proposes to regulate the collection, use and disclosure of "personal data". On the other hand, a bank is required to collect customer information for the said purposes and the use and disclosure of customer information is restricted pursuant to the Banking Act. Paragraph 3.8 of the DP Consultation Paper provides that sectoral regulators may apply to the Data Protection Commission (DPC) to exempt their licensees from specific requirements under the general DP law where necessary. Would DPC be open to exempt banks regulated by MAS from the application of the DP law (with regards to collection, use and disclosure), especially if the regulations applicable to banks prescribes more stringent requirements?
Bank D	Qn 1: No comments. Qn 2: Existing sectoral regulations, such as the Third Schedule of the Banking Act, and the Third Schedule of the Trust Companies Act, permit disclosure of "customer information" and "protected information" in certain situations. It should be made clear that the concurrent application of the DP law is not intended to interfere with or limit such existing provisions permitting disclosure – i.e. whatever disclosures are currently permitted under the Banking Act and Trust Companies Act will continue to be permitted and such legislation should have precedence in the event of conflict with the DP law.
Bank E	Qn 1: Para 2.9: Approval for Software As Service / cloud computing initiatives in SG has been low so far. If the introduction of this DP law makes such initiatives more viable, it would be good for the regulators to make a statement to this effect on onshore cloud computing (data held in SG) and offshore cloud computing (potentially approving use of clouds in countries with other DP laws). Qn 2: Having concurrent application of DP law with existing sectoral regulations may not be necessary unless the data could potentially be used for illegal activities or if the safeguards in that specific sector are not comprehensive enough.

Data Protection Act (DPA) – Banks' Feedback

	The concurrent application of DP law could impose more stringent DP standards. Given that Section 47 of the Banking Act already provides for stringent guidelines in respect to the disclosure of customer information, ABS may wish to consider asking MAS to seek exemptions for banks from the DP Act.
Bank F	Qn 1: Generally in support of the proposed DP law. Agree to the 'complaints-based' approach. Qn 2: No issue with concurrent application for proposed DP law with existing sectoral regulations.
Bank G	Q1: The proposed baseline approach seems flexible enough not to cause us huge issues. Q2: Given SIngaporean banking secrecy, we expect that our sector will already reach the baseline standard and will not find the new regulations difficult to meet. There will likely be some adjustments to how we handle certain client data and certainly employee data internally, but achieving these would not be too difficult.
Bank H	Qn 1: Singapore is an Open economy and a democratic country. So there will bound to be varying impact on those businesses that need personal data to grow their business such as Tourism, securities investment houses or share/property brokers and even Casino. Therefore it is best for Singapore to have a general DP law sooner so as to follow the international trend. Also the DP regime will teach business entrepreneurs to respect their customers /consumers right of privacy. Qn 2: It might not be feasible to have centralized agency to regulate the whole business community as the task is really immense. For example, in banking and finance sector alone, the sectoral regulations are already bulky to implement or comply. Imagine, all Financial Institutions will need to meet or comply with another set of national DP law. Too many rules will discourage entrepreneurship. Hence there should be a separation in regulations.
Bank I	Q1 and Q2: No, as banking secrecy has already been regulated.
Bank J	We welcome the introduction of consumer data protection regulations in Singapore as outlined in the MICA Consultation Paper dated 13 September 2011 ("the CP"). We consider that existing relevant sectoral regulations, as set out in the Banking Act Cap. 19, and the proposed data protection ("DP") regulations, are able to operate concurrently. We consider that the Banking Act represents a high standard with respect to the protection of personal data that comes within the meaning of customer information. On this basis, we consider that the rules and exemptions with respect to the treatment of customer information under section 47 and the Third Schedule of the Banking Act should apply in preference to the DP regulations with respect to such information.
Bank K	Where existing sectoral regulations and the DP law cover the same ground, the provisions of the existing sectoral regulations should take precedence and apply, especially any applicable exemptions and exceptions (such as exceptions to banking secrecy in the Banking Act). This would minimize the impact for sectors that are already regulated and provide clarity. The DP law should clarify this instead of leaving it to sectoral regulators to apply for specific exemptions. This would minimize the impact for sectors that are already regulated and provide clarity. Moreover, the DP law is only applicable to data of natural persons. However, sectoral regulations may have a wider reach. Should there be obligations in the DP law that are not required by sectoral regulations (e.g. solicitation/marketing activities via telephone, fax,

	SMS), and the sectoral regulators do not apply for specific exemptions or apply for an exemption but fail to obtain an exemption, this could potentially result in different standards and treatment being applied to customers who are natural persons and customers who are not natural persons.
	Questions in relation to the definition of "personal data": ***Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?*** ***Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?***
Bank A	Qn 3: Would "personal data" cover user comments or feedback on social media pages? Qn 4: it's not a concern if DP covers deceased because during campaigning we filter out the deceased customers based on information we have at that time. However, as we do not automatically receive death registration from government / official source we may unknowingly campaign a deceased customer.
Bank B	Qn 3: We would like to seek clarifications on the definition of "personal data" as follows: Sole proprietors, partnerships, companies etc are considered non-individuals and do not fall under the definition of personal data. As such, personal data of individuals under such corporate setups shall be excluded from the scope of personal data. We propose that the following shall not be specified as personal data as the information is subject to change and may not indefinitely represent an unique individual's identity. - Contact numbers - Email addresses - Home addresses In addition, based on the banking secrecy requirements under the Banking Act, disclosure of customer's address and contact numbers are permitted for the promotion of financial products and services to customers (between FIs regulated by MAS). In this case, the banking sectoral regulations have already taken into consideration data protection. Qn 4: As it is administratively complex, in terms of tracking the timeline of 20 years, identifying customers whom the Bank is not informed by relatives that they have passed away or to even obtain consent from the living relatives of the deceased, the proposed DP law should not apply to personal data of the deceased.
Bank C	No comments on the proposed definition of personal data, except for our comments below in relation to whether information such as recycled phone numbers are considered personal data of the previous individual for the purposes of the National DNC Registry. Our view is that the DP law should not cover the personal data of the deceased, which position is consistent with UK's Data Protection Act. The Singapore Banking Act permits the disclosure of customer information to (a) the personal representative of the deceased, or (b) any person in connection with an application for a grant of probate or letters of administration, and recipients of such

	customer information is not prohibited from making further disclosure to any other person. Accordingly, we are of the view that the DP law should not cover the personal data of the deceased.
Bank D	Qn 3: The proposed definition of personal data appears appropriate. We are of the view that it should cover information of deceased persons with no time limit as imposing a time limit seems arbitrary. Qn 4: No comments.
Bank E	Qn 3: The definition of personal data is very vast and open. We suggest that there should be a definitive list of the types of personal data hardcoded into the DP law for clarity. Qn 4: There is no need for the DP law to cover deceased persons as there is no new business to be done with such persons.
Bank F	Qn 3: Propose that mobile numbers be excluded from definition of personal data as this can change over time and as such, not a permanent identifier of the person. Qn 4: The proposed DP law should be applied uniformly for all customers, living or deceased. Given the complexity of handling deceased individual's information and the challenges that the organizations may face in verifying the individual's status, it will be difficult to accord different level of protection for living vs deceased individuals. This will ensure that data held by different organizations are handled the same way, regardless of whether they had registered their deceased status or not with the respective organisations. Whilst it seems reasonable to set some level of protection for individuals who have been deceased, it will be difficult to administer them if the minimum standard is set at 20 years. Currently, there are prescribed record retention policies specified within sectoral regulations. Hence, such information is not likely to be readily available in the organizations if the period set for the proposed DP law falls outside these record retention period. To achieve a consistent and balanced approach while minimizing compliance cost for organizations, we propose that the record retention policies prescribed within the sectoral regulations should be taken into consideration when deciding the retention period of such personal data.
Bank G	Q3: The definition of personal data meets international standards and appears to be workable with. Q4: Banking secrecy provisions already sufficiently protect the privacy of deceased people, from a banking industry perspective we would not see a requirement for additional measures.
Bank H	Qn 3: The word "information" or "personal data" has to be elaborated in greater details. Qn 4: DP law is to prevent disclosure of a living person or natural person PD whose legal rights of privacy are protected by Common Law in the absence of statutory law (or proposed DP law). However, when a person dies whether testate or intestate, its personal representative needs to apply to Court for either a Probate or Letter of Administration (LA). At that point in time, the deceased's PD would come to light. So where is the need to protect or "hide" the deceased personal data. But in the sectoral regulation like Banking Act Cap 19, irrespective of whether the customer is dead or alive, the FI must not disclose anything without the customer's personal representative's consent or in the absence of an Order of Court for probate or L.A.

	Assuming DPC wants to load in the DP law in the case of a deceased person, why place an additional administrative burden to make sure the DP can only be disclosed AFTER 20 years. Why 20 years?. Under Singapore Limitation Act the right to sue based on a contractual breach is either 6 or 12 years.
Bank I	Q3: The definition is vague and leaves many questions and interpretations open; thus guidelines would be crucial (cf. also 3.12, 3.14 and 4.10). Q4: It should cover personal data of deceased. Otherwise, it will be difficult to distinguish.
Bank J	We consider that the proposed definition of "personal data" may benefit from a clarification that it is information about an individual whose identity can reasonably be ascertained from such information. This is consistent with the intention of the DP regulations as specified in paragraph 3.11 of the CP. We suggest MICA consider the terms of the Banking Act with respect to the right to disclose information with respect to deceased customers (reference: Third Schedule, Part I paragraphs 1 and 2): 1. Disclosure is permitted by the appointed personal representative of the deceased customer; 2. Disclosure is in connection with an application for a grant of probate or letters of administration in respect of a deceased customer's estate. In other respects, we are likely to apply the same standards regarding the use, disclosure, retention, destruction, etc. of personal data of living and deceased individuals as in many instances we may not be aware of an individual's death (other than in the case of employees). On this basis, we generally consider that the approach suggested by MICA is appropriate.
Bank K	For clarity, we propose that the definition of "personal data" should be clarified to include information regardless of whether the information is accurate or not.
	Questions in relation to the organisations and activities covered by the DP law: ***Question 5: Do you have any views / comments on the proposed organisations covered by the DP law?*** ***Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations?***
Bank A	Q5: No comments Q6: No comments
Bank B	Qn 5: Refer to comments under Qn 1 and 2 above. Qn 6: The DP law needs to address the treatment of such organizations to ensure level playing field and consistency in terms of data privacy expectations.
Bank C	We have no comments on the type and size of organizations to be covered by DP law. We also have no comments on whether DP

	law should extend to organizations located outside Singapore. However, as commented above, our view is that there may be overlap between the DP law and the banking regulations applicable to banks in Singapore. The Banking Act prohibits disclosure of customer information of a bank in Singapore to branches of that bank outside Singapore (unless it falls within one of the exemptions under the Banking Act).
Bank D	Qn 5 and 6: Like some legislations with extra territorial reach, an important legislation like DP law should protect personal data collected from persons in Singapore. That should be the starting baseline. The enforceability issue should be considered separate from the principle of the DP law.
Bank E	Qn 5: No comments. Qn 6: The DP law should only be extended to organizations located within Singapore and for locally incorporated companies. It would defeat the purpose and undermine the DP law if it is not enforceable.
Bank F	Qn 5: No comments. Qn 6: Agree that proposed DP law should extend to organizations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore. This is especially important as cross-border data transfers become more commonplace with market developments like cloud-based computing.
Bank G	Q5: No comment. Q6: No comment.
Bank H	Qn 5: The DP law is to build consumer confidence and protect Singapore image. So all activities that collect, uses and store personal data from natural persons including corporate and unincorporated bodies should be covered. Why make exceptions? Qn 6: If the international standards as used in the UK and EU include organizations resident outside UK and EU, then in that case Singapore DP regime should follow. This is commonsense. Why allow a culprit to mess around the home country law. Identify the breach and the culprit first. How to address or penalize the culprit will come next. Enforcing punitive measures (like starting a court action in Singapore) against the foreign party are obvious not going to work because of the careless attitude of the foreign party and also the inability of the local court lacking jurisdiction to trial a defendant not subjected to Singapore law. One way is to post a Webpage at the DPC website stating those alien organizations that had breached Singapore DP law. DPC should start a campaign to tell the public that any data furnished to such alien organizations are furnished at their own risk.
Bank I	Q5: No comments. Q6: Although it is difficult to enforce, It should include organizations outside Singapore. The question is whether the law should only apply to organizations located in Singapore or also to those collecting data in Singapore only. The latter has some issues on enforcement, but even if not always enforceable, it is a hurdle anyway and having a law applying to them gives at least a chance to address issues.
Bank J	It appears that foreign companies that have registered under the Companies Act, such as our bank, would be considered an "organisation" within the meaning of the proposed DP regulations. We believe it would assist organisations if this interpretation was

	expressly confirmed. We agree with MICA's view that it is likely to be difficult to carry out effective investigation and enforcement actions with respect to the activities of offshore organisations that engage in data collection and/or processing in Singapore. We consider it appropriate for offshore organisations to be subject to any regulations that would apply in their "home" jurisdictions.
Bank K	No comments.
	Questions in relation to the general exclusions from the DP law: ***Question 7: Do you have any views / comments on the proposed general exclusions from the DP law?*** ***Question 8: With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?*** ***Question 9: Are there any other exclusions that should be catered for under the DP Act?***
Bank A	Q7: Even with explicit contest T&Cs, would organizations still be allowed to reveal identities of contest winners (e.g. lucky draws) in the media without contravening the proposed DP regulations? Q8: No comments Q9: No comments
Bank B	Qn 7, 8 & 9 : No comments.
Bank C	In our view, customer information collected by a bank for purposes of KYC and prevention of money laundering should be one of the general exclusions from the DP law. Similarly, the use or disclosure of customer information for the purposes of reporting suspicious transactions to the relevant authorities should be excluded as well. In addition, collection, use and disclosure of personal data for the purposes of providing banking services in which the customer has instructed or mandated the bank should also be excluded from the DP law.
Bank D	Qn 9: If a person has by specific consent or implied action agreed to put his information in the public domain, that should be excluded from the DP law.
Bank E	Qn 7: No comments. Qn 8: No comments. Qn 9: Data that is used for non-profit or non-monetary gains should also be excluded.
Bank F	No comments.
Bank G	Q7: We are not affected by the exclusions, so no comment Q8: As Q7 Q9: None that we would see
Bank H	Qn 7: The general idea of the proposed exclusions is that those PD made available by news organization to the public will be

	exempted or excluded from DP law. That gives the impression the power of the press over-rides the DP law. That could not be the intention. Instead of exempting news organization entirely, the exclusions should only relate to those PD that are found in court documents. The other exclusion will be record of documents that contain PD. Qn 8: This is a matter of culture differences between the West (UK and EU) and the East. Artistic value and literature are not so prevalent in the East. One way is to set the criteria that if the PD are in respect of public performances of an artistic and literary nature. Qn 9: The criminal record kept by the law enforcement agencies such as CID and CAD. The bankruptcy records or other civil cases kept by the Official Assignee or The Public Trustees.
Bank I	Q7: No comments. Q8: No comments. Q9: No comments.
Bank J	We consider that the proposed DP law should contain a general exclusion with respect to the collection, use, disclosure, retention, destruction, etc. of personal data where it is already subject to specific sectoral regulations, such as the Banking Act, to the extent that such sectoral regulations apply an equivalent or higher standard of protection of such data. Further, we suggest that the sharing of personal data with related companies be subject to a general exclusion to the extent that such related companies are subject to equivalent regulatory standards with respect to the collection, use, disclosure, retention, destruction, etc. of personal data.
Bank K	For clarity, the DP law should provide for an exception to permit an organization that collects data to disclose the information to its head office or affiliates who need to know. This is because the organisation in Singapore may need to disclose the information to its head office or affiliates for internal purposes such as risk management or reporting purposes. Alternatively, it should state clearly that where sectoral regulations permit an organisation to disclose such data, the organisation will be permitted to do so in accordance with the conditions in such sectoral regulations.
	Questions in relation to the general exclusions from the DP law: ***Question 10: Do you have any views / comments on the proposed general rules under the DP law?*** ***Question 11: With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?***
Bank A	Q10: No concern with similar treatment of data controllers and data processors. Q11: This "opt-out" approach may be more cost-effective. Reasonableness of notice should be studied. In any case, individuals should still have accessible avenues to "opt-out" subsequently.
Bank B	Qn 10: When an individual has given consent for the collection, use or disclosure of personal data, e.g. for a bank's sales and

	marketing purposes, it shall be deemed as consent given for that purpose and shall apply to all promotional activities of the bank regardless of areas and products. Customers can choose to unsubscribe if they do not wish to receive any promotional advice from the bank. Qn 11: We opined that an 'opt-out' approach, where individuals register any objection within a reasonable timeframe, will be more practical and cost-effective. The individuals may be slightly inconvenienced but (at least) they are aware and assume some responsibility in the consumer data protection regime system.
Bank C	In our view, the DP law should provide for flexibility for organizations to adopt a deemed consent approach.
Bank D	Qn 10: Pursuant to the Banking Act, the Bank is restricted from providing the customer information to any third party unless it is permitted under the Third Schedule of the Banking Act. Accordingly, the Bank will be required to obtain the customer's consent to provide information to third parties (authorities/enforcement agencies) and the consent obtained from the customer should not be solely for the provision of products and/or services. The Bank should be allowed to obtain a broader consent in order to facilitate such disclosure. Qn 11: It would be operationally efficient to have an "opt-out" method of obtaining consent, in addition to the other stated methods of obtaining consent. Many individuals do not actually have any issue with giving consent, but simply do not bother to respond to an organisation's request to provide consent. With regard to the requirement for the organisation to "notify" the individual and give reasonable time to opt out, perhaps the notification requirements should be made clear. E.g. will it be sufficient for the organization to send one letter to the individual's last-known address by normal mail?
Bank E	Qn 10 It is unnecessary to reveal the business contact information of the designated individual(s) who are responsible for the compliance to the DP Act since customers can contact the bank via the call centre, helpline, enquiry mailbox or any other method. Qn 11: Agreeable on such an approach. The opt-out approach is efficient and equitable to customers. Customers generally do not mind disclosing data since they are aware of such an action from the organization. However, for those customers who are insistent on not disclosing their data for other use, they still have a choice to opt out. Furthermore, it would be operationally challenging and costly for the organization to adopt an opt-in approach. General Comments: Paragraphs 3.31, 3.40, 3.41 and 3.49 - An organization is required to obtain the individual's consent for collection, use or disclosure of personal data. An organization may also not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal date beyond what is necessary to provide the product or service. This may have potential implications on the "consent for disclosure" clause currently used in the Bank's terms and conditions and application forms because they are drafted very widely to cover consent for disclosure for all purposes as deemed reasonable by the Bank.

Data Protection Act (DPA) – Banks' Feedback

Bank F	Qn 10: Under Para 3.31, the organization cannot require the individual to consent beyond what is necessary to provide the product or service. This might run contrary to certain sectoral-specific provisions, like in the Banking Act where the customer's written consent may in fact be broader. We propose that it be stated expressly that 3.31 is subject to specific sectoral legislation providing otherwise. As for Para 3.32, we agree that there should not be a detailed prescription of the manner in which consent is given, whether implicit or explicit bearing in mind that there is likely to be additional compliance costs associated to maintaining customer's preference. Qn 11: It is administratively cumbersome and also costly for organizations to require express consent to be given from time to time, especially if under Para 3.31, prior consent if given was in respect of a specific product or service. Possible solutions would be: 1. allowing the consent to be given on a wider basis, especially if the organization contemplates further products or services that may be offered that may require consent to be obtained 2. the "opt-out" approach whereby consent is deemed to be given when individuals are notified of an organization's intent to collect, use or disclose their personal data, but do not register any objections within a reasonable timeframe. Regarding Paragraph 3.36, we are of the view that giving an individual the right to withdraw his consent to the collection, use or disclosure of his personal data will give rise to practical and administrative difficulties for the organization e.g., operational functions may already have been outsourced to third party service providers. This is not something that can be resolved by passing the related cost to the customer, because where data is collected and disclosed as part of an outsourced service solution, it is not realistic practically to require the organization to cater to individual consent withdrawal requests at a later stage. The practical solution might be for the organization to terminate the provision of services to the individual, and that can be initiated by the individual (in the case of a banking customer, the customer can close his accounts with the bank).
Bank G	Q10: No comment. Q11: We would support this proposal from a business perspective, as it allows greater flexibility in collecting data.
Bank H	Qn 10: DP law should be thorough and define what is explicit consent and what is implied consent. It should also penalise and barred the culprit organisation from collecting, using and disclosing, accessing and storing PD indiscriminately. Also the rules should spell out what happens to those PD stored in the collecting organisation if it were voluntary or compulsorily dissolved. Qn 11: The exceptions for collecting PD should not be freely given to any private or public organization otherwise it would defeat the purpose of having a robust DP law. Therefore prior notice to use disclose and store should be given to the individual and allow reasonable time for the person to agree or disagree. Also the purpose for using and disclosing the PD should be made known. That will make the DP law very fair and transparent to everyone.
Bank I	Q10: No comments. Q11: Explicit consent should be provided. The reason for explicit consent is that an individual should make a conscious decision on his/her data and that the default should be on the protective side, i.e. no consent.
Bank J	We consider that it would be helpful to understand if MICA considers that organisations that are provided with personal data by other organisations (e.g. pertaining to such other organisations' employees and/or authorised representatives) need to exercise any

	particular care or due diligence. On the basis that, as specified in paragraph 3.32 of the CP, consent may be explicit or implied, we have no comment with respect to the "opt-out" approach as described in paragraph 3.35 of the CP.
Bank K	No comments.
	Questions in relation to the proposed rules on collection, use and disclosure of personal data: ***Question 12: Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?*** ***Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?*** ***Question 14: Do you agree with the proposed approach to the transfer of personal data***
Bank A	Q12: Under section 3.49, what will be the expected guidelines for purchasing prospects lists from third parties? E.g. to what extent is the purchasing company required to check that the party selling prospect lists has obtained consent to pass information to us? Q13: No concerns. Exception may need to be provided for business practicality reasons e.g. identifying an individual as a customer or cross-border work with overseas offices within the same organization. Q14: Banks may be required to transfer data outside SG for analytical work to be performed, for e.g. to a more cost effective country, in the foreseeable future (if not already for some). Therefore, the 'principle based' approach versus a more prescriptive approach is more appropriate.
Bank B	Qn 12 and 13: For collection of personal data, we are working within the framework of the bank and according to stipulated guidelines. A one-time customers' consent, be it implied, explicitly or implicitly, for the use of the personal data information should be sufficient, unless customer withdraw the consent in writing. On the point where it was proposed that organization must disclose the business contact information of an officer or employee of the organization who is able to answer any questions the individual may have about the collection of his personal data, we opined that the proposal is overly prescriptive. The essential point is to stipulate the need to have a at least one contact point to handle such enquiry and not prescribe the form nor mode acceptable. In banks' context, customer can post questions about the collection of his personal data, via call centre, email etc. Once the touchpoints receive such enquiries, they can forward the request to a centralized department who may be able to assist to collate the information required before reverting back to the customer. By having more touchpoints, it will also alleviate customer service issues e.g. staff is on leave and no one attend to the request. Qn 14: Existing Banking regulations have catered to such scenarios. The onus on the organization to ensure appropriate measures

	have been taken to protect personal data transferred outside Singapore shall cease to apply in situation where customers have given explicit consent for disclosure to be made to 3rd parties.
Bank C	We have no views on the proposed rules on the collection, use and disclosure of personal data except to repeat our comments that it may overlap with the sectoral regulations applicable to banks. A bank in Singapore is regarded as "ring-fenced" for the purposes of banking secrecy. A bank in Singapore is restricted from disclosing customer information to its branches (let alone affiliates) outside Singapore unless it falls within one of the exemption under the Banking Act.
Bank D	Qn 12: We agree with the principles of DP law. The collection of data from persons should clearly disclose the proposed use. This will make an organisation's usage of the information more efficient as the person would be open to being approached for the stated reason. With reference to paragraph 3.41, the Bank is bound by sectoral laws (Banking Act) which prohibit the disclosure of customer information (unless permitted under the Third Schedule of the Banking Act). The requirement to "notify" is mentioned at paragraph 3.44. Does MICA propose to prescribe the manner in which notification may be given? Qn 13: Principle of DP laws is the protection of personal information, then we are of the view that any exception to such rule must solely be for and in the interest of the person involved and not efficiency of the organisation (exceptions should be due to medical reasons, national security etc). With regard to the exception for outsourcing set out in paragraph 3.48, it should be made clear that this exception also applies where:- (a) an organisation outsources the collection or processing of personal data to multiple organisations; and (b) an organisation outsources the collection or processing of personal data to another organization, which in turn further outsources to another organization, and so on (multiples levels of outsourcing or data transfer), provided of course the other criteria in paragraph 3.48 are satisfied. Qn 14: For organizations which are already subject to strict sectoral regulations, it would be helpful to confirm that the measures currently required to be taken are sufficient. E.g. for Banks, will compliance with the MAS Guidelines on Outsourcing be sufficient to meet the "appropriate measures" requirement set out in paragraph 3.61?
Bank E	Qn 12: Please refer to our responses to Qn 10. Qn 13: For Para 3.45, it is unnecessary for organizations to seek consent for collection of members' personal data since these persons are considered as members and not any individuals loosely affiliated to the organization. As such, it is implied that their participation to the membership is voluntary and thus disclosure of the data can be considered as voluntary as well. Qn 14: No comments.
Bank F	Qn 12:

Data Protection Act (DPA) – Banks' Feedback

	1. It is proposed here that organisations need not obtain consent to collect employee personal data for the purposes of establishing, managing or terminating an employment relationship between the organisation and the individual. However, it is also mentioned that "before the organisation collects the employee personal data, the organisation should notify the individual that it will be collecting his personal data and the purposes for the collection." Presumably, the latter refers to the personal data of each employee that may not be about an individual's (e.g. marital status) employment. 2. As part of the recruitment screening and RNF screening, we conduct reference checks on Employee's education and employment history. Similarly, we may be approached by other institutions to release information on previous employee. Would the new regime apply to such cases of disclosure whereby Employee must provide explicit consent for the relevant institution/company to release the information to us? 3. Para 3.51 – We would highlight that one of the circumstances under which disclosure without consent may be allowed might be where the organisation is given to understand that there is fraud or suspected fraud involving the individual. And the disclosure is necessary either to assist the organization or the suspected victim of the fraud in investigations. 4. Question from Fund Management business: The following disclosures are made as part of the UT business operations: (a)CPF OA / SRS client details provided to CPF agent bank and distributors for daily trade processing and for quarterly reconciliation purposes. (b)CPF SA client details provided to CPF Board and distributors for daily trade processing and for quarterly reconciliation purposes. (c)CPF client trade details provided to external auditors during the fund audit process. (d)CPF client transaction / holding details are provided to law firms / public trustee only upon request received from the law firm / public trustee via request letter, attached with certified copy of death certificate and grant of probate whereby the client is deceased (estate cases) for audit confirmation purposes. Currently the fund manager does not have legal relationship with these CPF clients. Would the new regime apply to such cases of disclosure whereby CPF Clients must provide explicit consent for the relevant institution / company to release the information? Or are such disclosures excluded from the regime? 5. Comment in connection with corporate business: 1. As a bank, we receive from our corporate customers, information relating to their individual employees, which may or may not be public information. Any non-public information received will fall within the ambit of the Data Protection Act. 2. It will be administratively cumbersome and highly impractical for banks to obtain the necessary consents from the employees of our corporate customers. The onus for obtaining employees' consents should rest with their employers; ie. the corporate

	customers furnishing individuals' information to third parties. 3. To avoid the need for banks (or for that matter, any third party recipient) to generate additional paperwork to obtain from each of our corporate counterparties – (a) representations and warranties that they have obtained the requisite consents from their employees; and/or (b) covenants that they will procure necessary consents from employees, We would like to see the Data Protection Act stipulate clearly the obligation for employers to obtain the necessary consents from their employees before furnishing any employee's personal information to third parties. Recipients of personal information should be in the position to assume that parties furnishing personal information have obtained all necessary consents from the relevant individuals. Qn 13: Exception should be provided for organizations to collect, use and disclose an individual's personal data for the purpose of identifying him as a member within the organization. Qn 14. No comments.
Bank G	Q12: No comment. Q13: We are of the opinion that a static list of business exceptions runs the risk of not including a normal activity that was not thought of when the law was drafted. We would instead prefer a more flexible definition of exceptions, such as 'in the course of normal business administration' when handling staff data. Q14: Yes.
Bank H	Qn 12: At a glance, the proposed rules for Collection, Use, Disclosure, Store and Deletion seem to be adequate as these processes will relate to daily routine events like consulting a doctor, lawyer or filling up all sorts of application forms. Qn 13: Exceptions to the DP law should only be allowed where the situations requiring disclosure will directly benefit the individual concerned. But where the benefit goes to the collecting organization the DP law should not allow it. Qn 14: In the case of cross-border flow of data in banking, the FI concerned will need to comply with both the sectoral regulations imposed by the MAS mainly AML/CFT regulations and outsourcing guidelines and regulations. That means that DP law clearly should ensure that its provisions do not conflict with established sectoral regulations. The safest course to avoid conflict in law is for DP law to state that "appropriate measures" must be taken to protect the cross-border PD in transit and only to those countries which recognise DP law or have similar regulations in place.
Bank I	Q12: No comments Q13: Organizations should also obtain consent by the individuals for identification as member and internal circulation.

Data Protection Act (DPA) – Banks' Feedback

	Q14: We cannot judge whether both approaches fulfill the conditions of other major jurisdiction. In general, Singapore law should be deemed as adequate. The critical issue is whether such a solution will be accepted by other countries.
Bank J	With respect to personal data of members, we consider that such data should be subject to similar treatment to that of employees (as specified in paragraph 3.44 of the CP). We endeavour to ensure that personal data is properly managed and protected by appropriate contractual provisions with data transferees that are, in turn, also subject to appropriate governance and security controls and regulations with respect to confidential data. On this basis, we agree with the proposed approach as outlined in paragraphs 3.60 and 3.61 of the CP.
Bank K	With reference to the exception for personal data of employees in paragraph 3.44, notification by the organisation including the purposes of collection should not be necessary as long as the purposes are restricted to employment as specified in that paragraph. On a practical basis, organisations may need to use employee data for a range of purposes and such purposes are likely to change over the course of employment. Alternatively, if notification is necessary, the organisation should have the flexibility to issue a notification subsequent to collection of the personal data, especially if there is a change in the purpose of use.
	Questions in relation to the proposed rules on accuracy, protection and retention of personal data: ***Question 15: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?*** **Question 16: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?**
Bank A	Qn 15: On section 3.63, would there be mandatory requirement that organization periodically updates their demographic information of its customers? What is the expected frequency of such updates? Practicality and cost are key factors to consider in determining "reasonable effort". Qn 16: On section 3.67, would organization be allowed to contact a customer after a customer terminates their relationship with the organization? If allowed, would this window period be required to be stated in terms and conditions?
Bank B	Qn 15: In terms of customers' records, the Bank will retain physical copies of documents for the retention period stipulated by the various acts. In terms of soft copy information, e.g. customers' static info, accounts held etc, the Bank will keep the information so that the bank can satisfy, any enquiry or order from the relevant competent authorities in Singapore for information. Thus, to completely remove customers' data even if the banks have no use to it may not be feasible. Qn 16: For the banking industry, there are stipulated requirements for the retention of various records under the various Acts, thus it is difficult to determine and specify a suitable retention period upfront to the customer.
Bank C	We have no comments, except to comment that banks do keep customer information updated for the purposes of providing banking

	services and KYC purposes. Customer information is also retained for the required period for the purposes of KYC and other purposes.
Bank D	Qn 15: This does not seem practicable.
Bank E	Qn 15: For Para 3.66, It should be defined what it means by 'directly affects the individual' and should exclude this rule for marketing decisions. If an organization is making hundreds of business decisions everyday on what marketing offers a customer receives based on customer's data, it is impractical to expect that the organization retains these data which could be different at the point where the decision is made. Also businesses should not be required to allow customer to access these data as it will reveal business practices and erode business competitiveness. Qn 16: Para 3.67: companies should not be required to specify the data retention period as this will vary from attribute to attribute. Some data (such as IC or name) are relevant for the lifetime of the relationship with the individual (more than 50 years for some customers), whereas other attributes may only be valid for a short time period (e.g. income or email address). In a single account opening, the bank may capture 20 pieces of information on a customer – all with potentially different retention periods.
Bank F	Qn 15 and 16: It may not be practical for organisations to specify retention period at the point of collecting the personal data as not all personal information need to be treated with the same retention period. Similar to our response to Qn 4 above, this is managed within the record retention policies prescribed within the sectoral regulations and we propose to keep the approach consistent. However, when asked and consistent with existing practice, the organization will respond to specific questions regarding retention periods relating to specific types of documents.
Bank G	Q15: We would expect that the requirements under the DP are not stricter than those under the Banking Act. Q16: Specific retention periods are problematic as physical removal of electronic records is complex - e.g. old HR data on backup tapes. We would rather see retention for 'as long as the business purpose for retaining the data exists' - this gives us more flexibility.
Bank H	Qn 15: The onus to provide accurate information or PD falls on the individual. DP law cannot provide penalty for careless mistake by the individual. The onus to protect and store the PD must be the collecting organisations . However, there are existing rules of law like the Limitation Act providing a maximum period of 12 years for a claim to be made by an aggrieved party. The Companies Act provides 7 years to retain record and The MAS 626 Notice on AML/CFT (Anti money Laundering & Counter Financing of Terrorism) states a retention period of 6 years. Qn 16: Personally, all PD will become outdated in a matter of months. So it is quite pointless to keep outdated data for more than a year. Some organisations like Personal insurance require update of PD every year especially banking FI (Financial Institution) whose internal loan policy requires guarantors' particulars to be updated yearly.
Bank I	Q15: No comments Q16: No comments
Bank J	In light of the nature of the organisation, we have implemented a global standard with respect to the retention of records which provides, in general terms, that records be retained for a minimum specified period of time or such longer period as may be required (e.g. in light of potential or actual litigation). We look to destroy or anonymise personal data records that are no longer required for legal or business purposes, depending on the particular context, in line with its global standard. We consider that any absolute

	requirement to do so within a certain period, and any obligation to advise personal data providers at the time of collection of such requirement, may be unduly onerous on organisations such as us.
Bank K	The DP law should clarify that the onus of updating any change to the personal data lies on the individual and not the organisation collecting the data. Organisations should not be required to specify the retention period. The retention period will depend on the nature of the data and the relationship of the organisation with the person. As this may change over time, specifying a retention period at the time of collection may not be practical.
	Questions in relation to the proposed rules on access to and correction of personal data: ***Question 17: Do you have any views / comments on the proposed rules on access to and correction of personal data?***
Bank A	Qn 17: No comments
Bank B	Qn 17: We agree to impose a fee to charge customers on such retrieval of personal data.
Bank C	We are of the view that only existing customers of the bank should be allowed to access and correct their personal data.
Bank D	Qn 17 : Paragraph 3.71 states that "This exception also applies if the disclosure of the information would reveal confidential commercial information that if disclosed, could, in the opinion of a reasonable person, harm the competitive position of the organisation." It would be useful to confirm whether "confidential commercial information" would cover information on an organisation's outsourcing structure/relationships with vendors. Pursuant to 3.72, banks should be excluded from having to allow individuals access to their personal data or information because it would not be practical for the bank to disclose how the customer's data has been or is being used by the bank.
Bank E	Qn 17: Pt 3.68: The bank maintains many different banking systems which may all contain some elements of customer related data such as their transactions. It is not physically possible to provide a customer with a copy of all of their personal data and so guidelines should be set on the types of information that should be provided – for example, demographic, contact information would all be valid – whereas items such as a bank derived credit score should not be shared. Pt 3.68: Providing the names of the individuals to which data has been disclosed is also not realistic. CRM systems make customer data visible to a wide (but controlled) number of people within the bank to enable them to perform their duties – it's not practical to list all the users of the CRM system which have access to an individual's record. Para 3.69 – With reference to "Such corrected data should also be sent to any other organizations to which the personal data was disclosed during the year before the date the correction was made". This may not be necessary if the other organization does not need the information anymore as at the date of correction.

Data Protection Act (DPA) – Banks' Feedback

Bank F	Qn 17: As the organisation (eg. a bank) offers a suite of products and services to its customers, and the organisations to which customer data may be disclosed to will depend on the type of products and services that were offered and accepted by the customer, it is administratively not possible for the organisation (the bank) to maintain an accurate list of the organisations to which the data might have been disclosed to, in respect of any particular customer, at any one point in time. As an alternative, we would propose that a list of possible organisations which the individual's data might have disclosed to, be maintained, and that when requested, this list may be made available to the individual. It is not practical to require the disclosure of the specific names of the individuals in such organisations who might have been disclosed the data.
Bank G	Q17: This section is currently vaguely worded and will have to be more specific in final draft, or else many organisations will evade disclosure or charge large fees. However, we see nothing in the current format that is a problem for us.
Bank H	Qn 17: DP law is designed to protect the individual or legal person. Therefore it should allow the legal right to update or ask for the data destruction if and when the purpose is done.
Bank I	Q17: Ideally, individuals should be notified so that they will know how long their data is kept.
Bank J	In respect of individuals' requesting access to their personal data, we wish to understand the purpose and utility underlying the suggested provision of the names of individuals, in addition to details of organisations, to whom such data has been provided as this may also be considered as confidential information that needs to be properly managed. Of course, if required to comply with Singapore law as part of a discovery or other investigatory exercise in connection with legal proceedings or regulatory investigation, such information would be provided. We are concerned with respect to the potentially onerous impact, in terms of time, cost and administration required, of responding to frivolous or vexatious requests. We believe that organisations and individuals would benefit if the DP regulations were detailed as to meaning and scope of frivolous or vexatious requests. We would also like to propose that MICA consider whether organisations and individuals may contract directly with respect to the circumstances in which access to personal data would be provided as this may achieve greater clarity and reflect the requirements of both organisations and personal data providers. With respect to paragraph 3.69 of the CP, we consider that it should only be necessary to advise other organisations of "corrected" personal data to the extent that the relevant connection or relationship with the provider of the personal data is continuing or it is otherwise appropriate to do so. If there is no utility with respect to such correction, we consider that it should not be required.
Bank K	As the proposed definition of "personal data" is very wide, it would arguably include information about an individual which may be the result of an organisation's analysis of the raw data that was collected from the individual. The DP law should clarify that the individual should only be entitled to access and update such data that was collected from the individual but not information on the individual that was prepared or processed by the organisation based on the data that was collected. Information prepared by the organisation belongs to the organisation and the organisation should not be required to disclose this as the processed information may contain other information which may be confidential to the organisation. There are also concerns that making such processed information available to the individual may result in individuals who "fish" for such processed information, especially individuals who are disgruntled with the organisation, and thereby also indirectly cause an increase in the number of frivolous complaints or litigation cases. Therefore, such confidential information should only be made available in accordance with the process in normal court proceedings.

Data Protection Act (DPA) – Banks' Feedback

	Questions in relation to the proposed penalty and enforcement regime: ***Question 18: Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?*** ***Question 19: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?***
Bank A	Qn 18: What documentation would organizations be required to keep to show that they have complied with DP regulations? How long would the documentation need to be retained? Qn 19: No comments
Bank B	Qn 18 & 19: Enforcements shall be balanced, taking into consideration interests of customers as well as that of organizations. Penalties shall apply to the correct context, and not a standardize rule across the board. The banking industry is already governed by its sectoral regulations and in the same context, the penalty of the proposed DP law shall not be more stringent than that of the sectoral regulations.
Bank C	No comments.
Bank D	Qn 18 & 19: No comments.
Bank E	Qn 18 & 19: No comments.
Bank F	Qn 18: No comments. Qn 19: We propose that penalties should be imposed taking into consideration the number of repeated breach and magnitude of breach which are quantifiable measures or a reasonable level.
Bank G	Q18: The proposal seems a fair one. Q19: Although the proposed fines appear to be larger in international comparison, we do not see that being an issue for our bank as these fines are aimed at deliberate abuse.
Bank H	Qn 18: Enforcement notices should be publicised so that would-be consumers will be forewarned or prevented from giving away their PD unknowingly. The Appeal Board will act as a check and balance to the DPC. Qn 19: What are exactly the situations or events that will trigger a breach of DP law are more importantly to be considered and made known and then defined in the DP law. Whilst penalty or punitive measures should be melt out, such punishment should be commensurate with the nature and extent of the breach. A deterrent sum of S$1 million is surely designed to "bankrupt " culprit but it will not solve the problem.
Bank I	Q18: No comments.

	Q19: No comments.
Bank J	We agree with the views as expressed in the CP with respect to the proposed penalty and enforcement regime.
Bank K	No comments.
	Questions in relation to transitional arrangements: ***Question 20: Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?***
Bank A	Qn 20: No comments
Bank B	Qn 20: No comment.
Bank C	Please see our comments below in relation to Questions 20-22.
Bank D	Qn 20: No comments.
Bank E	Qn 20: No comments.
Bank F	Qn 20: Agree to a 'sunrise' period and would recommend that a minimum of two years be granted. While the DP regime is intended to protect the interest of consumers and safeguard individual's personal data against misuse, we propose that this be balanced against the need for consumers to take ownership of their personal data to avoid irresponsible disclosures.
Bank G	Q20: Nothing to add.
Bank H	Qn 20: Why not copies the Model Code since these are industry best practices recommended by OECD.
Bank I	Q 20: The definition of what data should be protected is of high importance in order to achieve a consistent approach across organizations and to achieve to goal.
Bank J	We consider that it would be useful that the DPC issue guidance on the meaning of "personal data" in terms of what data types could be considered as reasonably capable of resulting in the relevant individual's identity being ascertained.
Bank K	No comments.
	Questions in relation to transitional arrangements: ***Question 21: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate?*** ***Question 22: With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?*** ***Question 23: Are there certain organisations that may require different transitional arrangements?***
Bank A	Qn 21: No comments Qn 22: a) If existing customer previously did not opt-out from the organization's marketing campaign, can the organization continue to market to such customers after implementation of the new DP regulations?

	b) If we collect new contact information from an existing customer, e.g. mobile phone number, after implementation of new DP regulations, can such channel be considered part of "existing use"? Qn 23: No comments
Bank B	Qn 21: We need to first ascertain the actual impact of this regime before commenting on whether a two years "sunrise" period is appropriate. The enrolment of the banking industry into the proposed DP law can result in potential system developments and process enhancements. Hence, we foresee the "sunrise" period may even be longer than the period of 2 years. Qn 22: No comment. Qn 23: Refer to comments under Qn 1 and 2 above.
Bank C	We support a "sunrise" period of 1-2 years to allow organizations to prepare for compliance with DP law. We also support the proposal that consent is deemed given by the individual for the organization to use and/or process existing personal data for reasonable "existing use". However, it would be helpful to have guidelines on what constitutes "existing use". Would cross selling or referring a customer to other products offered by the same bank constitute "existing use"? In our view, the collection, use and disclosure of personal data for the purposes of providing banking services to our customers should be exempted from the DP law, and if so exempted, they should also be exempted from the transition period.
Bank D	Qn 21: A 2-year sunrise period would be appropriate Qn 22: Existing personal data should be exempted from the DP Act. Qn 23: No comments.
Bank E	Qn 21: To be fair to organizations, big and small alike, the "sunrise" period should only start after the DPC has been set up, significant progress has been made in terms of awareness-building, and best practices/guidelines have been provided. However, a point to note: Although it is deemed that smaller organizations do not have the infrastructure of personal data management processes in place hence requiring a longer "sunrise" period, it is also pertinent to know that larger organizations require more effort in changing processes, system enhancements and aligning all stakeholders involved in the process. Good to adopt a single "sunrise" period, but propose to have a longer one (at least 2 years for full implementation) since there are different requirements for different organizations. Qn 22: For existing personal data to be used for a new or different purpose, it may not be necessary to obtain fresh consent from customers as this may pose as a hassle to them to be contacted for such purposes. Unless the new or different purpose expresses some degree of material detriment to customers, this should not be implemented. Para 4.18 – with reference to "…use the same personal data for direct marketing where it had not done so previously, this would be considered a new use for which consent will need to be obtained." Does the organization need to proof that it has previously used the same information for direct marketing for that particular individual, or it is based on the organizations business activities as a whole?

	For arrangements on providing data to outsourced companies, partners and service providers for specific uses, it may be necessary to implement a longer "sunrise" period. Reasons include establishment of new service-level agreements, arrangement with outsourced companies to ensure compliance, audits/checks on a regular basis.
Bank F	Qn 21 : Response as above in Qn 19. Qn 22 and 23: No comments
Bank G	Q21: We are confident that compliance could be achieved within a one year sunrise period. Q22: No comment. Q23: No comment.
Bank H	Qn 21: One year is enough for everyone to gear up because Singapore bas been talking so much about Information Technology for so long that there is an urgent need to protect consumers' rights. Qn 22: Implementing costs or the headcount required to review whether existing data collection is in line with DP Guidelines or ensuring Consent is obtained for the use of the existing data set will be troublesome and costly at first. Overtime, everything should fall in line once the implementation gets started. Qn 23: It is difficult to ascertain who are going to be affected until the DPC makes known the whole series of Criteria, Guidelines and Rules. Offhand, it looks like telemarketing, credit card companies and property marketing companies or brokers will bear the blunt.
Bank I	Q21: No comments. Q22: No comments. Q23: No comments.
Bank J	We agree with the proposed treatment of existing personal data as outlined in paragraphs 4.15 to 4.19 of the CP.
Bank K	No comments.
	Questions in relation to proposed National Do-Not-Call registry: ***Question 24: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?***
Bank A	Qn 24: a) If an existing customer is listed in the DNC, but has not given instruction to opt-out of the company's marketing of its products, can the organization continue to market their products to such an existing customer? b) If a customer has already registered with DNC, but subsequently through a new customer/product agreement agrees to be contacted by an organization for marketing purposes, will DNC or new agreement take precedence?

	c) Will there be historical snapshots of the DNC available for audit purposes so that organizations can show that they have complied with DP regulations at a particular point in time? d) One suggestion for DNC is to use NRIC as a unique identifier for Singaporeans as phone numbers could be recycled. e) There will be a need to evaluate DNC identifiers for non-Singaporeans and Singapore PRs.
Bank B	Qn 24: While the proposed DP law aimed to protect the interests of consumer/public, online privacy, deliver economic benefits for Singapore and building consumer confidence etc, some of the proposals [such as 'Rules on access to and correction of personal data' (paragraph 3.68), 'National Do-Not-Call' Registry' (paragraph 5.5) etc] may be tedious and costly to manage and enforce. For proposal on the 'National Do-Not-Call Registry', a less prescriptive approach may be better and flexible for an organization to manage instead since they have control over the data. In addition, it may be difficult to operationalise the proposed National Do-Not-Call registry. Customers may have different requests and preferences. Some may request for all calls to be stopped while others may request for certain product information only. Such a 'Do-Not-Call' registry, which the bank already has a similar setup, should be maintained at organizational level instead of nationwide. In addition, the DP law or proposed DP law in jurisdictions such as Hong Kong, United Kingdom and Malaysia does not include the set-up of a National Do-Not-Call Registry. The Privacy Commissioner for Personal Data of Hong Kong has recently proposed to implement a National Do-Not-Call Registry. However, the Hong Kong government has decided not to pursue such a proposal in the review of its DP law. This could also mean that it may be administratively and operationally not feasible to implement such a national registry.
Bank C	If a National DNC Registry is set up in Singapore, we have the following comments: • To achieve operational effectiveness, organizations should have the ability to link and/or map their systems to the National DNC Register in a cost effective manner to ensure DNC records are available to organizations in a timely manner. For example, will the DNC database be sent by batch at request of organizations, or could organizations get a real-time sync to the database? • People often change phone number, and telecom companies recycle phone numbers to new customers. So there is the possibility that an individual will "inherit" a phone number of a previous individual who has registered that phone number with the National DNC Registry. Would DNC registration have a validity period (for example 3 years after registration) after which the DNC registration is cancelled and that individual have to re-register if they want to continue the DNC? • In our view, customers are probably most frustrated by calls for certain type of products e.g. unsecured lending (credit cards/personal loans). As a bank we do offer many other types of products and banking services. Could MICA consider making a distinction between unsecured calls (and other notable types) vs. less controversial calls? • Would the DNC restriction apply only to non-customers of the bank? Or, would the DNC restriction also capture existing customers of the bank (e.g. bank staff engaging our own customers)? If the DNC restriction applies to the bank's existing customers, it should be clarified that service calls (i.e. calls in relation to the provision of banking services) should be excluded from DNC, as contrasted with sales calls. • How will the DNC Registry ensure that the phone number registered by the individual actually belongs to that individual? Worst case: somebody makes a typo in registering his number in the DNC registry, and the bank can no longer call our own customer.
Bank D	(a) We are of the view that in the event a national Do-Not-Call ("DNC") registry is established, the Bank should not be required by law

	to check the registry. The Bank already has internal controls in place to ensure that if a customer requests not to receive marketing materials, the Bank will cease sending such marketing materials to him. (b) In the event a DNC registry is established and the Bank is required by law to comply with the registry, we are of the view that customers should be allowed to define the type of information they would like to receive (i.e. they may not wish to receive information from a beauty salon but may be open to receiving information on promotions offered by banks) and the channels that they wish to receive information through (i.e. they may not wish to receive telemarketing calls but are open to receiving SMS/electronic mail). (c) Paragraph 5.5 states "With a national DNC registry, organisations will be required by law to check the registry and ensure that they do not make telemarketing calls or send SMS/fax messages to the numbers registered, unless the individual had specifically given their consent for the organisation to call/send them telemarketing messages". How often will the Bank be required to check the DNC registry? If a customer chooses to place himself on the DNC registry, how will the Bank be alerted to it? There needs to be a system in place to alert the Banks to the customer's request otherwise it is not practicable for the Bank to check the registry each time we market/promote our products and/or services to the customer. Notwithstanding this provision, there may potentially be issues with individuals who have registered under the DNC registry AND who have also specifically given their consent for an organisation to call/send them telemarketing messages. Does the specific consent given to the organization prevail even if such consent was given prior to the setting up of the DNC, or prior to the individual's registration with the DNC? Would an "opt-out" consent (c.f. paragraph 3.35) constitute "specific consent" in this regard?
Bank E	Qn 24: National Do-Not-Call list might not necessarily benefit customer. Customer might only want to be placed under Do-Not-Call for specific organizations. The DP law should enforce individual organization maintain a Do-Not-Call at organization level so that customer can selectively opt-out. However, if the National Do-Not-Call list is to be implemented, MICA should consider the operational challenges that will be present with the national DNC registry. For example, usually there is a time lag between checking such registry and the actual execution of the call, SMS or fax. Unless there is a universally accessible and very cost effective channel to check against the registry JUST before the actual call, SMS or fax, it won't be able to cater for the situation where an individual happens to register while the contact is being processed. Also individuals might want to register DNC for only certain organizations but not all organizations. The DNC register should be accessible in a real-time callable service to enable seamless checking of customer numbers against the DNC in an automated fashion. Rules will be required to ensure phone numbers are in a standardised easily matchable format. A process needs to be in place to verify that phone number added to the service genuinely want to be added (i.e some form of SMS sent back to verify the request) – this would prevent members of the public simply entering any number onto this list without them owning the number.
Bank F	Qn 24: We would like to highlight some points for consideration when implementing a national DNC: a) Propose that a validity period of maximum of between 1 to 2 years be imposed for consumer's records on the DNC registry. Thereafter, consumers should re-apply to ensure that information is kept updated. b) Consumers should also be informed of a minimum 'grace' period before their applications are accepted and reflected in the

	registry. In addition, the onus should be left to the consumer to inform the national registry if there are changes to their personal data. Unless the consumer notifies the registry promptly, the new data will not be on the registry. For example, if a mobile number registered under DNC was subsequently transferred to a new individual, the customer may still receive telemarketing calls if his new number is not captured under DNC registry. c) For existing customers of organizations (Banks) with opt out capabilities, the consent (implicit or explicit) should over-ride the national DNC list since the organizations will maintain their own database. d) Where organizations engage 3rd Party vendors to perform telemarketing services using the vendors' own leads, the organization will not be in a position to police compliance by the vendor. The onus should be on the vendor to ensure that the data that they are using are not on the DNC registry. And the proposed penalties (if any) for non-compliance should not be enforced on the organizations, but on such vendors.
Bank G	Q24: No comment.
Bank H	Qn 24: It is not economical to set up a registry just to stop Telemarketing companies which provides job for many. Before setting up, why not ascertain from other matured DP regime, the extent of complaints made against telemarketing or others. After all, there are other medias for communications like MMS and emails sent by countless property brokers pushing new property deals unsolicited.
Bank I	Q24: A national Do-Not-call registry should be set up. This is a protection from nuisance calls but even more so, companies should go on the list as this would help against phishing calls.
Bank J	We have no comments.
Bank K	No comments.
	Other Comments
Bank A	No comments.
Bank B	We recognize the need for a general data protection (DP) law in Singapore to foster consumer confidence and regulate certain industry sectors where there are common instances of abuse and consumer complaints. However, the banking industry is already subjected to stringent banking secrecy requirements under the Banking Act which provide sufficient safeguards to protect customers' personal data. Under banking regulations, unless certain strict conditions for disclosure are met (per Banking Act 3rd schedule), customer consent has to be obtained before any customer information can be disclosed to third parties. As a service industry, it is imperative that banks would in the course of daily business dealings, contact customer for account servicing and relationship building purposes e.g. after-sales follow up and appointment fixing. Even for marketing purposes, banks have in place internal unsubscribe system to allow customers to opt-out of calls, sms, emails etc if they are not keen to receive such calls/communications. While some customers may not require updates on information and promotions on financial services and products, other customers may appreciate such information due to cater to their differing needs. For the reasons above, we view that banks should be exempted from the scope of the proposed DP legislation. The inclusion of banks will unnecessarily burden the banks with additional administrative cost and create practical difficulties to harmonise the varying

	expectations under Banking Act and the proposed DP law.
Bank C	No comments.
Bank D	No comments.
Bank E	No comments.
Bank F	No comments.
Bank G	No comments.
Bank H	No comments.
Bank I	From our bank's perspective, we do not have any specific comments on this new law. This is because as a Bank, we have all along had the banking secrecy provisions applicable to us. The banking secrecy regime is of a higher standard and with more severe penalties for breach than the new proposed data protection regime. The impact to us as a bank as I see it is minimal. From the IT point of view, there is no big change for the bank since we already have very strict data protection rules in place.
Bank J	No comments.
Bank K	No comments.