
# RESPONSE TO FEEDBACK ON THE PUBLIC CONSULTATION FOR MANAGING UNSOLICITED COMMERCIAL MESSAGES AND THE PROVISION OF GUIDANCE TO SUPPORT INNOVATION IN THE DIGITAL ECONOMY

**Issued 8 November 2018**

TABLE OF CONTENTS

## PART I: INTRODUCTION AND BACKGROUND

1.1 The Personal Data Protection Commission (the "PDPC") launched a public consultation on 27 April 2018 on Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy.

1.2 In the public consultation, PDPC sought views on the review of the Do Not Call ("DNC") Provisions, set out in Part IX of the Personal Data Protection Act 2012 ("PDPA"), and the Spam Control Act ("SCA"). PDPC also proposed an Enhanced Practical Guidance ("EPG") framework under the PDPA that will allow PDPC to provide guidance with regulatory certainty to organisations. These proposals are part of the PDPC's review of the PDPA.

1.3 In addition, PDPC sought feedback on the exceptions for the collection, use or disclosure of personal data without consent in the Second, Third and Fourth Schedules to the PDPA.

1.4 The consultation closed on 12 June 2018 with 29 responses, mostly from organisations (including business associations) from various sectors. Please refer to the PDPC's website for the full list of respondents and their submissions[1]. The PDPC thanks all respondents for the comments submitted to the public consultation.

1.5 This note summarises the key matters raised by respondents in this public consultation with respect to the review of the DNC Provisions and the SCA, as well as the proposed EPG framework. PDPC's responses and positions on these proposals taking into consideration the comments received are also provided in this note.

[1] Available at https://www.pdpc.gov.sg/legislation-and-guidelines/public-consultations/responses-received-on-12-june-2018.

## PART II: REVIEW OF DNC PROVISIONS AND THE SCA

### 2 Scope and applicability

2.1 In the public consultation, PDPC considered the common aims of the PDPA and SCA to address consumer annoyance and provide consumers with greater control over the number of unsolicited marketing messages received. PDPC consulted on its proposal for the DNC Provisions and the SCA to be merged under a single legislation ("New Act") governing all unsolicited commercial messages.

2.2 Under the proposed New Act, the DNC Provisions would continue to apply to specified voice, text and fax messages sent to Singapore telephone numbers, while the Spam Control Provisions[2] under the New Act would continue to apply to emails that are sent in bulk. The New Act would also remove overlaps and streamline the scope and applicability of the DNC and Spam Control Provisions for the sending of text messages in the following manner:

a) The DNC Provisions under the New Act would apply to unsolicited marketing calls made to Singapore telephone numbers and text messages that are sent to Singapore telephone numbers, regardless of whether they are sent in bulk.

b) The Spam Control Provisions under the New Act would be extended to apply to unsolicited commercial text messages where they are addressed to instant messaging ("IM") identifiers and are sent in bulk.

2.3 For the labelling requirements of commercial text messages sent via IM identifiers in bulk, PDPC had proposed that only the contact information is required (e.g., provide an email address at which the sender can be contacted).

Feedback received

2.4 Majority of respondents supported the proposal to merge the DNC Provisions and the SCA under a single legislation, and to extend the scope of the Spam Control Provisions under the New Act to include commercial text messages sent in bulk using IM identifiers.

2.5 Some respondents also sought clarifications on the proposals. In particular, some respondents requested for clarity on definitions such as 'unsolicited', 'in bulk', 'marketing' and 'commercial'. Clarifications were also sought on the specific IM identifiers or IM platforms that the New Act would apply to, as well as the application of the New Act in situations where users have control over who can send them IM messages (e.g., where users have to first add the sender on the IM platform before

[2] Refer to the requirements for unsolicited commercial electronic messages under Part III of the SCA.

the sender can send them IM messages) and whether it is required to provide an unsubscribe facility in such instances. Some respondents also queried if the New Act would also apply to in-app notifications, mobile push notifications, and pictures/videos which contain commercial messages.

PDPC's response

2.6 PDPC intends to retain the proposed scope and applicability. In consideration of the feedback received, PDPC also provides the following clarifications on the terms and definitions to be used in the New Act:

a) Where a sender has to be added by a user before the sender can send a commercial text message via the user's IM identifier, the message will still be considered an unsolicited commercial text message and the Spam Control Provisions under the New Act will apply if it is sent in bulk. In such cases, senders would need to provide an unsubscribe facility in such messages. This will cater for situations where, for example, the user can continue to follow the sender's social media page but can decide not to receive commercial text messages through the social media platform's IM channel.

b) The New Act will not apply to in-app notifications (e.g. notifications to download the latest version of an app) or a mobile device's notification feature.

c) The DNC and Spam Control Provisions under the New Act will not be limited to unsolicited marketing and commercial messages sent via text, but would also apply to images, videos and audio files that contain commercial messages. For instance, DNC Provisions will apply to messages sent via MMS audio files and Spam Control Provisions will apply to video files sent using IM identifiers.

## 3 Period for effecting withdrawal requests

3.1 Presently, the DNC Provisions and SCA impose different periods for effecting a withdrawal request. Under the DNC Provisions, a person must effect a request for withdrawal of consent for the sending of a specified message to a Singapore telephone number in 30 calendar days. Under the SCA, where a recipient submits an unsubscribe request, no further unsolicited messages shall be sent after the expiration of 10 business days. To minimise confusion and reduce compliance costs by streamlining processes for all unsubscribe and withdrawal of consent requests, PDPC had proposed to reduce the period for organisations to effect a withdrawal of consent to receive marketing messages under the DNC Provisions under the New Act to 10 business days, in line with the period for organisations to effect an unsubscribe request under the SCA.

Feedback received

3.2 The majority of the respondents did not support the proposal, with more than half suggesting to keep to the current 30 calendar days under the DNC Provisions, and/or to align the withdrawal period for the Spam Control Provisions under the New Act to 30 calendar days under the DNC Provisions. Some highlighted that 10 business days was too short particularly where organisations rely on manual processes to effect withdrawal requests, and cited IT constraints and time required to understand how individuals' information is being used within the organisation. Respondents also sought clarification on whether PDPC was proposing for the prescribed duration for checking the DNC Registry ("DNCR") to change from 30 calendar days to 10 business days.

PDPC's response

3.3 In view of the feedback received on the operational constraints to effect withdrawal of consent within 10 business days under the DNC Provisions, PDPC intends to reduce the withdrawal period in two phases. In the first phase, the withdrawal period for the DNC Provisions under the New Act will be reduced to 21 calendar days. The prescribed duration for validity of DNCR checks will correspondingly change to 21 calendar days. PDPC recognises that organisations may have to check the DNCR more frequently and may be concerned about the increase in compliance cost. Hence, PDPC will be reviewing the pricing mechanism for DNCR checks.

3.4 For the avoidance of doubt, the period to effect unsubscribe requests for the Spam Control Provisions under the New Act will remain unchanged at 10 business days.

3.5 In the second phase, PDPC intends to align the withdrawal periods under both the DNC and Spam Control Provisions under the New Act to 10 business days. Organisations are advised to review and implement changes to their IT systems and processes for effecting withdrawal requests, with the view to being able to effect withdrawal requests within 10 business days in the future.

## 4 Dictionary attack and address harvesting software

4.1 In the public consultation, PDPC noted that the use of dictionary attacks[3] and address harvesting software[4] is presently prohibited under the SCA, but is not prohibited under the DNC Provisions. PDPC had proposed to prohibit the sending of commercial messages (including the making of telemarketing calls) to all telephone numbers (not limited to Singapore telephone numbers), IM identifiers and email addresses generated by or obtained through the use of dictionary attacks or address harvesting software by persons in Singapore under the New Act. PDPC had also proposed for these provisions to be enforced under an administrative regime[5] under the New Act. However, repeat or egregious breaches may still be prosecuted as criminal offences.

Feedback received

4.2 Most of the respondents supported the proposal to prohibit the use of dictionary attack and address harvesting software for sending commercial messages. Several respondents sought clarification on the applicability of the prohibition in instances where mailing lists were obtained from third parties, where these actions were taken by machines/artificial intelligence and not by persons, and where organisations used address harvesting software on their own database.

PDPC's response

4.3 PDPC will retain the proposal to prohibit the use of dictionary attack and address harvesting software for sending commercial messages. PDPC also provides the following clarifications:

a) Senders will be liable when they use mailing lists generated through the use of dictionary attack or address harvesting software from third parties, to send unsolicited commercial messages (including the making of telemarketing calls). Third parties that generate and provide the lists, but do not use the lists to send unsolicited commercial messages, will not be liable.

b) The prohibition is intended to be technology neutral, and will apply regardless of whether the use of dictionary attack or address harvesting software was carried out by a human or through automated means.

[3] Under the SCA, dictionary attack means the method by which the electronic address of a recipient is obtained using an automated means that generates possible electronic addresses by combining names, letters, numbers, punctuation marks or symbols into numerous permutations.
[4] Under the SCA, address harvesting software means software that is specifically designed or marketed for use for (i) searching the Internet for electronic addresses; and (ii) collecting, compiling, capturing or otherwise harvesting those electronic addresses.
[5] Similar to the proposed enforcement approach for DNC Provisions under the New Act. See Chapter 6 of this document.

c) The prohibition does not apply when organisations use address harvesting software on their own database.

## 5 Business-to-business ("B2B") marketing messages

5.1 B2B messages are currently covered under the SCA. In the public consultation, PDPC sought comments on whether the DNC Provisions under the New Act should be extended to cover B2B marketing messages (i.e., marketing messages that are sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation[6]).

Feedback received

5.2 Most respondents commented that the DNC Provisions under the New Act should not cover B2B marketing messages, as doing so would hinder business contacts and networking. Some respondents raised concerns that if employees were allowed to place their business numbers on the DNCR to prevent the receipt of B2B messages, business contact persons cannot be reached for business purposes.

PDPC's response

5.3 In view of the feedback from organisations, PDPC intends to retain the current exclusion of B2B marketing messages from the DNC Provisions in the New Act.

## 6 Enforcing DNC breaches under an administrative regime

6.1 In the public consultation, PDPC proposed that the duty to check the DNCR, provide contact information and not conceal calling line identity ("CLI") be enforced under an administrative regime in the New Act. This would allow PDPC to resolve DNC complaints faster and empower it to issue directions (including financial penalties) for infringements of the DNC Provisions under the New Act. PDPC also proposed that a private right of action for infringements of the DNC Provisions should be provided under the New Act.

Feedback received

6.2 Majority of respondents supported the proposal to enforce the DNC Provisions under an administrative regime in the New Act.

6.3 Nonetheless, a few respondents suggested that defendants should continue to have the same set of rights as the current criminal DNC regime.

[6] Refer to paragraph 1(g) of the Eighth Schedule to the PDPA.

PDPC's response

6.4 PDPC intends to enforce the DNC Provisions under an administrative regime. However, PDPC intends to provide that repeat or egregious breaches of the DNC Provisions may still be prosecuted as criminal offences. Under the New Act, defendants will continue to have defences similar to the current regime. The DNC Provisions under the New Act will continue to be enforced by PDPC, and affected individuals and organisations will continue to have the statutory right to take private action. The Spam Control Provisions under the New Act will continue to provide for private right of action for affected individuals and organisations.

## 7 Liability of third-party DNC checkers and resale of DNCR lists

7.1 In the public consultation, PDPC proposed to impose an obligation on third-party checkers to communicate accurate information regarding DNCR results. Under the New Act, it was proposed that a third-party checker can be held liable for infringements of the DNC Provisions if these were due to inaccurate information that were provided to the sender. As the reselling of DNCR lists by third-party checkers increases the risk of potential DNC infringements, it was also proposed that the resale of any results of telephone numbers screened through the DNCR be prohibited.

Feedback received

7.2 Majority of respondents supported the proposal to impose an accuracy obligation and liability on third-party checkers.

7.3 Some respondents sought clarity on whether senders would still be liable for inaccuracies on the part of third-party checkers and whether they could be absolved if they had conducted due diligence. The main objection was that this would largely be a contractual matter between the sender and the third-party checker, and the sender could seek indemnity from the third-party checker for any penalties suffered.

7.4 Respondents had mixed views on the proposal to prohibit the resale of results of telephone numbers checked against the DNCR. Almost half of the respondents were of the view that the proposal to impose liability on third-party checkers would suffice to address the concerns relating to the irresponsible reselling of DNCR lists.

PDPC's response

7.5 PDPC intends to retain the proposal to impose an accuracy obligation and liability on third-party checkers under the New Act. However, PDPC clarifies that, whether or not the sender engages a third-party checker, it remains the sender's duty to ensure that Singapore telephone numbers are duly checked with the DNCR and specified messages are not sent to individuals who are registered with the DNCR, unless the

individuals had given clear and unambiguous consent to receive such messages. Hence, when specified messages are sent to Singapore telephone numbers registered with the DNCR, the sender may still be liable if the sender is unable to demonstrate that due diligence had been taken to ensure that the third-party checker had performed the necessary DNCR checks[7].

7.6 Taking into consideration the feedback received, PDPC will not proceed with the proposal to prohibit the resale of results of telephone numbers checked against the DNCR. On reviewing the merits of the proposal and respondents' counter-arguments, PDPC is persuaded that the prohibition may not be necessary if third-party checkers are already legally obliged to provide accurate DNCR results to senders who engage their DNC checking services, and where senders remain liable as mentioned in the above paragraph 7.5. Moreover, the resale of telephone numbers would also be subject to the consent and notification obligations under the PDPA.

## 8 Presumption of sending

8.1 In the public consultation, PDPC proposed to introduce a deeming provision under the DNC Provisions in the New Act such that the subscriber of the Singapore telephone number is presumed to have sent the specified message unless he or she proves otherwise. This was to improve enforcement efficiency and encourage subscribers to take active steps to prevent misuse of their telephone subscription service.

Feedback received

8.2 Respondents were divided on this proposal. Those who disagreed felt that such a presumption would shift the burden of proof unfairly to the subscriber who may lack the means to prove otherwise.

PDPC's response

8.3 PDPC has carefully considered the merits of the arguments against the proposal vis-à-vis the practical considerations faced in enforcing the DNC Provisions on the ground. On balance, PDPC intends to proceed with the deeming provision proposal, based on the reasons set out below.

8.4 Mobile subscribers have control over their own subscriptions and devices and are in the best position to safeguard their subscriptions and devices from illicit use. PDPC envisions that the deeming provision would encourage the right discipline in

[7] For example, seeking an undertaking from the third-party checker through appropriate terms and conditions of the contract, or obtaining a copy of the summary log of DNCR checks conducted by the third-party checkers, and confirm in writing or documented in an appropriate form, that the third-party checker has conducted the necessary DNCR checks.

subscribers to ensure the proper custody and use of their subscriptions and devices. Subscribers are also in the best position to detect misuse of their subscriptions and devices (for example, through the large bills incurred from the mass sending of specified messages by an unauthorised party). In the event that the subscriber's telephone number had been spoofed or device hacked, he or she should be in a position to produce records or evidence that he or she had not sent the message or call from the device. Furthermore, a deeming provision would substantially improve PDPC's enforcement efficiency, strengthening deterrence and overall compliance with the DNC regime.

8.5 Nevertheless, PDPC will take into consideration the facts of each case in its investigations. In exercising the deeming provision in its enforcement work, PDPC would be mindful of the particular circumstances of the alleged DNC infringement and give due regard to the subscriber's position.

## PART III: ENHANCED PRACTICAL GUIDANCE

### 9 Criteria and scope of Enhanced Practical Guidance Framework

9.1 The public consultation highlighted the objectives of the proposed Enhanced Practical Guidance ("EPG") framework. Under the proposed EPG framework, PDPC will be able to provide **guidance on complex compliance queries with regulatory certainty** ("determinations"). These determinations will provide confirmation as to whether a particular business activity complies with the Data Protection Provisions under the PDPA. This will provide organisations with the necessary assurance of compliance with the PDPA, especially when they embark on new and innovative data services.

9.2 On the queries that will be considered under the proposed EPG framework, PDPC had proposed to exclude queries relating to hypothetical situations, or queries that entail a review of the organisation's entire business model, processes or policies. In addition, PDPC had indicated that the request for PDPC's determination must be from the organisation performing the business activity in question.

9.3 PDPC had proposed to assess requests for PDPC's determinations under the proposed EPG framework based on the following criteria:

a) The query relates to a **complex or novel compliance issue** for which there is currently no clear position for its treatment under the PDPA;

b) The query **cannot be addressed by PDPC's general guidance and existing published resources**; and

c) The query **does not amount to a request for legal advice**[8].

Feedback received

9.4 Majority of responses were supportive of the proposed EPG framework, and were of the view that the guidance with regulatory certainty would be useful for addressing organisations' complex or novel compliance issues with respect to the PDPA.

9.5 On the type of queries that would fall within the proposed EPG framework, there were suggestions for PDPC to provide determinations for queries relating to proposed business activities or queries that are sufficiently conceptualised. This would allow organisations to seek determinations before investing substantial

[8] For example, PDPC will not accept EPG applications relating to compliance with the Protection Obligation under the PDPA, since assessment and implementation of security arrangements can be provided by professional DP and IT security services.

resources to develop new products and services.

9.6 Several respondents sought clarification as to whether determinations can be sought by professional advisors (e.g., lawyers) or industry bodies on behalf of organisations and members.

9.7 A few respondents also sought clarification on the criteria for which requests for determinations will be assessed. There were also calls for PDPC to provide examples on what would constitute "queries relating to complex or novel compliance issues" and "queries that would amount to request for legal advice".

PDPC's response

9.8 PDPC has taken into consideration the feedback received and provides the following clarifications on the scope and applicability of the EPG framework.

9.9 PDPC intends to provide determinations under the EPG framework for queries relating to proposed business activities that are more than just exploratory i.e., the proposal contains sufficiently detailed plans. PDPC also clarifies that determinations may be sought by professional advisors (e.g., lawyers) on behalf of organisations, or by industry bodies, on behalf of their members.

9.10 In terms of the criteria for which applications for determinations will be assessed, PDPC intends to retain its proposal. Examples of queries that would amount to request for legal advice include those that can typically be provided by lawyers or consultants (e.g., IT security arrangements to comply with the Protection Obligation under the PDPA). Assessment of whether the criteria have been met will be conducted by PDPC on a case-by-case basis (e.g., whether a compliance issue is complex or novel). Organisations should also apply for EPG in good faith (e.g., not to evade compliance with the Data Protection Provisions under the PDPA). PDPC further intends to issue a guide to provide clarity on the types of queries that may or may not satisfy the criteria for PDPC's determinations under the EPG framework.

## 10 Validity and effect of EPG determinations

10.1 In the public consultation, PDPC proposed for the determinations issued to an organisation to generally remain valid, including when the organisation is subsequently being investigated for a matter related to the subject of an EPG determination, unless:

a) There have been changes made to an aspect of the PDPA that are relevant to the determination; or

b) The information provided by the organisation with which PDPC's determination was made was false, misleading or no longer accurate.

10.2 In addition, PDPC will not initiate an investigation in the event PDPC finds any non-compliance with the PDPA solely based on the information submitted by the organisation during the EPG determination process. In such circumstances, PDPC may suspend the assessment and provide the organisation a reasonable period of time to rectify the non-compliance before resuming the assessment. However, in the event that a complaint is received during the course of assessment, PDPC reserves the right to terminate the assessment and commence investigations.

Feedback received

10.3 Clarifications were sought on the legal effect of EPG determinations, in particular, whether EPG determinations are sufficient to exempt organisations from liability in relation to subject matter for which the EPG determination had been sought. A few respondents asked whether the determination may be relied on by other organisations in similar situations.

10.4 A few respondents sought clarification on what PDPC considers to be "no longer accurate", and whether changes to business situations would render EPG determinations invalid. There were suggestions for PDPC to provide an avenue for organisations to re-seek confirmation of compliance with the PDPA where there are material changes after PDPC's determination had been sought.

PDPC's response

10.5 Taking into consideration the feedback received, PDPC intends to retain its proposal that it will not find the organisation in breach of the PDPA in relation to the subject matter for which it has issued a determination confirming that the matter is in compliance with the PDPA. This is save for certain prescribed circumstances, in particular, where there have been changes made to an aspect of the PDPA that is relevant to the determination, or the information provided by the organisation with which the PDPC's determination was made was false, misleading or no longer accurate – which would render the determination invalid. PDPC additionally clarifies that determinations may only be relied on by the requesting organisation. Where an application is submitted by multiple organisations, PDPC may issue the determination to all organisations making the application.

10.6 In relation to queries on what PDPC considers to be "no longer accurate", PDPC intends to assess the material inaccuracy of the information provided by the organisation that would have affected the EPG issued. Organisations may seek supplemental EPG if there are any material changes (e.g., changes to business

situations, products or services) to the proposal in its original application.

10.7 In addition, PDPC intends to impose a validity period for all determinations. The validity period will be decided on a case-by-case basis. Where exemptions from specific PDPA provision(s) are provided for as part of a determination, the validity period for the determination and exemption will be the same.

10.8 PDPC also intends to retain its proposal not to initiate investigations in the event it finds any non-compliance with the PDPA based on the information submitted by the organisation during the EPG determination process, regardless of whether the non-compliance is related to the scope of the EPG. Where there is an ongoing investigation into the organisation, EPG applications made to PDPC on the same subject matter will not be accepted.

## 11 Publication of EPG, Fees and Timeframe

11.1 PDPC had proposed that a redacted version of PDPC's determination to be published on a case-by-case basis without disclosing any confidential or commercially sensitive information. This is similar to the approach PDPC has taken for the current Practical Guidance, and doing so would help to raise awareness on matters which the determination had been provided.

11.2 PDPC had also proposed to charge organisations seeking determinations under the proposed EPG framework according to the type and size of the organisation. This is to ensure that EPG costs are not prohibitive for SMEs and start-ups.

Feedback received

11.3 Majority of the respondents were supportive of PDPC's proposal to publish the redacted version of EPG on a case-by-case basis, so as to allow other organisations facing similar situations to also benefit from the guidance. There was also a suggestion to allow organisations to make representations where their interests are affected by EPG determinations.

11.4 Several respondents sought clarification on the EPG fee structure and in particular, whether factors such as complexity of query and type of organisations would be taken into consideration.

PDPC's response

11.5 In view of the feedback, PDPC intends to retain its proposal to publish redacted versions of EPGs on a case-by-case basis, and would clarify that the organisation seeking the EPG will be given an opportunity to review the factual sections of the redacted EPG before publication. Selected determinations may further be converted

into FAQs or issued as advisory guidelines for educational purposes where appropriate.

11.6 PDPC also intends for the determination to take effect once issued to the applicant(s). Notwithstanding this, PDPC intends to have the discretion to review determinations should it receive any representations of adverse impact to consumer or public interests.

11.7 In relation to the EPG fee structure, PDPC will take into account factors such as the size and number of organisations involved in the EPG application, and the complexity of the query.

11.8 PDPC intends to provide more details and guidance on administration and procedural issues relating to the EPG application and assessment process, including the fee structure, in the guide on the EPG framework.

## PART IV: SECOND, THIRD AND FOURTH SCHEDULES TO THE PDPA

### 12 Exceptions to consent

12.1 The Second, Third and Fourth Schedules to the PDPA enumerate exceptions to the obligation to obtain consent for the collection, use and disclosure of personal data respectively. In order to ensure that extant exceptions remain relevant in the face of technological developments and changes in business practices, PDPC sought feedback from organisations on the practicality of relying on these exceptions in the public consultation. In particular, PDPC sought feedback for the following:

a) Whether the scope or conditions of any exception should be adjusted or clarified; and

b) Whether any exception is no longer necessary or relevant.

Feedback received

12.2 Respondents provided feedback mainly on the exceptions on (i) research purpose[9], (ii) business asset transaction[10], and (iii) provision of service for personal and domestic purposes[11].

12.3 On the research exception, respondents requested for clarity on the scope of research purpose, and clarity on the conditions to rely on the research exception (e.g., what was meant by 'impracticable' and how to determine whether 'linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest'). There were also suggestions to amend the exception to allow the use and disclosure of personal data for bona fide academic purposes (e.g., where research studies are approved by Institutional Review Boards ("IRBs")).

12.4 A respondent commented that the exception for business asset transactions appeared to only work for business asset transactions where the target company is a party to the transaction. Another respondent suggested that this exception be amended to improve its workability in the context of sale of shares transactions, and to include initial public offerings ("IPOs") and the sale of digital subscription businesses.

12.5 On the exception for where the personal data was provided to the organisation by

[9] Refer to paragraphs 1(i) and 2 of the Third Schedule to the PDPA, and paragraphs 1(q) and 4 of the Fourth Schedule to the PDPA.
[10] Refer to paragraphs 1(p) and 3 of the Second Schedule to the PDPA, and paragraphs 1(p) and 3 of the Fourth Schedule to the PDPA.
[11] Refer to paragraph 1(m) of the Second Schedule to the PDPA.

another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual, a respondent commented that the exception seemed to apply only to situations where the service is provided to 'that other individual', and suggested amendments to clarify its applicability to other individuals involved apart from 'that other individual'.

12.6 One respondent suggested an additional exception for the performance of contractual obligations, to allow an organisation to collect, use, and disclose personal data without consent to perform its obligations under a contract with the relevant individual or with a third party at the individual's request.

PDPC's response

12.7 PDPC will take the feedback into consideration as part of its review of the exceptions in the PDPA.

## PART V: CONCLUSION

13.1 This is the second public consultation that PDPC has conducted for the review of the PDPA. The PDPC will continue to solicit feedback and views on other key areas of review where needed.

13.2 Advisory guidelines and other resources will be provided to assist organisations in complying with the new requirements when they are introduced.

13.3 Once again, PDPC thanks all respondents for their comments and submissions to this public consultation.

END OF DOCUMENT