PERSONAL DATA PROTECTION COMMISSION
SINGAPORE

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

Issued 27 April 2018

TABLE OF CONTENTS

PART I: INTRODUCTION 3

PART II: REVIEW OF DNC PROVISIONS AND THE SCA 4

2 Background on current regime – DNC Provisions and the SCA 4

3 Proposed streamlining of requirements under DNC Provisions and the SCA 4

4 Proposed enforcement approach for DNC Provisions under the New Act 11

PART III: ENHANCED PRACTICAL GUIDANCE 13

5 Need for Enhanced Practical Guidance 13

6 Proposed criteria and scope 14

7 Proposed validity and effect of determinations 15

8 Proposed exemption under EPG framework 16

PART IV: SECOND, THIRD AND FOURTH SCHEDULES TO THE PDPA 17

9 Solicitation of feedback on exceptions to consent 17

PART V: SUBMISSION OF COMMENTS 18

PART I: INTRODUCTION

1.1 The Personal Data Protection Act 2012 (the "PDPA") governs the collection, use and disclosure of individuals' personal data by organisations. The PDPA's data protection obligations are set out in Parts III to VI of the PDPA (the "Data Protection Provisions").

1.2 On the other hand, the Do Not Call ("DNC") Provisions, set out in Part IX of the PDPA, provide a simple and effective way for individuals to opt-out of all marketing messages addressed to their telephone numbers. The Personal Data Protection Commission ("PDPC") oversees the development and operation of the DNC Registry ("DNCR") for individuals to register their Singapore telephone numbers and organisations to check and ensure they do not send marketing messages to telephone numbers registered in the DNCR.

1.3 Technological advancements have fuelled increasing adoption of marketing tools such as social media and instant messaging platforms. PDPC is reviewing the DNC Provisions to ensure they remain relevant today. The review also considers the Spam Control Act ("SCA"), which is a light touch legislation enacted in 2007 to combat spam, with the view to ensuring a technology neutral approach towards regulating unsolicited commercial messages.

1.4 The functions of the PDPC include, amongst others, promoting awareness of data protection in Singapore and administering and enforcing the PDPA. As part of facilitating organisations' compliance with the PDPA, PDPC currently provides guidance ("Practical Guidance") to address organisations' queries in relation to how the PDPA provisions would apply to a specific business activity. PDPC is considering introducing an Enhanced Practical Guidance ("EPG") framework under the PDPA that will allow PDPC to provide guidance with regulatory certainty to organisations, to support and facilitate the growth of innovative services and products involving the use of personal data.

1.5 In PDPC's earlier Public Consultation for Approaches to Managing Personal Data in the Digital Economy[1], PDPC had proposed an enhanced framework for the collection, use and disclosure of personal data. As a follow up, PDPC is also reviewing exceptions for the collection, use and disclosure of personal data without consent in the Second, Third and Fourth Schedules to the PDPA.

[1] The public consultation paper, responses received and PDPC's response to the feedback received are available at www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations.

PART II: REVIEW OF DNC PROVISIONS AND THE SCA

2 Background on current regime – DNC Provisions and the SCA

2.1 The DNC Provisions under the PDPA came into effect in 2014. The DNCR was established to provide individuals with a simple and effective way to opt-out of all specified messages[2] (also referred to as marketing messages in this document) in the form of text messages, fax messages or voice calls, sent to Singapore telephone numbers. The DNC Provisions require persons[3] to check the relevant DNCR before sending a specified message to a Singapore telephone number, unless the person has obtained clear and unambiguous consent from the individual or has an ongoing relationship[4] with the individual. Breaches of certain DNC Provisions are enforced as criminal offences.

2.2 The SCA, which applies to electronic messages (i.e., email and text messages) when sent in bulk[5], is a light touch legislation that was enacted in 2007. It is intended to fill the lacuna in tackling the less serious forms of spamming activities that were not within the purview of other laws (e.g., the then Computer Misuse Act). Amongst others, the SCA requires that an unsubscribe facility be provided in every unsolicited commercial electronic message[6] that is sent in bulk. Commercial messages include marketing messages and messages relating to dishonest gains or deception. The SCA allows for private right of action relating to the sending of unsolicited commercial electronic messages in bulk.

3 Proposed streamlining of requirements under DNC Provisions and the SCA

3.1 While the PDPA and the SCA were enacted as separate legislation with different enforcement regimes, both aim to address consumer annoyance and provide consumers greater control over the number of unsolicited marketing messages received. At the same time, the PDPA and SCA aim to balance both consumers' and organisations' interests by ensuring that the requirements for sending such messages are not overly onerous for organisations. This also enables organisations to market and communicate more effectively with consumers who are interested in receiving information on their offers, products and services.

3.2 With technological developments leading to increasing use of new marketing tools and instant messaging platforms for sending marketing messages, it is necessary to review the DNC Provisions and the SCA to ensure they remain relevant and effective in today's

[2] "Specified message" is defined in section 37 of the PDPA. Exclusions from the definition of specified messages are listed in the Eighth Schedule to the PDPA.

[3] The DNC Provisions apply to persons including individuals as well as companies, associations and other bodies of persons, corporate or unincorporated.

[4] Refer to the Personal Data Protection (Exemption from Section 43) Order 2013.

[5] Refer to section 6 of the SCA for the meaning of "sending in bulk".

[6] "Commercial electronic message" is defined in section 3 of the SCA.

landscape. Specifically, given that both the DNC Provisions and the SCA impose overlapping requirements on unsolicited marketing text messages, it is useful to consider how the requirements can be streamlined.

3.3 PDPC proposes for the DNC Provisions and the SCA to be merged into a **single legislation ("New Act") governing all unsolicited commercial messages**, following similar approaches in other jurisdictions, such as Hong Kong and United Kingdom[7]. The PDPA will continue to be the baseline legislation for personal data protection. Details on the scope of the proposed New Act are elaborated below.

Scope and applicability

3.4 Currently, both the DNC Provisions and the SCA apply to text messages that are sent to Singapore telephone numbers, but they do not cover text messages that are sent via instant messaging ("IM") identifiers (see paragraphs 3.7 to 3.15). In addition, the requirements for unsolicited commercial electronic messages under Part III of the SCA ("Spam Control Provisions") only apply to text messages that are sent in bulk, whereas the DNC Provisions apply to specified messages sent to Singapore telephone numbers regardless of whether they are sent in bulk.

3.5 For regulatory clarity, PDPC proposes to remove the overlap and streamline the scope and applicability of the DNC and Spam Control Provisions for the sending of text messages under the New Act in the following manner:

a) The DNC Provisions under the New Act will apply to unsolicited marketing 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 will be extended to apply to unsolicited commercial text messages where they are **addressed to IM identifiers and are sent in bulk**.

3.6 The DNC Provisions under the New Act will continue to apply to specified voice, text and fax messages sent to Singapore telephone numbers, while the Spam Control Provisions under the New Act will continue to apply to emails that are sent in bulk. The proposed changes will provide greater protection to individuals from unsolicited commercial messages and reduce ambiguity for organisations in complying with differing requirements when sending commercial messages.

[7] Refer to Hong Kong's Unsolicited Electronic Messages Ordinance and United Kingdom's Privacy and Electronic Communications (EC Directive) Regulations 2003.

Messages sent using IM identifiers

3.7 The present DNC Provisions were developed at the time when social media and IM platforms were not commonly used to send commercial messages, and the consumer impact of messages sent via such platforms was not significant then. However, the technology and commercial landscape today is different, and marketing practices have evolved. Organisations are increasingly relying on social media and IM platforms (e.g., through Facebook and WeChat) as marketing channels and alternatives to traditional SMS text messaging.

3.8 IM platforms generally use the users' email address, mobile number or IM identifier (i.e., account ID or login ID created by the user) for the sending of messages. Even though users are required to provide their contact details (e.g., email address or mobile telephone number) at the point of registration for verification purposes, messages may be sent via such platforms using IM identifiers instead of their email addresses or mobile telephone numbers.

3.9 As commercial messages sent via IM identifiers are not covered under the DNC Provisions or the SCA today, individuals who register their mobile numbers with the DNCR may continue to receive marketing text messages which are sent using their IM identifiers. Consumers would not be able to distinguish whether the marketing text messages have been sent to their mobile telephone numbers or sent using their IM identifiers.

3.10 To ensure the New Act remains attuned to industry practices and new technologies, and provide better protection for consumers from unsolicited commercial messages sent using their IM identifiers, PDPC proposes for **commercial text messages sent via IM identifiers in bulk to be included in the scope of the Spam Control Provisions under the New Act**. This means that individuals will be able to better manage such messages as organisations will need to comply with the Spam Control requirements such as providing an unsubscribe facility and their contact information, when sending commercial text messages using IM identifiers in bulk. If there is a contravention of the Spam Control Provisions under the New Act, civil action may be taken by affected individuals or organisations.

3.11 The proposed approach is aligned with approaches taken in other jurisdictions, where text messages sent using IM identifiers are addressed under their spam legislation[8]. It also takes into account the fundamental difference between mobile telephone numbers and IM identifiers.

[8] For example, Australia's Spam Act 2003, Canada's Anti-Spam Legislation and Hong Kong's Unsolicited Electronic Messages Ordinance.

3.12 Telephone numbers are a limited resource that is centrally assigned and issued by telecommunication operators. Telephone numbers that were previously assigned and issued but no longer in use can be re-assigned and re-issued to new subscribers. This feature makes a centrally administered DNCR for telephone numbers feasible.

3.13 There are a number of practical difficulties of implementing a national Register for IM identifiers. First, IM identifiers are assigned by the providers of the IM platform and they vary across platforms. As IM identifiers tend to be platform specific, registers for IM identifiers would need to record the associated IM platform. Second, it would be difficult to verify if an IM identifier is held by an individual in Singapore, and to track whether an IM identifier is still in use or has been terminated. Furthermore, new IM platforms are constantly being created while the popularity of existing ones may wax or wane. The list of registered IM identifiers is also likely to grow as users are unlikely to actively de-register IM identifiers that are no longer in use. These make the maintenance of a national Register for IM identifiers highly impracticable and costly.

3.14 Additionally, PDPC is mindful of the compliance costs for businesses should they be required to (i) check multiple Registers for different types of IM identifiers that they intend to send commercial messages to; and (ii) check for all IM identifiers, even though they may not belong to individuals in Singapore or may no longer be in use, before sending any commercial text messages.

3.15 For these reasons, the intention is to treat IM identifiers similarly to email addresses under the Spam Control Provisions under the New Act, which would be maintained as unsubscribe lists by organisations that intend to send unsolicited commercial text messages via IM identifiers in bulk.

Question 1: What are your views on the proposed scope and applicability of the DNC Provisions and the Spam Control Provisions?

Question 2: What are your views on including commercial text messages sent using IM identifiers under the Spam Control Provisions?

Labelling requirements

3.16 PDPC proposes to retain the current labelling requirements for specified voice, text and fax messages under the DNC Provisions (i.e., provision of contact information[9], and calling line identity ("CLI") not to be concealed[10]). PDPC also intends to retain the current labelling requirements for emails under the Spam Control Provisions (i.e., no false or

[9] Refer to section 44 of the PDPA.

[10] Refer to section 45 of the PDPA.

misleading titles and header information, provision of sender's contact and <ADV> label[11]).

3.17 For the labelling requirements of text messages sent via IM identifiers under the Spam Control Provisions under the New Act, it is proposed that **only the contact information is required** (e.g., provide an email address at which the sender can be contacted). The requirement for CLI not to be concealed under the DNC Provisions, is intended to ensure senders do not use a blocked, unlisted or spoofed number, in order to facilitate identification of the sender. This requirement would not be relevant for text messages sent via IM identifiers for a couple of reasons. First, the display name or ID will typically be shown (e.g., WeChat ID cannot be hidden) for text messages sent through IM identifiers. Second, the decentralised mode of creating and assigning display names or IDs for IM platforms makes this means of identifying the sender less relevant.

3.18 The requirements for <ADV> label and no false/misleading titles are also not applicable for messages sent via IM identifiers as the <ADV> label is meant to enable filtering of emails by spam filters, and text messages typically do not have subject titles.

Withdrawal period for specified voice, text and fax messages

3.19 Under the DNC Provisions today, a person must effect the request for withdrawal of consent for the sending of a specified message to a Singapore telephone number in 30 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.

3.20 PDPC proposes to **reduce the period for organisations to effect a withdrawal of consent to receive marketing messages under the DNC Provisions to 10 business days**, in line with the period for organisations to effect an unsubscribe request under the Spam Control Provisions. This will minimise potential confusion and compliance costs as organisations streamline processes for all unsubscribe and withdrawal of consent requests. This also strengthens the protection for consumers who will have their withdrawal requests to stop receiving marketing voice, text and fax messages effected more quickly.

Question 3: What are your views on the proposed reduction of the period for effecting withdrawal of consent to 10 business days, in line with the period to effect an unsubscribe request under the Spam Control Provisions?

[11] Refer to paragraph 3 of the Second Schedule of the SCA.

Dictionary attack and address harvesting software

3.21 The use of dictionary attacks[12] and address harvesting software[13] is presently prohibited under the SCA[14], but it is not prohibited under the DNC Provisions.

3.22 As part of the streamlining of requirements under the New Act, PDPC proposes to **prohibit the sending of commercial messages 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.** These provisions will be enforced under an administrative regime[15] under the New Act.

3.23 With these provisions, a sender will not be able to randomly generate Singapore telephone numbers and send marketing messages to those numbers, even if the person had checked the DNCR. This is to deter spammers who use technologies that make it easier to indiscriminately send unsolicited commercial messages (including robocalls[16]) to a large number of recipients, and will help ensure Singapore does not become a haven for such spammers.

Question 4: What are your views on prohibiting the use of dictionary attack and address harvesting software for sending of commercial messages to all telephone numbers, IM identifiers and email addresses?

Dishonest gains or deception

3.24 While messages relating to dishonest gains or deception are covered under the SCA, they are presently not expressly stated under the DNC Provisions[17]. PDPC is not proposing any change to the aforesaid coverage of messages relating to dishonest gains

[12] 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.

[13] 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.

[14] Refer to section 9 of the SCA.

[15] Similar to the proposed enforcement approach for DNC Provisions under the New Act. See paragraph 4.1.

[16] Robocalls refer to phone calls that use a computerised auto-dialler to deliver pre-recorded messages. Refer also to section 36 of the PDPA for definition of "voice call".

[17] Both the SCA and DNC Provisions cover messages advertising goods, services, land, interest or opportunity regardless whether these exist. However, the SCA goes beyond the coverage of the DNC Provisions in that it covers messages that assist or enable a person: (a) by deception, to dishonestly obtain property belonging to another person; (b) by deception, to dishonestly obtain a financial advantage from another person; or (c) to dishonestly obtain a gain from another person.

or deception under the DNC Provisions and the Spam Control Provisions under the New Act.

3.25 With the proposed streamlining for unsolicited marketing text messages to be covered by the DNC Provisions under the New Act (see paragraphs 3.4 to 3.6), unsolicited commercial electronic text messages relating to dishonest gains or deception which do not involve an offer of a good or service (e.g., kidnapping or fund raising scams), sent in bulk to Singapore telephone numbers would not be covered by the Spam Control nor the DNC Provisions under the New Act. The removal of the avenue for civil remedy under the Spam Control Provisions for such text messages is not expected to have a major impact as they will usually be the subject of criminal investigations.

Business-to-business (“B2B”) marketing messages

3.26 Currently, DNC Provisions do not apply to 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[18]) in order not to unduly hinder legitimate B2B marketing[19]. Past practices of maintaining separate telephone numbers for business and personal uses have given way to the increasingly pervasive use of mobile telephone numbers for both business and personal purposes. This has created uncertainty for organisations in complying with the DNC Provisions when sending marketing messages to such telephone numbers. On the other hand, B2B messages are currently covered under the SCA[20].

3.27 PDPC seeks comments on whether the DNC Provisions under the New Act should be extended to cover B2B marketing messages, to align the coverage of the DNC Provisions with the Spam Control Provisions. While expanding the scope of DNC Provisions under the new Act to cover B2B marketing messages may increase business costs for certain persons as they would now have to check the DNCR before sending B2B messages, it eliminates uncertainty and risks for persons sending marketing messages to a DNC-registered Singapore telephone number that may be an individual’s personal mobile number (not used for business purposes). This will also enable organisations to streamline their processes for sending marketing messages to both businesses and individuals (i.e., to check the DNCR before sending marketing messages to both businesses and individuals, unless they have obtained clear and unambiguous consent from the business or individual, or where they have an ongoing relationship with the business or individual[21]). Covering B2B marketing messages also provides more options for individuals using their telephone numbers for both work and personal purposes, as

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

[19] While DNC Provisions do not apply to B2B marketing messages, businesses may register their business numbers with the DNCR if they wish to minimise the number of business-to-consumers (“B2C”) marketing messages received.

[20] Refer to section 7(d)(ii) of the SCA.

[21] Refer to the Personal Data Protection (Exemption from Section 43) Order 2013.

they can choose not to receive B2B marketing messages by registering their numbers on the DNCR.

Question 5: Should B2B marketing messages be subject to the requirements under the DNC Provisions, in alignment with the coverage under the Spam Control Provisions?

4 Proposed enforcement approach for DNC Provisions under the New Act

Enforcing DNC breaches under an administrative regime

4.1 Currently, breaches of certain DNC Provisions (e.g., duty to check DNCR, provision of contact information and not to conceal CLI) are enforced as criminal offences under the PDPA. Taking into consideration the nature of the infringements vis-à-vis the harm caused, which are mainly annoyance and nuisance to recipients, PDPC proposes for **infringements relating to the duties to check the DNCR**[22]**, to provide contact information**[23] **and not to conceal CLI**[24] under the New Act to be enforced under an administrative regime. This allows PDPC to better allocate resources for faster resolution of cases investigated, and PDPC will be empowered to issue directions (including financial penalties) for infringements of the DNC Provisions under the New Act. A private right of action in respect of the DNC Provisions will also be provided under the New Act.

Question 6: What are your views on the proposal for the DNC Provisions to be enforced under an administrative regime?

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

4.2 Currently, organisations may rely on third-party checkers to check the DNCR on their behalf. However, these third-party checkers are not liable under the PDPA for DNC infringements resulting from the inaccurate DNCR results provided by them.

4.3 PDPC will continue to allow third-party checkers to check DNCR on behalf of organisations. However, PDPC proposes to **impose an obligation for third-party checkers to communicate accurate information regarding DNCR results**, and they can be held liable for infringements of the DNC Provisions under the New Act, as a result of inaccurate information that they had provided to the sender.

[22] Refer to section 43 of the PDPA.
[23] Refer to section 44 of the PDPA.
[24] Refer to section 45 of the PDPA.

4.4 In addition, as the reselling of DNCR lists by third-party checkers increases the risk of potential DNC infringements, PDPC proposes to **prohibit the resale of any results of telephone numbers that were screened through the DNCR.** This is to protect the integrity and accuracy of results of checks with the DNCR. Third-party checkers can still check on behalf of senders but may not sell or provide the results of such DNC checks to other parties that it did not check on behalf of. Senders who check directly with the DNCR as well as senders who receive DNCR results from third-party checkers will also not be allowed to sell or provide the results of such DNC checks to other parties.

> ***Question 7: What are your views on the proposed obligation to communicate accurate DNCR results, and liability on third-party checkers for any infringements of the DNC Provisions resulting from inaccurate information they provided?***
>
> ***Question 8: What are your views on the proposed prohibition of resale of results of telephone numbers checked with the DNCR?***

Presumption of sending

4.5 Section 43(1) of the current PDPA requires the identification and proof of the actual sender of the marketing message. PDPC's experience has been that senders of marketing messages are frequently subscribers of the telephone service and it does not matter to the recipient of the marketing message whether the subscriber sent the marketing messages personally or through an employee or agent. Further, the subscriber of the telephone service is expected to ensure that the telephone service is not misused. The subscriber cannot, for example, hand the SIM card to another person who then uses it to send marketing messages.

4.6 As such, PDPC proposes to **introduce a deeming provision under the DNC Provisions under 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 is expected to improve enforcement effectiveness and ensure greater responsibility on subscribers on taking active steps to prevent misuse of their telephone service. At the same time, should the specified message be sent by a third party, PDPC will consider any evidence submitted by the subscriber to substantiate the same.

> ***Question 9: What are your views on the proposed deeming provision?***

PART III: ENHANCED PRACTICAL GUIDANCE

5 Need for Enhanced Practical Guidance

5.1 Today, PDPC provides guidance ("Practical Guidance") in relation to how specific PDPA provisions apply to a specific business activity and factual situation facing the organisation. This is to reduce the uncertainty an organisation may face with respect to its compliance with specific obligations under the PDPA in the context of its particular situation. PDPC may provide Practical Guidance for complex queries that cannot be addressed by reference to PDPC's published resources (e.g., advisory guidelines, guides). PDPC's Practical Guidance does not constitute legal advice, and does not provide confirmation of an organisation's compliance or recommendation of a particular course of action that the organisation should take to comply with the PDPA.

5.2 In the course of providing Practical Guidance to organisations, PDPC has received requests from organisations seeking confirmation and assurance that their business practices are compliant with the PDPA. PDPC proposes to introduce an Enhanced Practical Guidance ("EPG") framework for the PDPC to provide organisations **guidance with regulatory certainty** ("determinations"). This is to facilitate the development of new and innovative data services, recognising the immense opportunities for innovations around the use of data as Singapore gears up to be a Digital Economy.

5.3 The proposed EPG framework will:

a) address the current gap for addressing complex compliance queries that cannot be addressed by published resources and professional data protection services or legal advice; and

b) provide regulatory certainty which current guidance provided by PDPC does not provide.

5.4 Overseas jurisdictions have provided for similar frameworks, where the data protection authority is able to issue guidance to organisations that are legally binding. For instance, the Office of the Information and Privacy Commissioner ("OIPC") for British Columbia may issue legally binding decisions[25] to confirm whether a matter is within its jurisdiction or whether an access request may be disregarded, amongst others. In Victoria, the Office of the Commissioner for Privacy and Data Protection ("CPDP") may provide certification[26] that a specified act or practice is consistent with an information privacy principle, an approved code of practice, or an information handling provision. In Singapore, a similar framework is provided for by the Competition and Consumer

[25] Refer to British Columbia's Personal Information Protection Act.

[26] Refer to Victoria's Privacy and Data Protection Act 2014.

Commission of Singapore ("CCCS"), which may issue decisions as to whether an agreement, conduct or merger situation infringes the Competition Act.

6 Proposed criteria and scope

6.1 Under the proposed EPG framework, PDPC may provide determinations on whether a particular business activity complies with specific Data Protection Provision(s) under the PDPA. The queries must be from the organisation(s) performing the business activity for which the guidance is sought. PDPC will also not provide determinations to queries relating to hypothetical situations, or queries that entail a review of the organisation's entire business model, processes or policies.

6.2 PDPC will assess requests for 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**[27].

6.3 Where there is an ongoing investigation into the organisation in relation to the issue in question by PDPC or other regulatory or law enforcement agencies, PDPC will not accept the EPG application.

6.4 PDPC's provision of determinations under the EPG framework will be chargeable. This is to deter frivolous requests and in consideration that a more rigorous assessment will be required in order for PDPC to provide determinations that are binding under the EPG framework. PDPC intends to calibrate the fees to be charged according to the type and size of organisation to ensure that costs are not prohibitive for SMEs and start-ups.

6.5 Under the EPG framework, PDPC will assess the facts of the case based on information provided by the organisation, and provide a **determination as to whether a particular business activity or course of action in the given circumstances complies with specific Data Protection Provision(s) of the PDPA**. PDPC envisages that the EPG assessment will be an iterative process with the organisation, and PDPC will take into account any proposed measures that the organisation may adopt. The EPG framework is intended to support organisations with innovative solutions but not intended for organisations to seek solutions from PDPC to comply with the Data Protection Provision(s). Hence,

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

organisations applying for EPG are expected to propose solutions for ensuring compliance. Notwithstanding PDPC's determination, organisations will be expected to conduct their own risk and impact assessments and take appropriate measures to mitigate any risks.

6.6 PDPC will continue to provide the current Practical Guidance and organisations may choose whether to request for the Practical Guidance or determinations under the EPG framework. Alternatively, organisations that require more certainty after receiving PDPC's guidance may apply for a determination under the EPG framework.

6.7 Similar to the current Practical Guidance provided by PDPC, a redacted version of PDPC's determination will be published on a case-by-case basis without disclosing any confidential or commercially sensitive information, to help raise awareness on matters which PDPC's determination was provided.

7 Proposed validity and effect of determinations

7.1 To provide regulatory certainty to organisations, PDPC proposes for the determinations issued 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.

7.2 Where the PDPC receives a complaint relating to the subject of an EPG determination that is no longer valid due to changes to the PDPA, PDPC may take into consideration factors such as the date of the change to the PDPA and may provide a grace period for the organisation to comply with the revised PDPA. Regardless of whether PDPC receives a complaint, organisations may seek further guidance from PDPC on complying with the revised PDPA.

Regulatory relief and information provided during EPG determination process

7.3 In addition, PDPC will not initiate investigations in situations where PDPC, in the course of assessing and providing a determination to an organisation, finds any non-compliance with the PDPA based on the information submitted by the organisation. 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. In the event that a complaint is received during the course of assessment, PDPC reserves the right to terminate the assessment and commence investigations.

7.4 PDPC will not use the information provided by the organisation for the EPG assessment as part of its investigations. This would ensure the integrity of the EPG Framework, and safeguard business confidentiality.

7.5 For the avoidance of doubt, the grace period (see paragraph 7.2) and the regulatory relief (see paragraph 7.3) provided under the EPG framework would only apply to the requesting organisation to which the EPG was given or is being assessed for (respectively), and not to any other organisation.

8 Proposed exemption under EPG framework

8.1 PDPC envisages that in some cases, EPG assessments may lead to the organisation applying for an exemption[28] where the organisation is unable to comply with specific PDPA provision(s) and is unable to rely on any exception under the PDPA for the business activity. For expediency, PDPC may provide for exemptions from specific PDPA provision(s) to be sought from Minister as part of its determinations issued under the EPG framework, where applicable.

Question 10: What are your views on the proposed Enhanced Practical Guidance framework?

[28] Refer to section 62 of the PDPA.

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

9 Solicitation of feedback on exceptions to consent

9.1 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, the PDPC seeks feedback from organisations on the practicality of relying on these exceptions. In particular, feedback is sought 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.

9.2 Organisations providing feedback on their experience in considering how specific exceptions apply in their specific circumstances should provide sufficient details in order for the PDPC to understand the practical issues faced. If there are confidential or commercially sensitive details, organisations may identify these and request for their redaction from the published feedback.

9.3 Organisations providing feedback based on advances in technology, changes in business practices or legislative changes since the enactment of the PDPA (including proposed amendments to the PDPA in prior public consultation) should provide sufficient details and a bibliography of key reference materials.

9.4 The PDPC may not consider feedback under this Part that are unsubstantiated or theoretical.

PART V: SUBMISSION OF COMMENTS

10.1 Parties that wish to submit comments on this public consultation paper should organise their submissions as follows:

a) cover page (including particulars of the organisation and contact person);

b) comments, with reference to specific sections or paragraphs if appropriate; and

c) conclusion.

10.2 Supporting material may be placed in an annex. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any comments. Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.

10.3 All submissions should reach PDPC by **7 June 2018**. Comments should be submitted:

a) in soft copy (in Microsoft Word format);

b) to the following e-mail address: corporate@pdpc.gov.sg; and

c) with the email header: "PDPC's Public Consultation on Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy".

10.4 The PDPC reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. If the PDPC grants confidential treatment, it will consider, but will not publicly disclose, the information. If the PDPC rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider this information as part of its review. As far as possible, parties should limit any request for confidential treatment of information submitted. The PDPC will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.

END OF DOCUMENT