PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

DRAFT ADVISORY GUIDELINES ON KEY PROVISIONS OF THE PERSONAL DATA PROTECTION (AMENDMENT) BILL

Issued 20 November 2020

TABLE OF CONTENTS

1 Introduction 3

2 Enhanced Framework for Collection, Use and Disclosure of Personal Data 4

Obtaining consent from an individual 4

Deemed consent 5

Exceptions to the Consent Obligation 14

Assessments for relying on deemed consent by notification and legitimate interests exception 20

3 Mandatory Data Breach Notification 30

Duty to conduct assessment of data breach 30

Criteria for data breach notification 33

Timeframes for notification 37

Exceptions from the requirement to notify affected individuals 37

Prohibition and waiver of the requirement to notify affected individuals 39

Mode of notification of data breach 40

Information to be provided in notification of data breach 41

4 Financial Penalties 44

5 Offences for Egregious Mishandling of Personal Data 50

Applicable defences 51

Re-identification of anonymised data 51

Annex A: PDPA's Enhanced Framework for the Collection, Use and Disclosure of Personal Data

Annex B: Assessment Checklist for Deemed Consent by Notification

Annex C: Assessment Checklist for Legitimate Interests Exception

1 Introduction

1.1 The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by organisations in Singapore. Enacted in 2012, it aims to strike a balance between the need to protect individuals' personal data and private organisations' need to collect, use and disclose personal data for legitimate and reasonable purposes. The Do Not Call (DNC) Provisions of the PDPA enable individuals to opt-out of receiving specified messages[1] in the form of text messages, fax messages or voice calls, sent to Singapore telephone numbers, by requiring persons to check the relevant DNC Register before sending a specified message to a Singapore telephone number[2]. The DNC Provisions and the Data Protection (DP) Provisions came into effect on 2 January 2014 and 2 July 2014, respectively.

1.2 The Personal Data Protection Commission (PDPC) is established under the PDPA with the key functions, amongst others, of promoting awareness of data protection in Singapore and administering and enforcing the PDPA.

1.3 Following public consultations conducted by the PDPC between 2017 and 2020 on key policy positions[3] and the draft Personal Data Protection (Amendment) Bill[4], the Bill was tabled in Parliament for First Reading in October 2020 and passed in Parliament in November 2020.

1.4 The draft Advisory Guidelines are intended to provide the PDPC's clarification on key provisions in the Personal Data Protection (Amendment) Bill and are not meant to exhaustively cover all the amendments to the PDPA. The Advisory Guidelines will be finalised and issued when the amendments to the PDPA come into effect[5].

[1] "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.

[2] Unless the person has obtained clear and unambiguous consent from the individual or has an ongoing relationship with the individual.

[3] The public consultations for these proposals and responses to the feedback received can be found at www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations.

[4] The public consultation and responses to the feedback received for the draft Personal Data Protection (Amendment) Bill can be found at www.mci.gov.sg/public-consultations/archived.

[5] The PDPC's Advisory Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines" and are subject to the disclaimers set out therein.

2 Enhanced Framework for Collection, Use and Disclosure of Personal Data

2.1 Section 13 of the current PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. This obligation to obtain the individual's consent is referred to in these Guidelines as the 'Consent Obligation'.

2.2 This obligation does not apply where the collection, use or disclosure of an individual's personal data is required or authorised under the PDPA or any other written law. However, organisations may still need to comply with other requirements of the DP Provisions. Please refer to **Annex A** for further information on the enhanced framework for the collection, use or disclosure of personal data, to obtain consent in a way that is meaningful to individuals.

Obtaining consent from an individual

2.3 Section 14(1) of the current PDPA states how an individual gives consent under the PDPA. An individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. If an organisation fails to do so, any consent obtained from the individual would be invalid.

2.4 Consent can be obtained in several ways. Consent that is obtained in writing or recorded in a manner that is accessible is referred to in these Guidelines as 'express consent'. Such consent provides the clearest indication that the individual has consented to notified purposes of the collection, use or disclosure of his personal data.

2.5 In situations where it may be impractical for the organisation to obtain express consent in writing, it may choose to obtain verbal consent. As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally, to prove that verbal consent had been given, in the event of disputes:

a) Confirm the consent in writing with the individual (which may be in electronic form or other form of documentary evidence); or

b) Where appropriate in the circumstances, make a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal consent.

Example: Written consent after signing up for services over the telephone

An individual wishes to sign up for certain services with a service provider over the telephone. The service provider may request the individual's consent for the collection and use of his personal data for the service provider's purposes and obtain the personal data from the individual over the telephone.

It would be good practice for the service provider to subsequently contact the individual and confirm his consent in writing. For example, by sending an email to the individual setting out the description of the personal data provided by the individual, and recording his consent to the collection, use and disclosure by the service provider for the service provider's purposes (which may be set out in its terms and conditions and/or other information provided in the email).

2.6 Organisations that wish to rely on the individual's consent to send specified messages to Singapore telephone numbers should ensure that the individual has given clear and unambiguous consent beforehand. Consent for the sending of specified messages to Singapore telephone numbers should be evidenced in written or other accessible form. For this purpose, verbal consent alone would be insufficient.

Deemed consent

2.7 Section 15 of the current PDPA already allows for consent deemed from an individual's action (referred to as 'deemed consent by conduct' in these Guidelines).

2.8 The Bill introduces two new forms of deemed consent:

a) **Deemed consent by contractual necessity**. This is where consent is deemed for the disclosure of personal data from one organisation to another for the necessary conclusion or performance of a contract/transaction between the individual and the organisation he had originally provided the personal data to; and

b) **Deemed consent by notification**. This is where consent is deemed from an individual's acquiescence after notification and where the notification is in compliance with certain requirements.

2.9 Further, where an individual gives or is deemed to have given consent for disclosure of his personal data by one organisation ("A") to another organisation ("B") for a

purpose, the individual is deemed to consent to the collection of his personal data by B for that purpose.

Deemed consent by conduct

2.10 Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances. Pursuant to section 15(1), consent is deemed to have been given by the individual's act of providing his personal data.

2.11 An individual may be regarded as voluntarily providing personal data where the individual takes certain actions that allow the data to be collected, without providing the data himself. Consent is deemed to be given to the extent that the individual intended to provide his personal data and took the action required for the data to be collected by the organisation.

Example: Deemed consent for processing of payment

Sarah makes a visit to a spa for a facial treatment. After the treatment is complete, the cashier tells her that the facial would cost her $49.99. She hands over her credit card to the cashier to make payment. The cashier need not ask for Sarah's consent to collect, use or disclose her credit card number and any other related personal data (e.g. name on credit card) required to process the payment transaction.

Sarah is deemed to have consented to the collection, use and disclosure of her credit card number and other related personal data for processing of the payment as she voluntarily provided the personal data and it is reasonable that Sarah would provide the personal data to pay for her facial.

Example: Deemed consent for health check-up

Eva goes for a health check-up at a clinic and is given information on the tests that will be conducted, which involves the collection of her blood pressure, height and weight. By proceeding with the tests, Eva is deemed to consent to the collection of her personal data by the clinic for the purposes of the health check-up.

Example: Deemed consent for taxi booking

Tina calls a taxi operator's hotline to book a taxi. The customer service officer asks for her name and number to inform her of the taxi number, which Tina provides voluntarily. Tina is deemed to have consented to the taxi company using her name and number to call or text her when her taxi arrives.

However, if the taxi operator runs a limousine service and wants to use Tina's information to market this service to her, Tina would not be deemed to have consented to the use of her personal data for this purpose. This is because Tina is providing her personal data for booking a taxi for a single trip, and not for receiving marketing information about the limousine service.

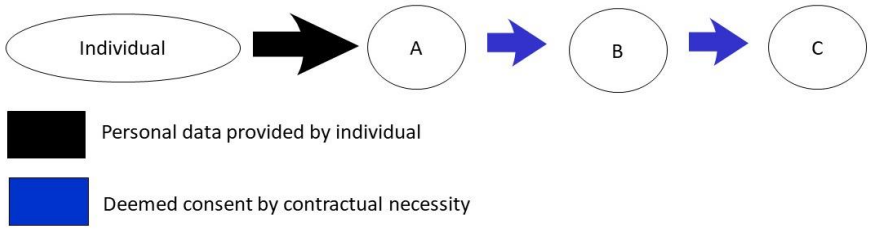
2.12 Depending on the facts in some cases, the PDPC may consider that consent is inferred or implied from the circumstances or the conduct of the individual in question. This is a form of consent where the individual does, in fact, consent to the collection, use and disclosure of his personal data (as the case may be) by his conduct, although he has not expressly stated his consent in written or verbal form[6].

Deemed consent by contractual necessity

2.13 The second situation in which consent may be deemed is where an individual provides his personal data to one organisation ("A") for the purpose of a transaction and it is reasonably necessary for A to disclose the personal data to another organisation ("B") for the necessary conclusion or performance of the transaction between the individual and A. Deemed consent by contractual necessity under the new section 15(3) extends to disclosure by B to another downstream organisation ("C") where the disclosure (and collection) is reasonably necessary to fulfil the contract between the individual and A. To be clear, deemed consent by contractual necessity allows further use or disclosure of personal data by C and other organisations downstream (refer to Diagram 1 below) where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and A.

[6] Please refer to *Re German European School Singapore* [2019] SGPDPC 8, in relation to implied consent inferred from the parents' decision to enrol their child and to continue his enrolment in the school, after having the school's by-laws made available to them.

Diagram 1:



Example: Deemed consent for processing of payment

In an example above, Sarah is deemed to consent to a spa collecting, using or disclosing her credit card details to process the payment for her facial. In the course of processing the payment, her credit card details are transmitted to the spa's bank who handles the payment. Since Sarah is deemed to consent to the disclosure of her credit card details by the spa to its bank, deemed consent by contractual necessity would apply to all other parties involved in the payment processing chain who collects or uses Sarah's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the contract between Sarah and the spa. These parties include, for example, Sarah's bank, the spa's bank, the banks' processers and the credit card scheme's payment system providers.

Example: Deemed consent for processing of GIRO deduction and tax relief

Benjamin donates $5,000 to a charity organisation and provides his personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on the charity organisation's website. The form clearly states the purposes of collection, use or disclosure of donors' personal data – for the charity organisation to process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. Since Benjamin consents to the collection, use and disclosure of his personal data by the charity organisation for the notified purposes, deemed consent by contractual necessity would apply to all other parties involved in the GIRO and tax relief processing chain who collects, uses or discloses Benjamin's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Benjamin and the charity organisation. These parties include, for example, Benjamin's bank, the charity organisation's bank, the banks' processers, and the tax authority.

Example: Deemed consent for processing of payment and delivery

Bella orders furniture from a retailer through an e-commerce platform and provides her personal data (e.g. credit card details, contact number and residential address) for the purchase and delivery of goods. She also selects the option to have her furniture delivered to her home by a delivery company.

The retailer can rely on deemed consent by contractual necessity to disclose Bella's personal data to the delivery company as the disclosure is reasonably necessary to fulfil the transaction between Bella and the retailer. The delivery company and all other parties involved in Bella's transaction with the retailer would also be able to rely on deemed consent by contractual necessity to collect, use or further disclose personal data where reasonably necessary to fulfil the transaction between Bella and the retailer. These parties include, for instance, the e-commerce company, the online payment gateway in which payment for the transaction is processed, the relevant banks and logistics service partners (e.g. sub-contractors in the entire delivery chain, including the last mile delivery to Bella's home).

Deemed consent by notification

2.14 The new section 15A of the PDPA provides that an individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data. Deemed consent by notification is useful where the organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any of the exceptions to consent (e.g. business improvement, research) for the intended secondary use. This is subject to the organisation assessing and determining that the following conditions are met, taking into consideration the types of personal data involved and the method of collection, use or disclosure of the personal data in the manner set out below:

a) **Conduct an assessment to eliminate or mitigate adverse effects**: Section 15A(4)(a) of the PDPA provides that an organisation must, before collecting, using or disclosing any personal data about an individual, conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual. The assessment for relying on deemed consent by notification will also have to take into consideration the method of notification and opt-out period (see paragraphs 2.14(b) and (c)). Apart from identifying the likely adverse effects, the organisation's assessment should consider any measures to be taken by

the organisation to eliminate, reduce the likelihood of or mitigate the adverse effects identified. Organisations should rely on the **Assessment Checklist for Deemed Consent by Notification** (at **Annex B**) to conduct the assessment. Please refer to paragraphs 2.29 – 2.34 on conducting the assessment.

b) **Organisation must take reasonable steps to ensure that notification provided to individuals is adequate**: Section 15A(4)(b) of the PDPA provides that an organisation must take reasonable steps to bring the following matters to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose of such collection, use or disclosure; and (iii) a reasonable period within which, and a reasonable manner by which, an individual can opt out of the collection, use or disclosure of his personal data for this purpose. The PDPC does not prescribe the method by which the individual should be notified, but the organisation must ensure the notification is adequate and effective in making the individual aware of the proposed collection, use or disclosure of his personal data[7]. Organisations may choose to rely on a single mode or multiple modes of communication in notifying individuals adequately. Some considerations for determining the appropriate mode(s) of communication include:

(i) The **usual mode of communication** between the individual and the organisation.

(ii) **Whether direct communication channels such as mail, email messages, telephone calls or SMS[8] are available**. Notification provided through **interactive portals and applications** may also be considered. These could include push notifications sent through mobile applications. These also include dashboards or consent portals where individuals can keep track of their interactions with the organisation, including their preferences on purposes for which they consent to the collection, use or disclosure of their personal data. However, organisations should note that these channels may not always be effective (e.g. contact information may not be updated).

(iii) **Number of individuals to be notified**. In particular, where the organisation intends to reach out to a large number of individuals, and

[7] Refer to Chapter 14 on the Notification Obligation in the Advisory Guidelines on Key Concepts in the PDPA, and PDPC's Guide to Notifications.

[8] Where the notification constitutes a "specified message", the organisation must comply with the DNC Provisions of the PDPA in sending the message via voice call, text or fax.

assesses that direct communication channels are not effective, other forms of **mass communication channels** may be considered. These include a micro-site on the organisation's corporate website, notification through the organisation's social media channels, and notifications through printed or other news media.

Example: Providing appropriate notification to users of mobile application

A health app company provides a mobile application that collects, uses and discloses personal data relating to individuals' lifestyle and wellness (e.g. number of steps walked, height, weight, age and gender). Users are able to view their activity data (e.g. sleep patterns, periods of activity, number of calories lost) through the mobile application.

The health app company intends to use the lifestyle and wellness data collected from its users to provide a personalised weight loss programme for its users. It intends to use the users' personal data to provide the personalised programme through the application installed on their devices. It assesses that there is no likely adverse effect to users in using their personal data for this purpose. Thereafter, each user can decide whether to participate after viewing the personalised programme (in which case express consent will be obtained).

The health app company decides that the best way to notify users is through the mobile application as it is a direct and effective way to communicate with users who are monitoring their activity through the application. To ensure inactive users of the application are notified, it notifies users by email and through its social media channels.

c) **Organisation must provide a reasonable opt-out period**: The organisation must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the personal data. Consent for the collection, use or disclosure of personal data is deemed to be given only after the opt-out period has lapsed. Any collection, use or disclosure of personal data for the purposes that have been notified should commence only after the expiry of the opt-out period. Deemed consent by notification should not be relied on where individuals would not have a reasonable opportunity and period to opt out (e.g. security monitoring of premises using video cameras). The PDPC does not prescribe a specific opt-out period, and organisations shall assess and determine a reasonable period for individuals to opt out of the collection, use or disclosure of personal data. Some considerations for determining the reasonableness of the opt-out period include:

(i) **The nature and frequency of interaction with the individual**. For instance, where an organisation sends push notifications through a mobile application used by individuals to track and update monthly medical check-up information, the opt-out period should not be shorter than one month.

(ii) **The communications and opt-out channels used**. Direct communications channels, particularly those that have a track record of being effective in reaching the intended customer base, may justify a shorter opt-out period than mass communications channels. Opt-out methods that are easily accessible and easy to use may also justify a shorter opt-out period (e.g. providing for opt-out via email or hyperlink).

2.15 After the opt-out period has lapsed and the individual no longer wishes to consent to the purpose, the individual can withdraw his consent for the collection, use or disclosure of personal data.

2.16 When requested by the PDPC, the organisation must provide to the PDPC its assessment for collecting, using or disclosing personal data based on deemed consent by notification. The organisation is not required to provide its assessment to individuals who request for it as it may contain commercially sensitive information.

Example: Hotel's sharing of personal data with partners

A hotel chain wishes to rely on deemed consent by notification to disclose personal data of its members (e.g. frequency and length of hotel stays, type of rooms, preferences and reviews) to travel website company to develop online travel resources and customised travel packages. The personal data it shares will not be used to obtain consent for sending direct marketing messages to members.

The hotel chain assesses that there is no likely adverse effect to its members in disclosing their personal data for this purpose. The hotel chain also assesses that emailing members on the intended sharing of their personal data is an appropriate and effective method of notification, as it regularly sent emails to its members regarding membership points, rewards and offers. It also assesses that 10 days is a reasonable period for individuals to opt out.

The hotel chain sends an email to its members which notifies them of the intended disclosure of their personal data to the travel website company for the purpose and provides a contact number for any queries on the intended disclosure. A hyperlink is provided in the email for members to opt out of it,

and the hotel chain requests that members who wish to opt out do so within 10 days from the date of the email.

Members who do not opt out within the 10-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for this purpose. The hotel chain will need to allow and facilitate any withdrawal of consent from members after the 10-day opt-out period.

Example: Banks' use of voice data for customer authentication

A bank collects voice data of customers when they call the bank's contact centre for managing disputes. Customers are informed that their voice data is collected for this purpose.

The bank intends to use the collected voice data (i.e. voiceprint) as an alternate means of authentication to complement existing verification methods (e.g. where the customer misplaces his credentials or where his mobile number is tagged to his bank account).

The bank assesses that its authentication of customers using voiceprint is sufficiently reliable and secure, and there is no likely adverse effect to its customers in using their personal data for this purpose. It also assesses that emailing customers on the intended use of their personal data would be an appropriate and effective method of notification, as the bank regularly sends emails to its customers regarding the changes in its business operations and privacy policy. It also assesses that 14 days is a reasonable period for customers to opt out.

The bank sends an email to its customers to notify them of the intended use of their voice data for authentication purposes and provides a contact number for customer queries. A hyperlink is provided in the email for customers who wishes to opt out of the use of their voice data for this purpose within 14 days from the date of the email.

Customers who do not opt-out within the 14-day opt-out period are deemed to consent to the use of their voice data for this purpose. After the expiry of the opt-out period, the bank may commence using voice data of customers who have not opted out to develop the biometric signatures that would be used for authentication. The bank must also allow and facilitate any requests from customers to withdraw their consent to use their voice data for this purpose after the 14-day opt-out period.

Example: Event company's use of sensors to collect visitors' personal data

An association is organising an exhibition for its members and intends to deploy sensors at the exhibition venue to collect facial images and movement data of those who visit the exhibition. The data collected would be used to analyse the exhibits visited and duration spent by each visitor. The exhibition is only open to members of the association and is not open to the public.

The association may not rely on deemed consent by notification by putting up notifications at the exhibition venue to inform visitors that facial images and movement data collected by sensors deployed at the exhibition venue would be used for analysing the exhibits visited and duration spent, as it would not be able to provide a reasonable period for them to opt out from the use of their data for this purpose.

2.17 The PDPC recognises that there are various ways of implementing the opt-out method. The PDPC will consider the circumstances and facts of each case in assessing whether the conditions for relying on deemed consent by notification have been met.

Consent for sending of directing marketing messages

2.18 The PDPC will prescribe in Regulations the purposes for which deemed consent by notification shall not apply. This will include the purpose of sending **direct marketing messages**.

2.19 Organisations should generally obtain express consent for the purpose of sending direct marketing messages to individuals. Such consent should be obtained through the opt-in method (e.g. requiring action to check an unchecked box in order to give consent); the PDPC does not consider the opt-out method (e.g. providing a pre-checked box and requiring action to opt-out) as appropriate for obtaining consent for the receipt of direct marketing messages. Similarly, consent obtained using the opt-out method will not constitute clear and unambiguous consent under the DNC Provisions for sending a specified message to a Singapore telephone number registered on the DNC Registry.

Exceptions to the Consent Obligation

2.20 The new section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual), only in the circumstances provided in the new First and Second Schedules to the PDPA. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.

Legitimate interests exception

2.21 "Legitimate interests" generally refer to any lawful interests of an organisation or other person (including other organisations). Paragraphs 2 to 10 under Part 3 of the new First Schedule to the PDPA relate to specific purposes that would generally be considered "legitimate interests", for instance, for evaluative purposes, for any investigation or proceedings, or for recovery or payment of debt owed. Legitimate interests exceptions in Paragraphs 2 to 10 under Part 3 of the new First Schedule are specific exceptions which organisations can rely on if these are applicable. The general legitimate interests exception ("legitimate interests exception") in Paragraph 1 under Part 3 of the new First Schedule is a broad exception that can be relied on for any other purposes that meet the definition of "legitimate interests", when other specific exceptions do not apply. To rely on this general exception, organisations will need to assess the adverse effect and ensure the legitimate interests outweigh any adverse effect.

2.22 As the legitimate interests exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes, the onus is on the organisation seeking to rely on this exception to comply with additional safeguards to ensure that the interests of individuals are protected. Organisations must assess that they satisfy the following requirements before relying on the legitimate interests exception:

a) **Identify and articulate the legitimate interests**. Organisations must identify and be able to clearly articulate the situation or purpose that qualifies as a legitimate interest.

b) **Conduct an assessment**. Paragraph 1(2)(a) read with paragraph 1(3) under Part 3 of the new First Schedule, provides that an organisation must conduct an assessment before collecting, using or disclosing personal data (as the case may be) to (i) identify any adverse effect that the proposed collection, use or disclosure is likely to have on the individual; and (ii) identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effect on the individual. Where it is assessed that there is likely residual adverse effect to the individual after implementing the measures, organisations are required to conduct a balancing test as part of the assessment to determine that the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect to the individual. Organisations may wish to use the **Assessment Checklist for Legitimate Interests Exception** (at **Annex C**) to conduct the assessment. Please refer to paragraphs 2.29 – 2.34 for the considerations when conducting the assessment.

c) **Disclose reliance on the legitimate interests exception**. Paragraph 1(2)(b) under Part 3 of the new First Schedule provides that organisations relying on the legitimate interests exception to collect, use or disclose personal data without consent must take reasonable steps to provide the individual with reasonable access to information that they are relying on the exception. This may be through any means that is reasonably effective (e.g. disclosure as part of the organisation's public data protection policy).

Identify and articulate the legitimate interests

2.23 In identifying the legitimate interests of collecting, using or disclosing the personal data for a purpose, organisations should be able to articulate the following:

a) ***What the benefits and who the beneficiaries are***: Organisations should identify the benefits arising from the collection, use or disclosure of the personal data, and who the beneficiaries are. The benefits identified should focus primarily on direct benefits of the collection, use or disclosure of the personal data. Examples of benefits include security of business assets and individuals at premises, prevention of fraud and misuse of services, etc. Organisations should also consider whether there could be any negative impact on individuals, or a particular group of individuals should the organisation not be able to collect, use or disclose the personal data without consent for the purpose. Apart from benefits to the organisation, beneficiaries could also include other organisations, the wider public or a segment of the public such as customers, employees, sectors or industries of the economy.

b) ***Whether the benefits are real and present***: In general, the identified benefits should not be purely speculative, and should include both tangible (e.g. increased business efficiency and cost savings) and intangible benefits (e.g. improved customer experience). The presence of related commercial or business interests does not subtract from the public benefits which may be derived, and all the benefits to each identified beneficiary should be considered.

2.24 Organisations cannot rely on the legitimate interests exception to send direct marketing messages. In general, organisations must obtain express consent to send direct marketing messages to individuals. In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the DNC Provisions of the PDPA[9].

[9] Refer to PDPC's Advisory Guidelines on the Do Not Call Provisions.

Disclose reliance on legitimate interests exception

2.25 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data must make it known to individuals that they are relying on this exception to collect, use and disclose personal data without consent. For example, an organisation could state in its public data protection policy that it is relying on the legitimate interests exception to collect, use or disclose personal data for purposes of security and prevention of misuse of services. To be clear, organisations are not required to make available their assessments of legitimate interests to the public or to individuals as part of disclosing reliance on the exception.

2.26 Organisations must also provide the business contact information of a person who is able to address individuals' queries about the organisations' reliance on the legitimate interests exception. This person may be the Data Protection Officer or someone charged with the responsibility to handle such queries. This is similar to the requirement under the PDPA where an organisation needs to inform an individual of the purpose of the collection, use or disclosure of his personal data when it enters into an employment relationship or appoints the individual to any office; or manages or terminates an employment relationship[10], except that the information relating to the reliance on the legitimate interests exception will have to be provided through channels that are external-facing (e.g. general notification in the company's data protection policy on its publicly-accessible website).

Justify reliance on legitimate interests upon the PDPC's request

2.27 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data are to document their assessments and steps taken to mitigate residual risks. Upon the PDPC's request, organisations are required to provide justification to the PDPC on their reliance on the legitimate interests exception, including their assessments of legitimate interests (which includes balancing tests), and other related documents. Given the potential commercial sensitivity of organisations' assessments, the assessments need not be made available to the public or to individuals.

[10] The new section 20(4) and (5) of the PDPA provides that, despite subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of entering into an employment relationship with the individual or appointing the individual to any office; or managing or terminating the employment relationship with or appointment of the individual, shall inform the individual of (a) that purpose; and (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation.

Examples of legitimate interests

2.28 Examples of legitimate interests include the purposes of detecting or preventing illegal activities (e.g. fraud, money laundering) or threats to physical safety and security, IT and network security; preventing misuse of services; and carrying out other necessary corporate due diligence[11]. Subjecting such purposes to consent is not viable as individuals may choose not to give consent or to withdraw any consent earlier given (e.g. individuals who intend to or who had engaged in illegal activities), impeding the organisations' ability to carry out such functions.

Example: Fraud detection and prevention purposes by a company

An insurance company intends to collect, use and disclose personal data about its customers' past insurance claims for fraud detection and prevention.

The insurance company conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data outweigh any adverse effect to the individual. Insurance company states in its data protection policy on its website that it is relying on the legitimate interests exception to collect, use and disclose personal data for fraud detection and prevention purposes.

In this case, the insurance company may rely on the legitimate interests exception to collect, use or disclose personal data for detecting and preventing fraud.

Example: Fraud detection by multiple companies

A healthcare service provider and multiple insurance companies intends to share personal data (i.e. medical records, payment information, patient's health insurance policies, claim records) to detect and prevent healthcare fraud and abuse (e.g. duplicated claims) by creating a fraud detection model.

The companies conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of personal data outweighs any adverse effect to the individual. These companies also include in their respective data protection policies on their websites that they are relying on the legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

[11] This would apply to organisations that intend to conduct further and necessary corporate due diligence on customers, potential customers and business partners in addition to existing statutory requirements. For instance, the collection, use and disclosure of personal data for the consolidation of official watch lists.

The companies may rely on the legitimate interests exception to collect, use and disclose the personal data of their customers to detect and prevent misuse of their services.

Example: Hotels' detection and prevention of misuse of services by guests

Several hotels intend to compile and share a blacklist of hotel skippers (i.e. hotel guests with track record of not fulfilling their payments for use of hotel services) to prevent further misuse of their services. The blacklist would contain the personal data of hotel skippers (i.e. full name, NRIC/passport number, amount owed and details of non-payment) who have two or more occurrences of non-payment for the use of hotel services.

These hotels conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of the personal data outweigh any adverse effect to the individuals. These hotels also include in their respective data protection policies on their websites that they are relying on legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

The hotels may rely on the legitimate interests exception to collect, use and disclose the personal data of customers to detect and prevent misuse of their services.

Example: Bank's network analysis to prevent fraud and financial crime, and perform credit analysis

A bank intends to integrate data across individuals and their associated organisations and businesses to build further profiles about them. The use of personal data allows the bank to identify individuals who may have committed a financial crime or received funds in relation to a crime; and to identify individuals and organisations with credit inter-dependencies to form better assessments of their actual credit standings and sources of funds for repayment.

In addition to comply with the Monetary Authority of Singapore's (MAS) requirements[12], the bank conducts an assessment of legitimate interests and assesses that the benefits of using the data (i.e. detection and deterrence of flow of illicit funds through Singapore's financial system, understanding prospects' or customers' financial standing) outweigh any likely adverse effect to the individuals (e.g. identification of individuals with potential nefarious

[12] Banks in Singapore are required to ensure their collection, use and disclosure of personal data are in accordance with the MAS requirements to prevent money laundering and countering the finance of terrorism.

intentions, enforcement actions by authorities, and impact on credit facilities to individuals assessed to be of poorer credit standing).

The bank includes in its privacy policy that it is relying on the legitimate interests exception to collect, use and disclose personal data for conducting credit checks, analyses and due diligence checks as required under applicable laws.

In this case, the bank may rely on the legitimate interests exception to collect, use and disclose personal data to prevent fraud and financial crime, and perform credit analysis.

Example: Collection and use of personal data on company-issued devices to prevent data loss

As part of its internal security defence and data loss prevention strategy, a technology company intends to install a data loss prevention software on the laptops, desktops and mobile devices which it issues to its employees so that it can effectively detect any unauthorised data leakage, disclosure or loss of its information. The tool collects a variety of personal data about its users (e.g. user log-in details, device information, files, device communications and content).

The technology company conducts an assessment of legitimate interests and assesses that the benefits of the collection of personal data to protect its commercial and proprietary interests outweigh any likely adverse effect on its employees.

The technology company includes in its privacy policy and employee handbook to inform its employees that it is relying on the legitimate interests exception for the collection and use of personal data through the software installed on company-issued devices.

Assessments for relying on deemed consent by notification[13] and legitimate interests exception[14]

2.29 Organisations are required to conduct assessments of any likely adverse effect to the individual when relying on deemed consent by notification or the legitimate interests exception.

2.30 In general, the PDPC considers adverse effect to include any physical harm, harassment, serious alarm or distress to the individual. There may be circumstances where individuals may be affected by businesses' decisions resulting from the use of

[13] Refer to section 15A(4)(a) of the PDPA.
[14] Refer to Paragraph 1(2)(a) and (3) of the PDPA under Part 3 of the new First Schedule.

personal data (e.g. differential pricing for customers of differing purchase history or payment track records). To be clear, while the collection, use or disclosure of an individual's personal data could result in differentiated treatment of individuals, not all instances of differential charges (e.g. insurers charging persons with pre-existing health conditions a higher insurance premium) or refusal to provide services (e.g. rejecting loan application from an individual with poor credit rating) will be considered "adverse effect". The PDPC generally considers prevailing social norms, including practices that a reasonable person would consider appropriate, when determining whether there is likely adverse effect to the individual.

2.31 As part of the assessment, organisations are also required to identify and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any adverse effect to the individual. In determining whether the measures implemented to eliminate or mitigate the likely adverse effects identified are appropriate, the PDPC adopts a commercially reasonable standard. Examples of reasonable measures and safeguards include minimising the amount of personal data collected, encrypting or immediate deletion of personal data after use, functional separation, access controls, and other technical or organisational measures that lower the risks of personal data being used in ways that may adversely impact the individual.

2.32 Where it is assessed that there are likely **residual adverse** effects to the individual after implementing the measures, **organisations will not be able to rely on deemed consent by notification** to collect, use or disclose personal data for the purpose. Whereas for the legitimate interests exception, organisations are required to conduct a balancing test as an additional step in the assessment to determine whether the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect on the individual. **Organisations may rely on the legitimate interests exception if the legitimate interests outweigh any likely residual adverse effect** to the individual.

2.33 **Joint assessments** may also be conducted by the disclosing and receiving organisations when relying on deemed consent by notification or legitimate interests exception to collect and disclose the personal data. In such cases, the assessment will factor in the considerations of the organisations involved. Alternatively, the disclosing and receiving organisations may conduct their assessments separately and provide their own justifications for the collection or disclosure of personal data for the identified purposes.

2.34 In determining the likely adverse effect on the individual, the organisation should consider the following:

a) ***The impact of the collection, use or disclosure of the personal data on the individual****:* Organisations are required to assess both the **severity and likelihood** of any adverse effect that may arise from the collection, use or disclosure of personal data. The assessment referred to in these Guidelines requires an assessment of **all reasonably foreseeable risks and adverse effect to the individual** resulting from the intended collection, use or disclosure. In general, the more severe the adverse effect of the collection, use or disclosure to the individual, the more unlikely the benefits of the collection, use or disclosure would outweigh the likely adverse effect. Please refer to paragraph 2.30 on adverse effect.

b) ***The nature and type of personal data and whether the individuals belong to a vulnerable segment of the population****:* In general, the potential adverse effect to individuals will be higher if the personal data is sensitive in nature. Organisations should also consider the individuals to whom the personal data relate, and whether they belong to a vulnerable group such as minors[15], individuals with physical or mental disabilities, or other special needs. The adverse effect may be more severe if the individuals belong to a vulnerable segment of the population.

c) ***The extent of the collection, use or disclosure of personal data and how the personal data will be processed and protected****:* Organisations should consider how extensive the collection, use or disclosure of an individual's personal data will be, and how the personal data will be collected, used or disclosed (e.g. whether collection is one-off or on a continuous basis). Organisations shall ensure that they do not collect, use or disclose more personal data than is reasonably necessary in order to achieve the purpose. For instance, collection of more types of data about an individual is likely to have a higher risk and adverse effect than collection of only specific types of personal data. How the personal data is protected, such as the implementation of access controls to prevent any unauthorised access, use or disclosure, may also affect the likelihood of adverse effect to the individuals.

d) ***Reasonableness[16] of the purpose of collection, use or disclosure of personal data****:* Organisations should ensure that the purpose of the collection, use and disclosure of personal data is proportionate and appropriate in the circumstances. In general, the context should be considered when assessing the reasonableness of purpose. For example, when using or disclosing personal data for a secondary purpose, organisations may wish to consider

[15] Refer to Chapter 7 of PDPC's Advisory Guidelines on the PDPA for Selected Topics.
[16] Refer to section 18 of the PDPA on Purpose Limitation Obligation.

the primary purpose and how the personal data was collected, and whether it affects the reasonableness of using or disclosing the personal data for the new purpose.

e) ***Whether the predictions or decisions that may arise from the collection, use or disclosure of the personal data are likely to cause physical harm, harassment, serious alarm or distress to the individual***: Where the collection, use or disclosure of personal data is to make predictions or decisions about individuals, organisations should also consider prevailing social norms and practices that a reasonable person would consider appropriate in determining if the decisions are likely to result in unfair discrimination, physical harm, harassment, alarm or distress to the individual.

2.35 Please refer to **Annex B** for the Assessment Checklist for Deemed Consent by Notification, and **Annex C** for the Assessment Checklist for Legitimate Interests Exception.

Business improvement exception

2.36 Part 5 of the new First Schedule and Division 2 under Part 2 of the new Second Schedule ("business improvement exception") enable organisations to use, without consent, personal data that they had collected in accordance with the DP Provisions of the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes[17]:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

2.37 In order to rely on the business improvement exception, organisations will need to ensure the following:

[17] "Relevant purposes" are defined in Paragraph 1(2) under Part 5 of the new First Schedule.

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and

b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

2.38 The business improvement exception also applies to the sharing of personal data (i.e. collection and disclosure) between entities belonging to a group of companies[18], without consent, for the following business improvement purposes:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of **existing or prospective customers** (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for **existing or prospective customers** (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

2.39 Business insights relating to individuals will be considered personal data if an individual can be identified from that data, including other information that the organisation has or is likely to have access (e.g. insights and predictions generated about a specific individual). The PDPC recognises that it may be necessary for organisations to share data regarding customer behaviour and preferences to improve products as part of the feedback loop in product development. In such cases, organisations may rely on the business improvement exception as the sharing of personal data is relevant to the eventual aim of improving, enhancing or developing new goods or services.

2.40 **"Existing customers"** refer to individuals who have a history of purchasing or hiring any goods or using any services provided by the organisation. "**Prospective customer"** generally refers to an individual who:

[18] "Group of companies" refers to related corporations within the meaning of the Companies Act (Cap. 50).

a) informs or has informed the organisation of his interest in its goods or services. The level of interest includes subscription to a mailing list and extends to requests for information concerning specific goods or services.

b) conducts or is conducting negotiations to purchase or hire or use any goods or use of services provided by the organisation. Negotiations can range from exploratory discussions to negotiations with a view to conclude an agreement.

2.41 Organisations relying on the business improvement exception to share personal data within the group will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without sharing the personal data in an individually identifiable form;

b) The organisations' sharing of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances; and

c) The organisations involved in the sharing are bound by any contract or other agreement or binding corporate rules requiring the recipient(s) of personal data to implement and maintain appropriate safeguards for the personal data.

2.42 Organisations cannot rely on the business improvement exception to send direct marketing messages[19]. In general, organisations must obtain express consent to send direct marketing messages to individuals. In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or facsimile, the organisation must comply with the DNC Provisions of the PDPA[20].

Example: Use of personal data to create credit risk model for operational efficiency

A bank intends to use personal data it has of its customers (i.e. income and transaction history with the bank) to create a credit risk model to reduce the time taken for it to assess and approve loan applications.

The bank assesses that it requires the use of data in individually identifiable form for this purpose, and that its use of personal data to create the credit risk model or loan application approvals is considered appropriate to a reasonable person.

[19] Refer to Paragraph 1(6) under Part 5 of the new First Schedule.
[20] Refer to PDPC's Advisory Guidelines on the Do Not Call Provisions.

The bank considers the use of credit risks models for loan application approvals to be a common industry practice.

The bank may rely on the business improvement exception to use personal data without consent to create a credit risk model to improve operational efficiency and service improvement (i.e. reduced time for loan applications).

Example: Use of personal data to understand spending habits and develop new credit services

A credit card company wants to use its customers' personal data (i.e. credit payment history) to derive insights on spending habits of its customers, to develop its new line of credit card and design new credit card reward schemes. The credit card company assesses that (a) it requires the use of data in individually identifiable form for the purpose; and (b) its use of personal data is considered appropriate to a reasonable person.

The credit card company may rely on the business improvement exception to use its customers' personal data without consent to understand its customers better and to develop new products and services.

Example: Use of personal data to train machine learning models

A wearables company intends to develop and provide a new functionality in its health tracking mobile application to provide its customers with timely reminders based on changes to individuals' vital signs. The company intends to use the personal data of its customers (i.e. heart rate, steps count) to train its machine learning model for the monitoring of vital signs and develop the new functionality.

The wearables company assesses that the use of anonymised data is enough for model training to develop and provide the new functionality. However, it assesses that the historical personal data of each customer is necessary when personalising the new product feature for that customer, and that its use of personal data for this purpose is considered appropriate to a reasonable person.

The wearables company may rely on the business improvement exception to use its customers' personal data without consent to improve or enhance its products or services and personalise services or goods for its customers.

Example: Sharing of personal data within a group of related corporations to learn or understand behaviour and preferences of prospective customers

A supermarket and a seafood restaurant belong to a group of companies. The supermarket intends to share the personal data of its customers (e.g. customers' shopping propensity) with the seafood restaurant so the seafood restaurant can learn and understand its prospective customers better (e.g. to offer dining privileges for seafood lovers).

In order to rely on the business improvement exception to share personal data with the seafood restaurant, the supermarket must ensure that the personal data discloses relates to individuals who are (i) the supermarket's customers and (ii) the seafood restaurant's customers or prospective customers. The supermarket should not disclose the shopping propensity of all its customers without first doing the check on overlaps of customers between itself and the seafood restaurant. In this case, the supermarket will only be sharing personal data of its customers who are also customers of the seafood restaurant or who signs up to receive the seafood restaurant's marketing information.

The supermarket should also ensure that the seafood restaurant is bound by an agreement (e.g. contract, binding corporate rules) that requires the seafood restaurant to implement and maintain appropriate safeguards for the personal data shared.

Example: Sharing of personal data to automate claim approvals to improve operational efficiency and develop new insurance products

A healthcare service provider and an insurance company belong to a group of companies. The insurance company intends to collect personal data from the healthcare service provider (i.e. medical records, payment information) to create an automated claim assessment system to improve the insurance company's efficiency and to develop new insurance products.

The healthcare service provider assesses that the sharing of individually identifiable data may not be necessary as the insurance company can use non-individually identifiable data (e.g. aggregated patient profile data) to develop an automated claim assessment system. Furthermore, the sharing of medical information for this purpose is unlikely to be considered appropriate to a reasonable person.

The healthcare service provider and the insurance company may not rely on the business improvement exception to share personal data without consent for this purpose.

Sending of direct marketing messages and preparatory activities to marketing

2.43 To be clear, organisations cannot rely on the new exceptions for legitimate interests or business improvement for the purpose of **sending direct marketing messages**.

2.44 Notwithstanding this, organisations may rely on the new business improvement exception to use existing customers' personal data for data analytics and market research to derive insights and understand their existing customers prior to their business marketing activities. The PDPC considers these to be **preparatory activities for marketing purposes** and are to be distinguished from the sending of direct marketing messages to individuals.

Research exception for the use and disclosure of personal data without consent

2.45 While the business improvement exception is intended to enable organisations to use personal data to improve their products, services, business operations and customer experience, the research exception is intended to enable organisations to conduct broader research and development that may not have any immediate application to their products, services, business operations or market. Commercial laboratories that carry out research for the development of science, institutes of higher learning that conduct research into the arts and social sciences, and organisations that carry out market research are examples of organisations that can continue to rely on the research exception. The research exception provides that organisations may **use** personal data for a research purpose, including historical and statistical research, subject to the following conditions:

a) The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

b) There is a clear public benefit to using the personal data for the research purpose;

c) The results of the research will not be used to make any decision that affects the individual; and

d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual.

2.46 Similarly, organisations may rely on the research exception to disclose personal data for a research purpose, including historical and statistical research. All the conditions for use of personal data for a research purpose are applicable together with the following **additional condition**:

a) It is impracticable for the organisation to seek the consent of the individual for the disclosure.

2.47 When assessing whether it would be "impracticable" for the organisation to seek consent of the individual, the specific facts of the case will have to be considered. Factors that the PDPC considers relevant in assessing whether it is "impracticable"

to seek consent may include, but are not limited to:

a) Organisation does not have current contact information of the potential research subject or sufficient information to seek up-to-date contact information. The organisation should be able to demonstrate that the potential research subject cannot be reached using the contact information, such as by attempting to contact the potential research subject.

b) Given the target population required for meaningful conclusions to be drawn from the research, the quantum of the research grant and the period allotted for the research, the costs of attempting to seek consent from each potential research subject would impose disproportionate resource demands and burden on the organisation or take up so much time that carrying out the research is no longer viable. In this regard, there is no fixed number of subjects that would be determined as "impracticable" to seek consent from. Such an assessment would be based on all relevant circumstances of the case, which may include the nature and extent of the personal data required, whether or not there is an existing relationship with the individuals, and other factors affecting the difficulty of contacting the required research subjects.

c) Exceptional circumstances where seeking the research subject's consent would affect the validity or defeat the purposes of the research, in particular, where seeking consent would skew the research or introduce bias into the research such that no meaningful conclusions can be drawn. Organisations should nevertheless consider whether it is possible to seek consent in a manner that would not introduce such bias.

2.48 The PDPC considers the degree of practicability. Mere inconvenience, such as to the organisation or the potential research subject, would not amount to "impracticability". Organisations relying on this exception have to demonstrate that the additional costs or time delays resulting from having to contact individuals for consent is so onerous such that the research is no longer viable. Organisations may use convenient and practical means for individuals to provide consent, for instance through an online form or replying to a letter, email, text message or recording of voice call, instead of requiring the individual to make a trip to the organisation for the purpose of giving consent.

3 Mandatory Data Breach Notification

3.1 Part VIA of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC where it is assessed to be notifiable. Data intermediaries (DIs) that process the personal data on behalf and for the purposes of another organisation (including a public agency) are also required to notify that other organisation or public agency of a data breach detected. This obligation is referred to as the data breach notification obligation (DBN Obligation) in these Guidelines.

Duty to conduct assessment of data breach

3.2 Once an organisation has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its DI), the organisation is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA.

3.3 Assessments should be done expeditiously as the likelihood of significant harm to affected individuals may increase with time. Any unreasonable delay in assessing a data breach will be a breach of the DBN Obligation and the PDPC can take enforcement action.

3.4 While there may be varying circumstances that would affect the time taken to establish the facts of a data breach and determine whether it is notifiable, organisations should generally do so within 30 calendar days. If an organisation is unable to complete its assessment within 30 days, it would be prudent for the organisation to be prepared to provide the PDPC an explanation for the time taken to carry out the assessment.

3.5 To demonstrate that it has taken reasonable and expeditious steps to assess whether the data breach is notifiable, the organisation must document all steps taken in assessing the data breach[21]. Please refer to paragraphs 3.36 – 3.38 on the information to be provided in notifications.

Data breaches within an organisation

3.6 A data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data within an organisation is not a notifiable data breach. For example, where the HR department of an organisation mistakenly sends an email attachment containing personal data to another department within

[21] The organisation may be required to produce supporting documentation on the steps taken for its assessment of the data breach as part of its notification to the PDPC, or for any investigation by the PDPC of a suspected breach.

the same organisation that is not authorised to receive it, and the data breach is contained within the organisation, the data breach is not subject to the DBN Obligation.

> **Example: Misplaced storage drive**
>
> Sarah, a HR executive, misplaces an organisation-issued storage device containing the personal data and work evaluation reports of her company's staff and interns in her company's premises.
>
> After a few days, the misplaced storage drive is found in her company's premises by another staff, Rachel. Sarah's company confirms that Rachel immediately returned the storage drive to the HR department upon finding it, and that no one accessed the storage drive while it was misplaced.
>
> In this case, the DBN Obligation would not apply as it occurred within the organisation.

Data breaches discovered by a DI

3.7 Where a data breach is discovered by a DI that is processing personal data on behalf and for the purposes of another organisation or public agency, the DI is required to notify the organisation or public agency without undue delay from the time it has credible grounds to believe that the data breach has occurred[22]. This ensures the organisation is (i) informed of data breaches in a timely way; (ii) able to decide on the immediate actions to take to contain the data breach; and (iii) assess whether the data breach is a notifiable data breach.

3.8 The DBN Obligation does not impose a requirement on the DI to assess whether the data breach is notifiable, or to notify affected individuals and/or the PDPC. The organisation that engaged the DI remains responsible for doing so, even if it enlists the help of a DI to conduct the assessment of the data breach or to notify the affected individuals and/or the PDPC on its behalf.

3.9 As a good practice, organisations should establish clear procedures for complying with the DBN Obligation when entering into service agreements or contractual arrangements with their DIs, having regard to factors such as the volume and types of personal data involved, the type and extent of data processing, and the potential

[22] A DI processing personal data on behalf of and for the purposes of a public agency must also notify the public agency of the occurrence of the data breach without undue delay if the DI has reason to believe that a data breach has occurred in relation to that personal data.

harm that may result from a data breach[23].

Data breaches involving more than one organisation

3.10 In situations where a data breach involves personal data in the possession or under the control of more than one organisation, the organisations involved are individually responsible for complying with the DBN Obligation in respect of that data breach.

3.11 Organisations may agree that one of the organisations takes the lead in conducting the assessment to determine whether the breach is notifiable. Organisations have to draw its own conclusion from the assessment, and should accurately document and record the agreements, breach assessments and decisions.

3.12 Where a data breach is notifiable to the PDPC, each organisation has to notify the PDPC. As a matter of administrative convenience, organisations may use the same information where relevant to individually submit the notification. Where the data breach is notifiable to affected individuals, the PDPC may provide further guidance to the organisations involved on managing the notification to affected individuals so that affected individuals only receive notifications and updates from a single source in respect of the notifiable data breach to minimise confusion.

Example: Data breach involving multiple organisations

As part of a business partnership, retailers ABC, DEF, and GHI establish a joint membership scheme where consumers can join as members to receive retail benefits.

A data breach involving the unauthorised disclosure of individuals' personal data and financial information is discovered when a member alerts ABC that she received an email containing the personal data of another member that was sent to her erroneously. The email contains the other member's purchasing history and the credit card details used for the payment of each purchase.

ABC obtains the agreement of all the organisations involved to take the lead in conducting the assessment of the data breach and share its findings and assessments with the rest. ABC determines that the data breach is notifiable. DEF and GHI come to their own conclusions and agree with ABC's assessment. The agreement, assessment and conclusions are documented and recorded by all the organisations involved.

ABC, DEF and GHI notify the PDPC of the data breach in compliance with the DBN Obligation by each submitting a DBN through the breach notification portal,

[23] The contractual clauses may include requirements around the communication of data incidents, processes for confirming a data breach, and responsibility for containing and remediating a data breach, where relevant.

and attaching a common notification template to be used for the notification of the affected members.

The organisations, in consultation with the PDPC, agree that ABC is best positioned to notify the affected members and provide further updates (if any), as it is the organisation with the closest and most direct relationship with the members.

Criteria for data breach notification

Significant harm to affected individuals

3.13 Organisations are required to assess whether a data breach is notifiable as it is likely to result in significant harm[24] to the affected individuals. Given the likelihood of harm arising from a data breach, notification ensures affected individuals are aware and able to take steps to protect themselves (e.g. change password, cancel credit card, monitor account for unusual activities).

3.14 To provide certainty to organisations on the data breaches that are notifiable, the PDPC will prescribe in Regulations, the personal data (or classes of personal data) that is considered likely to result in significant harm to affected individuals if compromised in a data breach. Where a data breach involves any of the prescribed personal data, the organisation will be required to notify the affected individuals and the PDPC of the data breach.

3.15 The personal data (or classes of personal data) to be prescribed include:

a) Individual's **full name**[25] or **full national identification number**[26] in combination with any of the following personal data:

(i) **Financial information which is not publicly disclosed**. Examples include salary/remuneration, loan/credit history, financial account number, bank account, credit/debit card numbers, credit report, net worth bankruptcy status, source of wealth, which is not publicly disclosed.

(ii) **Life/health insurance information which is not publicly disclosed**. This

[24] Significant harm could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms of harms that a reasonable person would identify as a possible outcome of a data breach.

[25] Full name refers to the name used to identify an individual and must include the individual's first and last name, whether from official sources (e.g. NRIC/passport) or provided to/used by the organisation. It does not apply to the individual's initials.

[26] National identification number includes NRIC number, birth certificate number, FIN, work permit number, passport number, and any foreign national identification number.

refers to any health insurance information of an individual or any claims information relating to the individual, including claims appeals, which is not publicly disclosed.

(iii) **Specified medical information**. This refers to any assessment, diagnosis, treatment, prevention or alleviation **by a medical professional** of an ailment, condition, disability, disease or disorder or an injury affecting any part of the human body or mind), that concerns any of the following: sexually-transmitted diseases, fertility information (e.g. IVF), organ donation, abortion information, substance abuse, addiction, biological parenthood (e.g. sperm donor, sperm recipient), suicide, domestic and child abuse, or sexual abuse).

(iv) **Information leading to identification of a vulnerable adult, child or young person who is the subject of an investigation or relating to court proceedings involving a child and young person** (including information on places of temporary care and protection or places of safety)[27].

(v) **Private key**[28] **used to authenticate or sign an electronic record or transaction**.

b) Individual's **account information**[29] in combination with any required biometric data, security code, access code, password or answer to security question **used to permit access to or use of the account**, where the account can be subsequently misused for fraudulent transactions or to access any information in paragraph 3.15(a).

Example: Unauthorised access of patients' medical records

The database administrator of a medical clinic discovers an unauthorised access of some of its patients' medical records. The medical clinic immediately assesses the data breach, including the number of patients' records and the types of data affected. The medical clinic determines that the data breach involves medical records including personal data such as patients' NRIC numbers and other

[27] Examples include court-related documents or information (e.g. statement of facts/charge sheets), court orders (e.g. care and protection orders, Family Guidance orders, probation orders, Juvenile Rehabilitation Centre orders, orders in relation to vulnerable adults), family violence/child abuse history, details of incidents, family circumstances or conflicts.

[28] A private key is usually a series of alphanumeric characters used to generate a digital signature in processing a transaction, which confirms that the transaction comes from a specific user.

[29] Account information includes user account ID or username, bank account number, credit or debit card number.

national identification numbers, residential addresses, allergies and medical histories. The medical records of approximately 50 patients are affected.

The data breach is assessed to be notifiable as it involves individuals' national identification numbers and medical information, and these are deemed to likely result in significant harm to the affected individuals. The medical clinic is required to notify the PDPC and the affected individuals of the data breach.

Example: Theft of portable storage drive containing hotel guests' details

A portable storage drive containing the details of approximately 1,000 guests of a hotel chain is stolen. The drive includes personal data of guests such as their full names, passport details, flight information, durations of stay with the hotel chain, and credit card details.

The data breach is assessed to be notifiable as it involves guests' national identification numbers and credit card details, and these are deemed to likely result in significant harm to the affected individuals. The hotel chain must notify the PDPC and the affected individuals of the data breach.

Significant scale of breach

3.16 Data breaches of a significant scale may indicate a systemic issue within the organisation. Notifying the PDPC of such data breaches will allow it to provide guidance to organisations on remedial actions to address the data breach as well as any systemic changes to prevent future occurrences.

3.17 Data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Where a data breach affects 500 or more individuals, the organisation is required to notify the PDPC, even if the data breach does not involve any prescribed personal data in paragraph 3.15.

3.18 If an organisation is unable to determine the actual number of affected individuals in a data breach, the organisation should notify the PDPC when it has reason to believe that the number of affected individuals is at least 500. This may be based on the estimated number from a preliminary assessment of the data breach. The organisation may subsequently update the PDPC of the actual number of affected individuals when it is established.

Example: Unauthorised access to database containing customers' profiles

The IT administrator of online retail store discovers an unauthorised access to its customers' database. The database contained customers' names, membership numbers, contact information and their current balance of loyalty points and dates of their expiry.

The online retail store is unable to determine the exact number of individuals whose personal data is affected in the data breach at the outset. Nevertheless, as the affected database contains the personal data of 700 customers, the online retail store proceeds to notify the PDPC of the data breach. Subsequently, the online retail store determines the exact number of customers whose personal data is compromised and provides the updated information to the PDPC.

As the data breach does not involve any of the prescribed personal data, the data breach is deemed to be unlikely to result in significant harm to an individual and the online retail store would not be required under the DBN Obligation to notify the affected customers of the data breach.

Example: Disclosure of 250 students' library loan history

A private education institution discovers an unauthorised disclosure of its students' library loan records. The data breach involves the personal data of 250 students, including their full names, student matriculation numbers and library loan histories for the past one year.

As the data breach does not involve any of the prescribed personal data, the data breach is deemed to be unlikely to result in significant harm to an individual and the private education institution need not notify the affected students of the data breach. In addition, as the scale of the data breach is not significant (i.e. fewer than 500 affected students), the private education institution need not notify the PDPC of the data breach.

Example: Loss of document containing personal data of 10 cyclists

A member of cycling interest group misplaced a document containing the cycling route of a previous cycling expedition and names of the 10 cyclists involved in the expedition.

As the data breach does not involve any of the prescribed personal data, and the data breach is not of a significant scale (i.e. fewer than 500 affected individuals), the cycling interest group need not notify the affected cyclists nor

the PDPC of the data breach.

Timeframes for notification

3.19 Upon determining that a data breach is notifiable, the organisation must notify:

a) the PDPC as soon as practicable, but in any case, no later than three (3) calendar days[30]; and

b) where required, affected individuals as soon as practicable, at the same time or after notifying the PDPC.

3.20 These timeframes for notifying the PDPC and/or the affected individuals commences from the time the organisation determines that the data breach is notifiable. Any unreasonable delays in notifying the relevant parties will be a breach of the DBN Obligation.

3.21 Prescribing a cap of three (3) calendar days provides clarity for organisations as to the definitive time by which they will have to notify the PDPC by.

3.22 Where an organisation is required to notify affected individuals of a data breach, it should notify the affected individuals at the same time or after it notifies the PDPC.

Exceptions from the requirement to notify affected individuals

3.23 The new section 26D of the PDPA provides for exceptions to the requirement to notify affected individuals of a notifiable data breach in certain circumstances.

3.24 **Where an exception applies** to a data breach that is likely to have significant harm to the affected individuals (e.g. as instructed by a prescribed law enforcement agency), the organisation need not notify the affected individuals, but it is still required to notify the PDPC of the data breach. In the event that the PDPC determines that the exception does not apply, the organisation would be required to notify the affected individuals of the data breach.

Remedial action

3.25 An organisation may rely on the remedial action exception if timely remedial actions have been taken by the organisation or its DI, in accordance with any prescribed requirements, that renders it unlikely that the data breach will result in significant

[30] The first day of the three days starts on the day after the organisation makes the determination that there is a notifiable breach. To illustrate, if an organisation determines on 1st January that a data breach is notifiable, it must notify PDPC by 4th January.

harm to the affected individual.

3.26 Such remedial actions need not necessarily be taken before notifying the PDPC. Remedial actions (or further remedial actions) may also be taken after notifying the PDPC and receiving guidance from the PDPC. In the event that, after notifying the PDPC, the organisation applies further remedial actions such that the data breach is no longer likely to have significant harm to the individuals, the organisation may rely on the exception not to notify the individuals concerned.

Example: Disclosure of an email attachment containing the personal data of 1,000 customers

A travel agency has a panel of vendors that processes its payments. An email attachment containing the personal data of 1,000 customers of the travel agency is sent to the wrong vendor by accident. The attachment includes full names, credit card details and passport numbers.

The employee who sent the email immediately contacts the receiving vendor, which confirms that the attachment has not been accessed and that it has permanently deleted the email with the attachment.

The travel agency assesses that it may rely on the remedial action exception as it has taken reasonable measures to address the data breach such that it is not likely to result in significant harm to the affected individuals.

However, the travel agency is still required to notify the PDPC of the data breach according to the requirements under the DBN Obligation as the data breach involves more than 500 individuals, including their financial information and national identification numbers.

Technological protection

3.27 Where there are appropriate technological measures applied to the personal data (e.g. encryption, password-protection, etc) before the data breach which renders the personal data inaccessible or unintelligible to an unauthorised party, the exception for technological protection applies. In such cases, the organisation need not notify the affected individuals of the data breach.

3.28 In assessing whether the technological protection measures taken are sufficient for the technological protection exception to apply, organisations should take into consideration whether the technological protection is of a commercially reasonable standard and the prevailing industry practices in the sector. Organisations can also consider the availability and affordability of the options in determining what are reasonable technological protection measures.

Example: Loss of encrypted storage drive

A HR director misplaces an encrypted storage drive containing 200 employees' medical insurance details of his company such as employees' full names, medical schemes, past medical claims, and remaining claims balance.

The HR director's company assesses that the technological protection exception applies, as the encryption standard (AES 256-bit) in the storage drive is of a reasonable standard when the loss occurred and that any unauthorised access to the encrypted data of the misplaced storage drive is unlikely. As such, the company need not notify the affected employees of the data breach.

However, as the personal data involved includes employees' financial and health information, the company must notify the PDPC of the data breach.

Example: Loss of laptop containing health information

Pharmaceutical research laboratory maintains a list of patients with a rare communicable disease. The list contains personal data of 1,000 patients, including their full names, medical histories and treatment details. Only researchers who deal with these patients are given access to the list. The list is stored in the pharmaceutical research laboratory's intranet and can also be accessed with the correct credentials through authorised laptops. There are three layers of security measures put in place for accessing these laptops - (i) BIOS password; (ii) BitLocker; and (iii) Windows password. One of their researchers loses his authorised laptop.

The pharmaceutical research laboratory assesses that the technological protection exception applies, as it is unlikely that a third party could overcome the three layers of protection measures put in place to access the list via the lost laptop. In addition, the credentials of the researcher are not stored on the laptop.

However, as the personal data involved includes individuals' health information, and the number of potentially affected individuals is more than 500, the pharmaceutical research laboratory must notify the PDPC of the data breach.

Notification allows the PDPC to assess whether there is any systemic issue within the organisation, for example, lapse in security arrangements leading to higher risk of similar incidents occurring. PDPC can advise the organisation on taking preventive measures to lower the risk of similar incidents.

Prohibition and waiver of the requirement to notify affected individuals

3.29 Organisations are prohibited from notifying the affected individuals if a prescribed

law enforcement agency so instructs them. This is to cater to situations where the breach is the subject of an ongoing or potential investigation by a law enforcement agency and notifying the affected individuals will compromise investigations or prejudice enforcement efforts under the law. Organisations are also prohibited from notifying the affected individuals if the PDPC so directs them.

3.30 In addition, the PDPC may, on the written application of an organisation, waive the requirement for an organisation to notify affected individuals in exceptional circumstances where notification to affected individuals may not be desirable. This includes circumstances where there are overriding national security or national interests, or there are ongoing investigations by an agency authorised by law[31] where such investigations are not publicly known.

3.31 In deciding whether to grant a waiver, the PDPC will have regard to advice from the relevant law enforcement agency or public agency. For instance, a law enforcement agency may prohibit an organisation from notifying affected individuals for a period of time to avoid compromising an investigation. A law enforcement agency may also delay an organisation's notification if the notification would likely lead to further data breaches, should vulnerabilities in an organisation's IT security system become publicly known before it could be rectified.

Mode of notification of data breach

3.32 Where organisations are required to notify affected individuals of a data breach, they should ensure that the mode of notification used is appropriate and effective in reaching the affected individuals in a timely way. Organisations may employ their regular mode of communication with the affected individuals to send the notification.

3.33 Where there is no regular mode of communication with the affected individuals, the organisation should determine the most appropriate mode of notification to reach out to the affected individuals. As there are many different modes of notification that could evolve with technology, organisations may determine the most efficient and effective mode of notification to inform affected individuals.

Example: Disposal of client's personal data

An employee of a voluntary welfare organisation discovers that case documents containing their ex-clients' financial, medical and family history are disposed of in an unsecured manner instead of being shredded as per the voluntary welfare organisation's data retention policy. However, the voluntary welfare organisation is not able to ascertain the scale of the data breach as the

[31] Including investigations conducted by an organisation to discharge obligations under the law.

documents were sold to a 'rag-and-bone' man.

The data breach is assessed to pose a significant harm to the affected individuals, as financial and health records are compromised. As such, the voluntary welfare organisation should notify the PDPC and the affected individuals of the data breach.

The voluntary welfare organisation should also assess the mode and manner of notifying the affected individuals that would best serve the interest of the affected individuals. As the affected individuals could be significantly distressed given the sensitivity of the personal data breached, the voluntary welfare organisation decides to notify the affected individuals through personal phone calls by trained personnel to address any immediate questions and allay their concerns.

Information to be provided in notification of data breach

3.34 An organisation notifying affected individuals and/or the PDPC of a notifiable data breach is required to provide relevant details of the data breach to the best of its knowledge and belief. The notification should also include relevant information about the organisation's data breach management and remediation plans. Information to be provided in the organisation's notifications will be prescribed in the Regulations.

Notification to the PDPC

3.35 To ensure proactive steps are taken by the organisation to manage and remediate the data breach, information to be provided in the organisation's notification to the PDPC shall include:

a) **Facts of the data breach**

(i) Summary of the facts relating to the data breach that the organisation has managed to establish thus far, on a best effort basis;
(ii) Approximate number of individuals and type(s) of personal data affected by the data breach; and
(iii) If not intending to notify affected individuals, brief justification for the organisation's reliance on any applicable exception(s).

b) **Data breach handling**

(i) Chronology of how the organisation (or its DI, where applicable) first became aware of the data incident (i.e. suspected data breach);
(ii) Where the data breach notification to the PDPC is not made within three (3) calendar days of ascertaining that it is a notifiable breach,

reasons for the delay in notification to the PDPC and any supporting evidence; and

(iii) Organisation's plan to manage the data breach incident (e.g. data breach management plan, remediation plan, communications plan).

c) **Contact details**

(i) Contact details of person(s) whom the PDPA may contact for further information or clarification.

Notification to affected individuals

3.36 Notification to affected individuals should be clear and easily understood. It should include guidance on the steps affected individuals may take to protect themselves from the potential harm arising from the data breach. Where appropriate, organisations should notify parents or guardians of young children whose personal data has been compromised.

3.37 Organisations are not required to provide to the PDPC the notification to be sent to affected individuals. Organisations should include the following information in their notifications to affected individuals:

a) **Facts of the data breach**

(i) How and when the data breach occurred; and
(ii) Type(s) of personal data involved.

b) **Data breach management and remediation plan**

(i) What the organisation has done or will be doing in response to the risks brought about by the data breach;
(ii) Potential harm the individual may suffer arising from the data breach; and
(iii) Steps that the individual may take to prevent any potential misuse of his or her personal data or to reduce the significant harm arising from the data breach.

c) **Contact details**

(ii) Contact details of the organisation's representative whom the affected individual can contact for further information or assistance.

3.38 Organisations may customise their notification to affected individuals, as long as it includes the required content. In addition, decision on the appropriate actions that the individual may take is dependent on the circumstances of the data breach. This may include choosing to tailor the recommended protective actions that individuals could take depending on the individual's circumstances or providing general

recommendations that apply to all affected individuals.

Notification to other regulators

3.39 Where an organisation is required to notify a sectoral regulator or law enforcement agency of a data breach under other written laws, the organisation must notify that sectoral regulator or law enforcement agency accordingly. Additionally, it must also notify the PDPC and affected individuals (if required) according to the timeframes for data breach notification under the PDPA. An organisation is not regarded to have fulfilled the DBN Obligation under the PDPA just by fulfilling any other breach notification requirements set out under other written laws.

4 Financial Penalties

4.1 The new section 48J provides that the PDPC may impose up to S$1 million on organisations for a breach of the DP Provisions. For a breach of the DNC Provisions, PDPC may impose up to S$200,000 in the case of an individual and up to S$1 million where it is an organisation. At least one year after the PDPA amendments come into force, subject to Ministerial review, section 48J of the PDPA provides that the PDPC may impose a financial penalty of up to S$1 million or 10% of the organisation's annual turnover in Singapore[32], whichever is higher, for a breach of the DP Provisions[33]. For a breach of the prohibitions on the use of dictionary attacks and address-harvesting software under the new section 48B(1), the PDPC may impose a financial penalty of up to S$200,000 in the case of an individual; and where it is an organisation, up to S$1 million or 5% of the organisation's annual turnover in Singapore[34], whichever is higher. For a breach of the other DNC Provisions, the financial penalty cap will remain the same at up to $200,000 in the case of an individual and up to S$1 million where it is an organisation. The higher end of financial penalties applies to egregious cases and provides the PDPC with more flexibility in meting out financial penalties based on the circumstances and seriousness of the breach.

4.2 In determining the amount of financial penalty to be imposed, the PDPC will take into account factors set out in the PDPA. Some of these factors have been taken into consideration by the PDPC in determining financial penalty amounts in past enforcement cases. The non-exhaustive list of factors set out in the PDPA provides greater transparency as to how the PDPC makes a determination of the quantum of financial penalties to impose.

4.3 Organisations may wish to refer to past Commission Decisions[35] where the PDPC had taken these factors into account in determining the financial penalty. The list of factors and examples of past cases are provided in Table 1 below.

Table 1: Factors and examples of past enforcement cases

S/N	Factors	Past enforcement cases
a)	the nature, gravity and duration of the non-compliance by the	***Institute of Singapore Chartered Accountants [2018] SGPDPC 28*** – The fact that the unauthorised disclosure was limited to a single

[32] Where the organisation's annual turnover in Singapore exceeds $10 million.
[33] For contravention of any provision in Part III, IV, V, VI, VIA or VIB.
[34] Where the organisation's annual turnover in Singapore exceeds $20 million.
[35] Commission's Decisions can be found at https://www.pdpc.gov.sg/Commissions-Decisions.

S/N	Factors	Past enforcement cases
	organisation or person, as the case may be	unintended recipient for a short period of 10 minutes was taken as a mitigating factor in the financial penalty calibration (see paragraph 22 of the Grounds of Decision). ***Ninja Logistics Pte Ltd [2019] SGPDPC 39*** – The fact that the organisation was cognisant of the risks of unauthorised access and disclosure to the exposed personal data through the tracking function page, but failed to resolve the issue for more than 2 years, was taken as an aggravating factor (see paragraph 18 of the Grounds of Decision). ***SPH Magazines Pte Ltd [2020] SGPDPC 3*** – The facts that the compromised password had not been changed for a long period of 10 years and the organisation was unable to detect the unauthorised access of personal data for about 2 years, were taken as aggravating factors (see paragraph 13 of the Grounds of Decision).
b)	the type and nature of the personal data affected by the non-compliance by the organisation or person, as the case may be	***Aviva Ltd [2018] SGPDPC 4*** – The disclosure of sensitive personal data, in particular medical condition and sum assured, was treated as an aggravating factor (see paragraph 30 of the Grounds of Decision). ***Singapore Health Services Pte. Ltd. and Integrated Health Information Systems Pte. Ltd. [2019] SGPDPC 3*** – The financial penalty imposed on each of the two organisations took into account the high number of individuals affected and high sensitivity of the personal data exfiltrated (see paragraph 139 of the Grounds of Decision). ***Option Gift Pte Ltd [2019] SGPDPC 10*** – The organisation was found in breach for the unintended disclosure of up to 426 individuals' personal data due to a coding error in its system. The disclosed personal data comprised login identifications, email addresses, delivery addresses and mobile numbers. The Commission considered, among other things, the number and type of personal data compromised, and

S/N	Factors	Past enforcement cases
		imposed a lower financial penalty (see paragraph 9 of the Grounds of Decision).
c)	whether the organisation or person (as the case may be), as a result of the non-compliance, gained any financial benefit or avoided any financial loss	***Sharon Assya Qadriyah Tang [2018] SGPDPC 1*** – The profiteering from the sale of personal data was taken to be an aggravating factor in calibrating the financial penalty (see paragraph 32 of the Grounds of Decision). ***Amicus Solutions Pte. Ltd. and Ivan Chua Lye Kiat [2019] SGPDPC 33*** – Profiteering from the sale of personal data was treated as aggravating in calibrating the financial penalty (see paragraphs 52 and 53 of the Grounds of Decision).
d)	whether the organisation or person (as the case may be) took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action	***Zero1 Pte. Ltd. and XDEL Singapore Pte. Ltd. [2019] SGPDPC 37*** – Quick remedial action by XDEL Singapore Pte. Ltd. to rectify the code checking function on the notification webpage system was treated as a mitigating factor in calibrating the financial penalty (see paragraph 26 of the Grounds of Decision). ***Singapore Telecommunications Limited [2019] SGPDPC 49*** – Prompt action taken to mitigate the impact of the breach by implementing a temporary fix within 11 hours, was taken as a mitigating factor (see paragraph 14 of the Grounds of Decision).
e)	whether the organisation or person (as the case may be) had, despite the non-compliance, implemented adequate and appropriate measures for compliance with the requirements under this Act	***Propnex Realty Pte Ltd [2017] SGPDPC 1*** – The facts that the organisation had in place a data protection policy which was made known to its agents and staff, and that its in-house compliance team (with assistance from external consultants) had been conducting annual internal audits to assess system access risk, data integrity risk and risk of configuration issues in the production environment were considered in calibrating the financial penalty (see paragraph 32 of the Grounds of Decision).

S/N	Factors	Past enforcement cases
		ComGateway (S) Pte. Ltd. [2017] SGPDPC 19 – The fact that the organisation had been conducting regular penetration tests, vulnerability tests and code reviews to guard against online security threats was considered in calibrating the financial penalty (see paragraph 37 of the Grounds of Decision).
f)	whether the organisation or person (as the case may be) had previously failed to comply with this Act	***Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd [2016] SGPDPC 15*** – Financial penalty against Toh-Shi Printing Singapore Pte Ltd took into account the fact that this was the second time within about a year that a breach of the same case fact pattern had occurred (see paragraph 38 of the Grounds of Decision). ***Aviva Ltd [2018] SGPDPC 4*** – The fact that the organisation had encountered a similar incident previously was treated as an aggravating factor (see paragraph 30 of the Grounds of Decision).
g)	the compliance of the organisation or person (as the case may be) with any direction given under section 48I or 48L(4) in relation to remedying or mitigating the effect of the non-compliance	This factor has not arisen in past cases. The PDPC may consider the fact that an organisation did not comply with a previous direction for the incident as an aggravating factor in the financial penalty calibration for the incident.
h)	whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with this Act	***Singapore Health Services Pte. Ltd. and Integrated Health Information Systems Pte. Ltd. [2019] SGPDPC 3*** – The Commission decided to impose the highest and second highest financial penalties against Integrated Health Information Systems Pte. Ltd. and Singapore Health Services Pte. Ltd. respectively in recognition of the severity and extent of the data breach and the serious lapses (see paragraph 138 of the Grounds of Decision). ***Amicus Solutions Pte. Ltd. and Ivan Chua Lye Kiat [2019] SGPDPC 33*** – In calibrating the financial penalty, the Commission took a hard

S/N	Factors	Past enforcement cases
		stance against the unauthorised sale of personal data. In its decision, the Commission emphasised that profiting from sale of personal data by organisations without consent of individuals was the kind of activity which the PDPA sought to curb and would be dealt with severely. The Commission further warned that any profits from the unauthorised sale of personal data may be taken into account in calculating the financial penalty to be imposed (see paragraphs 54 and 55 of the Grounds of Decision).
i)	the likely impact of the imposition of the financial penalty on the organisation or person (as the case may be), including the ability of the organisation or person to continue the usual activities of the organisation or person	***O2 Advertising Pte. Ltd. [2019] SGPDPC 32*** – The Commission reduced the financial penalty amount after considering the organisation's representation of its dire financial circumstances (i.e. massive loss due to fraud involving S$3.2mil, elderly 72-year-old sole owner who intended to continue the business on a significantly reduced scale) (see paragraphs 12 and 13 of the Grounds of Decision). ***Advance Home Tutors [2019] SGPDPC 35*** – The Commission reduced the financial penalty amount to avoid imposing a crushing burden on the organisation, following its representation that it was a small home business which did not generate much revenue (see paragraphs 27 and 30 of the Grounds of Decision).
j)	any other matter that may be relevant	***Aviva Ltd [2018] SGPDPC 4*** – The fact that the organisation was in the business of handling large volumes of personal data, the disclosure of which may cause exceptional damage, injury or hardship to affected individuals was taken as aggravating (see paragraph 30 of the Grounds of Decision). ***DS Human Resource Pte. Ltd. [2019] SGPDPC 16*** – Despite the organisation's representation of its efforts to automate its business processes in response to the Government's push for small and medium enterprises (SMEs) to go digital, the Commission decided to maintain the financial penalty. This was to convey the message that

S/N	Factors	Past enforcement cases
		good data management and protection practices need to be adopted from the onset of the digitalisation process even for SMEs, and these can be proportionate without being too costly (see paragraph 14 of the Grounds of Decision). ***Creative Technology Ltd [2020] SGPDPC 1*** – The Commission considered as a mitigating factor the organisation's effort of going through its email logs to determine the number of affected user emails which contained either names or partial names, even though it had deleted the database (see paragraph 13 of the Grounds of Decision).

5 Offences for Egregious Mishandling of Personal Data

5.1 New offences will be introduced under Part IXB of the PDPA to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation (including a public agency). The offences are for:

a) Knowing or reckless unauthorised disclosure of personal data;

b) Knowing or reckless unauthorised use of personal data for a gain or to cause a harm or loss to another person; and

c) Knowing or reckless unauthorised re-identification of anonymised data.

5.2 The introduction of these offences does not detract from the policy position to hold organisations primarily accountable for data protection. Organisations remain liable for the actions of their employees in the course of their employment with the organisations[36]. The new offences are to criminalise egregious misconduct by individuals whose actions had not been authorised by the organisation. To be clear, circumstances where the conduct is in the nature of a private dispute are not intended to be the subject of criminal prosecutions under these offences. Examples of private disputes include, disputes over ex-employees taking an organisation's customer list when joining a competitor or setting up a competing business, where the ex-employee obtained the consent of the customers to do so.

Authorisation

5.3 The new offences are not intended to cover instances where the individuals are authorised to disclose, use or re-identify the data. Authorisation may take different forms: it may be found in an organisation's written polices, manuals and handbooks, or an organisation may provide ad-hoc authorisation for a specific action or activity (which could be verbal or in writing). Authorisation should be provided by someone in the organisation who is empowered to do so or who is ostensibly empowered to do so by reason of his seniority or position in the organisation. Below are instances where individuals are considered to be acting under authorisation:

a) **Employees** acting in the course of their employment (including volunteers), in accordance with their employers' policies and practices, or whose actions are authorised by their employers. Employees should be assured that if they adhere to their employer's policies and practices, they will not run the risk of criminal sanctions for these offences.

[36] Refer to section 53 of the PDPA.

b) **Service providers** engaged and authorised by organisations through service contracts or written agreements to carry out the disclosure, use or re-identification of data.

Applicable defences

5.4 The PDPA provides for the following defences for the new offences:

a) **The information is publicly available and where that information was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case.** This defence is intended to only cover personal data that is already in the public domain. For example, a dataset contains identity information (e.g. name, photo, email address) and other personal data (e.g. financial data). An individual will not be able to rely on this defence where the affected person's *identity information* is publicly available (e.g. on social media) but where other *re-identified personal data* of the affected person in the dataset is not publicly available;

b) **Where the conduct is permitted or required under other laws**;

c) **Where the conduct is authorised or required by an order of the court**; and

d) **Where the individual reasonably believes that he had the legal right to do so**. This defence covers situations where consent has been provided by the individual to whom the personal data relates, for example, a relationship manager who obtains consent from his clients to continue to use and disclose their personal data when he moves to another company. In other similar situations, for example a professional who brought in his clients when he joined a partnership and brings them along when he moves to another partnership; or an account manager who brings the customers he had worked with from his previous company to his new employment where he has obtained the customers' consent to do so, while there may be a dispute over whether the relationship manager, professional or account manager has the legal right to do so, the dispute is in the nature of a private civil dispute and it is not an a criminal offence. This defence is also intended to cover journalistic reporting and whistleblowing.

Re-identification of anonymised data

5.5 For the offence outlined in paragraph 5.1(c) of knowing or reckless unauthorised re-identification of anonymised data, additional defences are provided for the following circumstances:

a) **Testing the effectiveness of the anonymisation of personal data in the possession or under the control of an organisation or public agency, as the case may be**;

b) **Testing the integrity and confidentiality of anonymised information in the possession or under the control of an organisation or public agency**; and

c) **Assessing, testing or evaluating the systems and processes of an organisation or public agency for ensuring or safeguarding the integrity and confidentiality of anonymised information in the possession or under the control of the organisation, or transmitted or received by the organisation or public agency**.

5.6 As such, these additional defences may be applicable to the following individuals:

a) **Data Professionals**. Cybersecurity specialists, data scientists, AI engineers and statisticians in the information security and encryption industry, whose work involves the re-identification of anonymised data in order to carry out research and development or to test the robustness of their organisations' information security products and service, or their clients' information security systems.

b) **Service providers** engaged and authorised by organisations to recover data from anonymised dataset (e.g. dataset anonymised by a former employee in the course of work but who has since left and none of the current employees have the decryption key) or to carry out security testing activities, including re-identifying anonymised datasets to test whether anonymisation employed is robust.

c) **Researchers, teachers and academics** who need to re-identify anonymised data as part of their research work or for teaching on anonymisation and encryption.

d) **White-hat hackers** who independently carry out effectiveness testing of organisations' information security systems either in their personal capacity or as part of bug bounty programmes.

END OF DOCUMENT