WONGPARTNERSHIP LLP

RESPONSE TO THE PUBLIC CONSULTATION ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL

28 May 2020

WONGPARTNERSHIP LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982

Contact Partner: Lam Chung Nian
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com

1. INTRODUCTION

1.1 We wish to thank the Ministry of Communications and Information ("**MCI**") and the Personal Data Protection Commission ("**PDPC**") for the opportunity to comment on the *Public Consultation Paper: Draft Personal Data Protection (Amendment) Bill, including Related Amendments to the Spam Control Act* (issued 14 May 2020) ("**Consultation Paper**").[1]

1.2 As one of Singapore's largest and leading law firms, with many clients in the public infrastructure space, financial services, telecommunications, healthcare, media, essential services, as well as technology sectors, we are happy to share our thoughts and concerns in relation to the Consultation Paper, as it may have material impacts on many of our clients in relation to their collection, use, disclosure, and processing of personal data under the Personal Data Protection Act (No. 26 of 2012 of Singapore) ("**PDPA**") in Singapore.

1.3 In preparing our responses herein, we have had discussions with our clients to understand their concerns. We are fully supportive of the PDPC's efforts to engage in stakeholder discussions, and would be happy to further discuss or elaborate on any of the points submitted upon.

1.4 Following our review of the Consultation Paper as well as the draft Personal Data Protection (Amendment) Bill 2020 ("**Bill**"),[2] we are pleased to provide our comments below and highlight some concerns which we think merit further deliberation and consideration.

2. STRENGTHENING ACCOUNTABILITY

Mandatory Data Breach Notification

2.1 In paragraphs 13 to 26 of the Consultation Paper, MCI/PDPC proposes to introduce a mandatory data breach notification requirement where organisations will be required to *inter alia*:

(a) notify PDPC of a data breach that (i) result in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates (the "affected individuals"); or (ii) is of a significant scale; and

(b) notify affected individuals if the data breach is likely to result in significant harm to them.

("**Proposed Mandatory Data Breach Notification Requirement**").

2.2 We wish to highlight the following concerns in respect of the Proposed Mandatory Data Breach Notification Requirement, also incorporating concerns raised by our clients:

(a) Under the Proposed Mandatory Data Breach Notification Requirement, where an organisation has reason to believe that a data breach has occurred affecting personal data in its possession or under its control, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

In this regard, some of our clients have highlighted that while organisations are required to conduct an assessment as to whether the data breach is a notifiable data breach, there is a lack of clarity as to when a data breach may be considered to result in, or is

[1] https://www.mci.gov.sg/-/media/mcicorp/doc/public-consultations/public-consultation-on-pdp-amendment-bill---14may2020/public-consultation-on-pdp-amendment-bill.ashx

[2] https://www.mci.gov.sg/-/media/mcicorp/doc/public-consultations/public-consultation-on-pdp-amendment-bill---14may2020/pdp-amendment-bill.ashx

likely to result in, "significant harm" to the individuals to whom any personal data affected by a data breach relates.

It would be helpful if the PDPC could provide a statutory definition or further guidance as to the factors to be taken into account in assessing the nature of the "harm" and any relevant thresholds before the PDPC would hold the view that "significant harm" has been occasioned, so that organisations have clarity in their assessment as to when a data breach will be considered a notifiable data breach.

Further, given that the organisation bears the primary responsibility of conducting such an assessment, the PDPC should also provide assurances that the organisation would be deemed to have discharged its obligation to conduct an assessment of the data breach if the organisation is found to have conducted such an assessment in a reasonable manner, even if the PDPC ultimately disagrees with the organisation's assessment.

(b) We also understand that MCI/PDPC intends to prescribe in the regulations, categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals.

We urge the MCI/PDPC to not adopt an overly expansive list of such data. In particular, an overly broad scope of such prescribed categories of personal data will result in huge compliance costs on organisations processing such prescribed categories of personal data in their business operations, and also economic wastage arising from resources and claims devoted to addressing such matters if the listing is too extensive.

We are of the view that conceptually, the list ought to be limited to identifiers which are permanent and irreplaceable.

For example, identifiers such as debit / credit card numbers have been referenced, but in reality, these may be easily replaced by the issuing financial institutions. Furthermore, without other accompanying identifiers (e.g. names, expiry date and CVV numbers for debit / credit cards) they cannot be used for charging the customer.

Further, in prescribing such categories of personal data, the PDPC also ought to ensure that these categories of personal data are aligned with the prevailing industry guidelines in the treatment of the relevant personal data (e.g. treatment of patient data under the Ministry of Health guidelines).

(c) Under the Proposed Mandatory Data Breach Notification Requirement, where a data breach is assessed to be a notifiable data breach, the organisation is required to notify PDPC as soon as practicable, no later than three calendar days after the day the organisation determines that the data breach meets the notification criteria.

In this regard, some of our clients have raised concerns over the feasibility of three calendar days, especially in complex cases where multiple parties may be involved in the investigation and assessment process, which may warrant further investigation and assessment even after a data breach is ascertained to be notifiable. It would be particularly challenging for organisations to complete and conclude the investigation for the organisation to provide the PDPC such notification of the data breach and provide the requisite details therewith within the short timeframe of three calendar days.

Hence, it is respectfully submitted that MCI/PDPC consider:

(i) amending the notification timelines and provide longer notification timelines (e.g. three working days instead of three calendar days) so as to better facilitate the organisation's own internal investigation and assessment process;

(ii) allow for organisations to submit ad-hoc requests for an extension of the notification timeline, especially where organisations may legitimately require additional time to conclude their investigations and fully establish the facts so as to ensure that any notification to the PDPC and/or individuals are accurate and complete (e.g. notifying PDPC within three working days or such other periods as the PDPC may permit in writing); and

(iii) notification of PDPC of the fact of the incident based on information available to the organisation at the time of the submission would be sufficient to discharge the requirement, and recognising that investigations may be a continuing and ongoing process and organisations may submit supplementary incident reports to the PDPC following the initial notification.

(d) Finally, we would like to also highlight that while some of the organisations are well-placed to operationalise the Proposed Mandatory Data Breach Notification Requirement given existing parallel data breach reporting requirements under separate regulatory regimes (e.g. under the MAS technology risk management framework for the financial institutions and/or Cybersecurity Act 2018 (No. 9 of 2018) for critical information infrastructure owners), several of our clients have also highlighted that they will require additional time to operationalise the Proposed Mandatory Data Breach Notification Requirement.

Hence, the PDPC may consider providing for a "sun-rise" period in respect of the Proposed Mandatory Data Breach Notification Requirement so as to give organisations some lead time to operationalise these additional data breach notification requirements.

Removal of Exclusion of Application of the PDPA for Organisations Acting on Behalf of Public Agencies

2.3 In paragraphs 27 to 29 of the Consultation Paper, MCI/PDPC proposes to remove the exclusion for organisations that act on behalf of a public agency in relation to the collection, use or disclosure of personal data ("**Public Agency Exclusion**").

2.4 While we understand that the purpose for the removal of the Public Agency Exclusion was to close the legislative gap where non-Government entities acting as agents of Government are not covered under the PDPA or the Public Sector (Governance) Act 2018, the change will have a major impact on assumptions made or assurances given when the organisations entered into the arrangements with the public agency.

2.5 As such, we respectfully submit that the removal of the Public Agency Exclusion should only take effect in respect of appointments, arrangements and/or agreements entered into after a specified effective date, and should not apply to any pre-existing agreements between private organisations and the public agencies given that such pre-existing agreements would have been premised on the common understanding that the collection, use, or disclosure of personal data by such private organisations would have been excluded from the application of the data protection provisions under the PDPA.

3. ENABLING MEANINGFUL CONSENT

Legitimate Interests Exception

3.1 In paragraph 40 of the Consultation Paper, MCI/PDPC proposes to introduce a new general legitimate interests exception to enable organisations to collect, use or disclose personal data in circumstances where it is in the legitimate interests of the organisation and the benefit (includes any economic, social or security benefit) to the public (or any section thereof) is greater than any adverse effect on the individual ("**Proposed Legitimate Interests**

Exception"). In particular, before collecting, using or disclosing the individual's personal data, the organisation must first conduct an assessment, and inform the individual, in any reasonable manner, that it is collecting, using or disclosing personal data (as the case may be) under the Proposed Legitimate Interest Exception. Additionally, the Consultation Paper also expressly provides that the Proposed Legitimate Interests Exception must also not be used for sending direct marketing messages to individuals.[3]

3.2 We are of the view that to require organisations to balance public benefit against adverse effect to the individual before organisations are entitled to rely on the Proposed Legitimate Interests Exception to collect, use and/or disclose individual's personal data without consent will result in this exception being too narrow.

3.3 In particular:

(a) If the Proposed Legitimate Interests Exception only applies where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate,[4] this will significantly circumscribe the utility of the Proposed Legitimate Interests Exception.

(b) In comparison, under Article 6(1)(f) of the GDPR, the balancing exercise only requires the controller to assess whether the legitimate interest pursued by the controller or by a third party is overridden by the individual's interests, rights or freedoms. Hence, the legitimate interests are not limited only to the organisation in question, but also any third party, including a third party individual. Additionally, the balancing exercise only requires the balancing of the identified legitimate interests pursued against such individual's interests, rights or freedoms.[5]

(c) Hence, while the Proposed Legitimate Interests Exception brings the PDPA regime one step closer in the alignment of the legal bases for which organisations may collect, use and/or disclose personal data under the GDPR and the PDPA, the divergence in the details between the Proposed Legitimate Interests Exception and Article 6(1)(f) of the GDPR adds to uncertainty as well as compliance costs for organisations who are regulated by the GDPR as well as the PDPA regimes.

3.4 Further, we are also of the view that there is no compelling reason for excluding the sending of direct marketing messages to individuals from the scope of the Proposed Legitimate Interests Exception. In particular, we would highlight that:

(a) Given the comprehensive safeguards under the Proposed Legitimate Interests Exception, which requires organisations to *inter alia* conduct an assessment before the collection, use and disclosure of personal data as well as to inform the individual of the organisation's reliance of the Proposed Legitimate Interests Exception for such collection, use or disclosure of personal data, we are of the view that these are adequate safeguards for the collection, use and/or disclosure of personal data for the purposes of sending of direct marketing messages to individuals.

[3] Paragraph 40 of the Consultation Paper, and Clause 31 of the Bill.

[4] Paragraph 40 of the Consultation Paper.
In paragraph 40 of the Consultation Paper and Clause 31 of the Bill, MCI/PDPC proposes to introduce a new general legitimate interests exception

[5] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

(b) For reference, Recital 47 of the GDPR also provides that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest".

3.5 Given the foregoing, we respectfully submit that the Proposed Legitimate Interests Exception should recognise that organisations may collect, use or disclose personal data about an individual where it is in the legitimate interests pursued by the organisation and/or any third party, and such legitimate interests are greater than any adverse effect on the individual. Additionally, the Proposed Legitimate Interests Exception ought to also recognise direct marketing to individuals as one of the potential legitimate interests that organisations may pursue.

3.6 In any case, the PDPC also ought to recognise and explicitly provide that the collection, use and/or disclosure of personal data within a group of companies is a legitimate interest of an organisation, and there should not be any need to demonstrate a public interest or benefit.

3.7 Many clients having corporate group structures have provided feedback that many common functions are intra-sourced within the group – for example, payment processing, IT infrastructure or human resource functions may be handled by a corporate group office, which may be distinct from the legal entity providing goods or services to customers. Such intra-group data transfers are not only prevalent amongst groups of companies but are a reflection of how many groups are organised (i.e., with centralised business functions (e.g. finance, human resource, legal, etc.). It would be impractical to require group organisations to seek to obtain the individual's fresh consent for such intra-group transfers as there is a real requirement to permit for entities within the group to share personal data for efficient operations.

3.8 It is thus respectfully submitted that MCI/PDPC considers recognising an exception to the need for consent where organisations within a corporate group collect, use or disclose personal data for purposes consistent with the purposes for which any group company had originally collected such personal data, including administration, processing or performance of any contracts, and where such purposes have been notified to the individuals concerned. This exception should not require the organisation to demonstrate any larger public or systemic benefits.

<u>Business Improvement Exception</u>

3.9 In paragraph 40 of the Consultation Paper, MCI/PDPC proposes to introduce a new business improvement exception to make clear that organisations may use personal data (that was collected in accordance with the PDPA) without consent for the following business improvement purposes, if such purposes cannot reasonably be achieved without the use of the personal data in an individually identifiable form and the use of the personal data by the organisation does not have any adverse effect on the individual to whom the personal data relates:

(a) to improve or enhance any goods or services provided by the organisation, or develop new goods or services;

(b) to improve or enhance the methods or processes, or develop new methods or processes, for the operations of the organisation;

(c) to learn about and understand the behaviour and preferences of the individual or any other customer of the organisation in relation to the goods or services provided by the organisation; and/or

(d) to identify goods or services provided by the organisation that may be suitable for the customers of the organisation other than individual customers

("**Proposed Business Improvement Exception**").[6]

3.10 Many clients have indicated they are in support of the MCI/PDPC's proposal to introduce the Proposed Business Improvement Exception given that it provides the much-needed clarity for organisations to utilise their personal data records for providing better and more relevant products.

3.11 However, we would highlight certain concerns as follows:

(a) While paragraph 40(b) of Consultation Paper provides that the intention is for the Proposed Business Improvement Exception to apply to a group of companies (e.g. subsidiaries of the organisation), this does not appear to be consistent with the statutory language used in Clause 32 of the Bill.

In particular, we note that paragraph 2 of Part 2 of the Second Schedule only allows organisations (and not the group of companies) to *use* the personal data without consent for the specified purposes (which may suggest organisations are not entitled to disclose the personal data under this same exception to other organisations in the group).[7]

(b) Additionally, there is also a lack of recognition that most of the organisations may not have the capability internally and/or within the group to conduct such data analytics, and would, therefore, have to rely on specialised third-party service providers to assist in performing such data analytics on their behalf.

As such, the law should similarly recognise business realities where organisations would have to outsource such data analytics functions, and should not be placed in a position where they would be placed unfairly under more stringent compliance requirements for such outsourcing activities.

Hence, we are of the view that the Proposed Business Improvement Exception ought to be clarified to allow for the collection, use and/or disclosure of personal data by such third-party service providers to undertake such business improvement purposes on behalf of the organisation (again, the placement of this exception in Part 2 Schedule 2, as opposed to the First Schedule, would suggest that it is specifically confined to internal use by the organisation of its own records, and may call into question whether any disclosure to or collection by an outsourced provider, or as mentioned above, other group companies, would be permitted).

In this regard, we are of the view that such an expansion should not give rise to concern as there are adequate safeguards in that the organisations nevertheless still bear the burden of demonstrating that the purpose for which the organisation collects, uses or discloses the personal data cannot reasonably be achieved without the collection, use or disclosure of personal data in an individually identifiable form, and such collection, use or disclosure of personal data by the organisation does not have any adverse effect on the individual to whom the personal data relates.

3.12 In light of the foregoing, we respectfully submit that the Proposed Business Improvement Exception should be expanded to include the collection, use and/or disclosure of personal data amongst the organisations' affiliates and/or third-party service providers for the aforementioned

[6] Paragraph 40 of the Consultation Paper, and Clause 32 of the Bill.

[7] Clause 8 of the Bill provides that under the amended Section 17 of the PDPA, an organisation may use personal data about an individual without the consent of the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 2 of the Second Schedule.

business improvement purposes (e.g. by placing the Proposed Business Improvement Exception under the revised Schedule 1 of the PDPA).

Identification and Assessment of Adverse Effect

3.13 In paragraphs 37 to 42 of the Consultation Paper, MCI/PDPC proposes to impose a requirement for organisations to *inter alia* identify and assess the adverse effect on the individual before the organisation will be able to rely on the enhanced framework for the collection, use and disclosure of personal data, such as:

(a) the Proposed Legitimate Interests Exception, where the organisation needs to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is in the legitimate interests of the organisation; and the benefit to the public or any section of the public of the collection, use or disclosure (as the case may be) is greater than any adverse effect on the individual;

(b) the Proposed Business Improvement Exception, where the organisation needs to be satisfied that the intended use of the personal data cannot reasonably be achieved without the use of the personal data in an individually identifiable form, and the use of the personal data by the organisation does not have any adverse effect on the individual to whom the personal data relates; and

(c) the proposed deemed consent by notification, where organisations are required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual.

3.14 We would like to highlight that:

(a) The PDPC should clarify and provide further guidance on the law as to what would constitute "adverse effect" on individuals and how such "adverse effects" may differ from "significant harm" under the PDPA.

(b) Some of our clients have also raised concerns that there is a lack of clarity as to the standard by which organisations are expected to identify such adverse effects on the individuals and/or carry out such assessments, particularly where organisations will face practical challenges in identifying every possible adverse effect on the individual.

Hence, consistent with the PDPC's shift to a risk-based accountability approach, we are of the view that PDPC ought to recognise that organisations would only be required to conduct an identification and assessment exercise to a reasonableness standard.

In the same vein, the same reasonableness standard ought to be similarly extended to the organisation's assessment as to the applicability of the various consent exceptions under the PDPA to the organisation's processing of personal data, and the organisation ought to be excused from its reliance on such exceptions where the organisation was found to have conducted such an internal assessment in a reasonable manner, even if the PDPC ultimately disagrees with the organisation's assessment on the applicability of the consent exceptions.

(c) Further, we also note that MCI/PDPC has referenced the Data Protection Impact Assessment ("**DPIA**") as one of the accountability tools introduced by the PDPC for organisations to demonstrate accountability in meeting data protection standards.

The Guidelines issued by the PDPC so far are very prescriptive, and appear to be directed at a DPIA undertaken when introducing a new IT system, hence it recommends

a phased lifecycle approach. For the purposes of invoking these exceptions, such an approach may be too formalistic and burdensome on organisations.

Instead, MCI/PDPC may wish to make clear that while the DPIA is one method by which organisations can conduct the aforementioned assessment of the adverse effects on the individual, organisations should be allowed reasonably conduct such assessments in such form and manner as the organisation determines to be appropriate in the specific context and circumstances, by reference to identified criteria. This will provide organisations with the flexibility to determine the type of assessment that needs to be conducted against their business and operational needs as well as avoiding unnecessary compliance costs. An example of such an approach is how the Monetary Authority of Singapore approaches technology risk management, in its Technology Risk Management Guidelines, where best practices are identified, and the management of each regulated institution is expected to make its own assessments as to the compliance steps to be taken, but no specific procedure is prescribed for this.

We should also mention that under the GDPR, the use of impact assessments is generally reserved for processing that is likely to result in a high risk to individuals (e.g. where sensitive data or a significant number of data subjects are involved). In other cases, the data protection authorities have generally recommended for organisations to adopt a more light-touch risk assessment tool based on the specific context and circumstances of the processing.[8]

Other Comments

3.15 In addition to the above points highlighted in the Consultation Paper, we would also like to take the opportunity to provide comments on certain other areas which MCI/PDPA may wish to consider:

(a) Business Asset Transactions Exception

Under Paragraph 11 of Part 3 of the First Schedule under Clause 31 of the Bill, we understand that MCI/PDPC proposes to streamline and consolidate the exceptions to consent, including the business asset transaction which allows an organisation to collect, use and/or disclose personal data about an individual without the consent of the individual where the personal data about an individual is:

(i) collected by an organisation, being a party or a prospective party ("**X**"), to a business asset transaction with another organisation ("**Y**") from the Vendor;

(ii) used or disclosed by X in relation to the business asset transaction with the Vendor; or

(iii) disclosed by Y to X for the purposes in sub-paragraph (a) above,

("**Business Asset Transactions Exception**").

For an organisation to rely on the Business Asset Transactions Exception, the personal data must be (i) be about an employee, a contractor, a customer, a director, an officer or a shareholder of Y; and (ii) relate to the party of Y or its business assets with which the business asset transaction is concerned.

We are of the view there is no compelling reason for the Business Asset Transactions Exception to be narrowly limited to the categories of personal data above and in

[8] See the Information Commissioner's Office sample legitimate interests assessment template at https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

particular, narrowly applied to the personal data of individuals in connection with Y. In particular, we think that there is a lack of recognition that there may be business asset transactions where Y and the business assets/target company in question may be different parties (e.g. in a share purchase transaction where the target company will not be a party to the business asset transaction), and the collection, use and/or disclosure of personal data of employee, a contractor, a customer, a director, an officer or a shareholder of business assets/ target company are equally, if not more important, to facilitate the business asset transaction.

For example, the employee personal data of the business assets/target company may need to be disclosed and collected by the acquiring company to facilitate the integration of the group companies' human capital resources to realise the synergies of the share sale transaction.

The exception should also be recast beyond merely addressing "business asset transactions", i.e., transactions structured as a sale of the assets of an organisation, to also include other transaction structures which may equally involve a need to understand the personal data records and handling practices of the organisation, e.g. purchase of shares in the company, or amalgamation of the company.

(b) Individual Interests

Under Paragraph 1 of Part 1 of the First Schedule under Clause 31 of the Bill, we note that organisations may collect, use or disclose personal data about an individual without the consent of the individual, where such collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any purposes which are clearly in the interests of the individual.

In this regard, one of our clients has raised concerns that there is ambiguity as to what is intended by "clearly in the interests of the individual", and it is not clear in what situations will organisations be able to collect, use or disclose the individual's personal data for purposes which is clearly in the interests of the individual. In light of the foregoing, PDPC should also assist organisations in making their assessment of the applicability of the consent exception to their processing of personal data by clarifying what is intended by "clearly in the interests of the individual" and provide further guidance and illustrative examples demonstrating the applicability of this consent exception.

(c) Access Request and Security of the Organisation

Under Section 21(3) of the PDPA, an organisation shall not provide an individual with the requested information pursuant to the access request if the provision of that information could reasonably be expected to *inter alia* (i) threaten the safety or physical or mental health of an individual other than the individual who made the request; (ii) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; or (iii) be contrary to the national interest.

While these exceptions are currently tied towards the potential harm towards the individual requestor, a third-party individual and/or the wider public, we are of the view that the potential harm towards the organisation ought to also be considered and included as an exception to the organisation's access obligation.

In particular, the organisation ought to be allowed to reject the individual's access request where there is a threat to the security of the organisation. For example, an individual's request for access to CCTV footage in sensitive areas may inadvertently

expose the organisation to security threats because "blind spots" in the organisation's security coverage may then be exposed.

4. INCREASING CONSUMER AUTONOMY

Data Portability Obligation

4.1 In paragraphs 43 to 52 of the Consultation Paper, MCI/PDPC proposes to introduce a new data portability obligation where an organisation must, at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control to another organisation in a commonly used machine-readable format ("**Proposed Data Portability Obligation**").[9]

4.2 In this regard, we would like to highlight that many of our clients continue to raise concerns in connection with the introduction of the Proposed Data Portability Obligation and would like MCI/PDPC to reconsider the introduction of the Proposed Data Portability Obligation in light of the significant compliance costs and manpower requirements required to operationalise and comply with the Proposed Data Portability Obligation.

4.3 In addition, we would also like to highlight the following concerns:

(a) The broad scope of data[10] covered by the Proposed Data Portability Obligation may potentially conflict with the organisation's intellectual property rights comprised in these datasets. We are of the view that there is a lack of clarity over how the confidentiality exception[11] may also extend to protect intellectual property rights, as well as proprietary data processing methodologies:

(i) Under the current approach take under the Proposed Data Portability Obligation, we think that there is a general lack of recognition that intellectual property rights are private property rights which grants the intellectual property owner certain rights to exclude others, and where intellectual property rights confer upon the rights-holders legal monopoly over their intellectual property rights, there are already sufficient safeguards under the respective intellectual property regimes against any abuse of such legal monopoly (e.g. through statutory compulsory licensing mechanisms as well as statutory exceptions and limitations).

(ii) In particular, under international treaty norms, any copyright exceptions ought to only apply in certain special cases, which do not conflict with a normal exploitation of the copyright material, and should not unreasonably prejudice the legitimate interests of the rights holders.[12]

(iii) While we acknowledge that there is a need to allow organisations to have access to more data to spur the development of innovative data-driven applications that will benefit consumers, such concerns needs to be balanced

[9] Paragraph 43 to 52 of the Consultation Paper, and Clauses 13 and 16 of the Bill.

[10] We note that the Proposed Data Portability Obligation will be scoped to cover:
(a) user provided data (i.e. data that is provided to the organisation such as name, contact information, credit details, delivery address); and
(b) user activity data (i.e. .data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors),
held in electronic form, including business contact information.

[11] The proposed confidentiality exception allows organisations to reject any data portability requests in relation to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation

[12] Article 13 of the TRIPS Agreement which provides that "Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder".

against the organisation's intellectual property rights comprised in these data, including trade secrets and database rights where applicable.

(iv) In the increasingly data-driven digital economy, an organisation's competitive advantage and value of their intellectual property assets may lie precisely in that organisation's capabilities in data collection processes (e.g. their ability to collect and parse data to tailor their products and services for their users). For example, the value of an organisation employing artificial intelligence ("**AI**") technologies to drive its business innovation would be largely driven by the amount of data the organisation is able to collect, including the availability of user-activity data used to train their AI algorithms. Similarly, significant investments are made by organisations to build up the organisations' capabilities to collect and process large amounts of data as well as the collection and proprietary methodologies to curate (or "clean") these data sets (sometimes known as "cleaning" models) to meaningfully understand raw user activity data. However, if organisations are obliged to port user activity data pre and post-treatment by such proprietary methodologies, the intellectual property assets, as well as the competitive edge of businesses which generate value based on its ability to collect and treat data, could be eroded, creating a dampening effect on innovation.

(v) In this regard, we note that the proposed confidentiality exception preserves some of the organisation's rights insofar as these data constitute confidential commercial information. However, greater clarity may be required as to the interaction between the Proposed Data Portability Obligation and the protection of intellectual property rights and trade secrets of the organisation under the law.

(vi) By way of comparison, Article 20(4) of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") provides that the data subject's right to data portability "shall not adversely affect the rights and freedoms of others", which may include trade secrets or intellectual property and in particular the copyright protecting the software.[13]

(vii) The Proposed Data Portability Obligation should not be allowed to allow individuals to misuse the information in a way that would constitute a violation of intellectual property rights.

We are of course mindful that not all datasets may, in fact, be protected by intellectual property rights, for example, the dataset does not meet requirements for copyright protection as a compilation. However, where the dataset will enjoy intellectual property protection, it is not clear that if the data portability right will operate as a form of a statutory licence to the intellectual property rights – as such, the GDPR approach is well-founded in recognising this concern and yet will not affect the data portability obligation where the dataset is not in fact subject to intellectual property protection.

Given the foregoing, we respectfully submit that the PDPC should make it clear that consistent with the GDPR, the proposed amendments under the PDPA should reflect that the data portability rights will not affect any intellectual property rights owned by the disclosing party.

[13] Article 29 Data Protection Working Party confirmed in the Guidelines on the right to data portability (as last revised and adopted on 5 April 2019) at page 12.

(b) Under the Proposed Data Portability Obligation, porting organisations will be required to transmit prescribed personal data in the possession or under the control of the porting organisation to the receiving organisation specified in the data porting request.[14]

We are of the view that there is a lack of recognition that in practice, different parties may have possession and control of the specified personal data. In other words, porting organisations with possession of the personal data may be prevented, contractually, technically or legally, from transmitting such personal data to the receiving organisations where a third party is the organisation with control over the personal data.

For example in the private healthcare industry, while private hospitals may have possession of a patient's medical records, each consultant specialist physician treats his/her patient under the auspices of his/her own clinic, and would therefore also controls patient records generated in the course of his/her review or consultation with the patient (and this remains even when the patient is warded at the hospital). As such, whilst patient notes or test results may be stored in a hospital database, it is not in fact in a position to comply with data portability request as it does not own or control these patient records.

Given the foregoing, the PDPC should recognise that organisations with only possession of the personal data (and not control) should not be required to comply with data portability requests, and limit the Proposed Data Portability Obligation to only porting organisations with possession and control of the personal data.

(c) Additionally, we note that the PDPC recognises that there exists several data porting models which may serve different scenarios or business models.[15] However, we would like to highlight that there is a lack of recognition that the B2B data porting "push" or "pull" models to facilitate the porting of data between organisations may not be entirely suitable for all industries and/or services, and alternative data porting models such as B2C data porting models may be more appropriate in certain situations.[16]

As such, the PDPC should ensure that the Proposed Data Portability Obligation is flexible enough to provide for such alternative data porting models to be adopted where it is determined to be more suitable for the respective industry sectors. In particular, the definition of the receiving organisation ought to be able to recognise that the receiving party might be the requesting individual as well to facilitate the adoption of B2C data porting models. Alternatively, a B2C model may be prescribed as sufficient to discharge the porting obligation.

4.4 Additionally, we also understand that the Proposed Data Portability Obligation will only come into effect with the issuance of regulations that will prescribe requirements that apply to the porting of specific datasets, and PDPC will work with the respective industry regulators to develop these requirements which will address *inter alia* the "whitelist" of data categories covered by the Proposed Data Portability Obligation, the technical and process details, the data porting request models as well as the safeguards for individuals in relation to the Proposed Data Portability Obligation.

4.5 Given the varied nature of data involved as well as market dynamics in each of the sectors, we are supportive of the PDPC's commitment to engage each of the respective sectors to develop these detailed data portability requirements where the industry stakeholders will be in the best position to provide more detailed comments on the challenges they face as well as any other

[14] Under Section 26E of the Proposed Data Portability Obligation,

[15] Paragraph 47(c) of Consultation Paper.

[16] See Section 1798.100(d) of the California Consumer Privacy Act.

unique problems they may have in complying with the Proposed Data Portability Obligation. In these engagements and/or when detailing the data portability regulations, the PDPC should also clarify:

(a) how will the Proposed Data Portability Obligation interface with the relevant sectoral regulatory framework and guidelines as well as any prevailing industry practice, such as the *Code of Practice for Competition in the Provision of Telecommunication Services 2012* for the telecommunication industry, the *Code of Practice for Market Conduct* for the media market, or Ministry of Health guidelines in relation to the disclosure of patient data;

(b) how will the Proposed Data Portability Obligation interface with data portability requests across multiple sectors where standards may be different (e.g. from the financial industry to the tech industry, etc.);

(c) how will the Proposed Data Portability Obligation interface with the PDPA's transfer limitation obligation, where organisations may be requested to transmit the specified personal data to an overseas office of a business entity with presence in Singapore;

(d) whether the porting organisations are expected to provide the requestor with the reasons for rejection of the data portability request, even where such reasons could be confidential, offensive and/or contrary to national interest;

(e) the definition of commercially sensitive information, and whether personal data involving the organisation's products and services pricing may constitute such commercially sensitive information;

(f) the definition of "reasonable time and fees" for porting data;

(g) the definition of "ongoing relationship with the individual" in connection with the porting organisations. For example, in the healthcare sector, there is no clear indication as to what might constitute an ongoing relationship between the healthcare provider and the patient, in particular where there is no subscription, account services or a defined period as to when patients may revisit (even if they have been encouraged or advised to);

(h) whether the porting organisations would be allowed to reject and/or remove certain personal data before transmitting the information to the receiving organisation where the transmission of requested personal data in the data porting request might prejudice the porting organisation's legitimate and reasonable interests and/or business operations, and whether the porting organisation will be required to inform the individual requestor of such removal of personal data;

(i) when will personal data be considered to constitute "derived data"; and

(j) whether other organisations will be allowed to make data porting requests on behalf of a group of individuals, e.g. where corporate clients are requesting for their employees' personal data to be ported to another service provider.

<u>Preservation of Personal Data in relation to Access / Data Portability Requests</u>

4.6 In paragraph 71 of the Consultation Paper, MCI/PDPC proposes to introduce a requirement for organisations to preserve personal data requested (or a copy) pursuant to an access request and/or data portability request for a prescribed period of (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later.

4.7 While we understand that there is a need to preserve the availability of a meaningful remedy should the individual succeed in his/her application, the rights of the individuals need to be balanced against the organisation's interests and the costs of compliance. In particular, we note that:

(a) Some of our clients have raised significant concerns over the introduction of such a preservation requirement and have highlighted that there is no compelling reason for businesses to retain and/or preserve the individual's personal data where such retention is no longer necessary for legal or business purposes, and that organisations should be allowed to determine when its electronic records are deleted.

Further, the introduction of this preservation requirement introduces uncertainty for organisations given that there is no fixed timeline as to when the individual will exhaust his/her right to apply for a reconsideration request to PDPC and such further appeals.

As such, organisations may be potentially expected to preserve such personal data requested (or a copy) for an indefinite period of time without clarity as to when the organisation would be allowed to dispose of such data, thereby incurring high compliance costs in terms of tracking the status of such reconsideration requests and/or timelines as well as operationalising the preservation of such personal data.

For example, for most CCTV systems, CCTV footage would be automatically erased after a certain period of time, and organisations would have to spend significant infrastructure and manpower training costs to operationalise the preservation obligation as well as tracking and maintaining the database of preserved personal data.

Given the foregoing, we would respectfully submit that MCI/PDPC might wish to reconsider its proposal to introduce such a preservation requirement. In any case, we also note that the PDPC nonetheless reserves the right to review an organisation's refusal to provide access to the requested personal data and provide such directions to the organisations under Section 28(2) of the PDPA, including to direct the organisation to provide access to the personal data within such time as the PDPC may specify.

(b) Even if the PDPC decides to continue to introduce such a preservation requirement, we would respectfully submit that the PDPC should impose a prescribed reasonable maximum period that organisations are obliged to preserve personal data requested pursuant to an access and/or data portability requests after the rejection of the request, and allow organisations to impose an additional reasonable fee for the preservation of such personal data. This will not only minimise the organisation's compliance costs and enable the organisations to recoup the relevant costs for operationalising the new preservation requirement, but also prevent individuals from abusing the system with frivolous or vexatious access and/or data portability requests.

<u>Improved controls for unsolicited commercial messages</u>

4.8 In paragraph 54 of the Consultation Paper, MCI/PDPC proposes to *inter alia* amend the Spam Control Act (Cap. 311A) to cover messages sent to instant messaging accounts through platforms such as Telegram and WeChat. In this regard, MCI/PDPC also noted that such platforms "are currently not covered by the DNC Provisions and the Spam Control Provisions".

4.9 In light of the foregoing, please could MCI/PDPC clarify whether the other instant messaging platforms will also automatically fall within the scope of the proposed amendments and whether such instant messaging platforms are not presently covered by the PDPA's Do Not Call Provisions as well as the Spam Control Act.

5. STRENGTHENING EFFECTIVENESS OF ENFORCEMENT

5.1 In paragraph 58 of the Consultation Paper, MCI/PDPC proposes to increase the maximum financial penalty for data breaches under the PDPA to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.

5.2 While we note that the higher financial penalty cap was introduced to serve as a stronger deterrent, and provide PDPC with more flexibility in meting out financial penalties based on the circumstances and seriousness of a breach, we would like to highlight that there have been various concerns over the formulation of higher financial penalty cap:

(a) Many of our clients have expressed concerns over the increased financial penalty cap of 10% of an organisation's annual gross turnover in Singapore, and have also highlighted that there is no compelling reason for the financial penalty to be calculated based on the organisation's turnover, which unfairly punishes organisations with high turnover and lower profit margins.

In particular, for example, property sector clients will have very high revenue figures as their properties sold in the course of their routine course of business have high transaction values, and such a formulation therefore unfairly exposes them to very high ceilings for PDPA related penalties.

(b) There are also concerns surrounding the equity of the penalties where organisations are subjected to differing amounts of penalties for breaches of the same degree and nature.

(c) While the intention is to introduce flexibility for the PDPC in meting out financial penalties based on the circumstances and seriousness of a breach, we note that the proposed financial penalties do not differentiate between the different breaches of the PDPA as well as the severity of the different breaches.

By way of contrast, under the GDPR regime, depending on the provisions of the GDPR which are breached, administrative fines range from 10,000,000 EUR or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher to administrative fines up to 20, 000, 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(d) Further, while the policy intention is for the financial penalty is capped at 10% of the organisation's annual gross turnover in Singapore, Clause 17 of the Bill does not appear to expressly limit the financial penalty to 10% of the organisation's annual gross turnover in Singapore. [17]

Under the PDPA, organisations may also include foreign entities with operations in Singapore and/or Singapore entities with overseas businesses that collect, use and/or disclose personal data about an individual.[18] By capping the financial penalty at 10% of the organisation's most recent audited accounts, there is a possibility that this will also

[17] Clause 17 of the Bill provides *inter alia* that the amount of the financial penalty must not exceed, where the direction is given to an organisation or a person with an annual turnover exceeding $10 million (as ascertained from the most recent audited accounts of the organisation or person available at the time the direction is given), and the failure to comply that is the subject of the direction occurs on or after the date of commencement of section [17] of the Personal Data Protection (Amendment) Act 2020 — 10% of the annual turnover.

[18] Section 2 of the PDPA defined organisations to include any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident or having an office or place of business in Singapore.

include the company's turnover and/or profits from the organisation's business in other jurisdictions.

In contrast, we note that Section 69(4) of the Competition Act (Cap 50B) clearly provides that no financial penalty fixed by the competition commission may exceed 10% or such other percentage of the turnover of the Singaporean business.

(e) Given the foregoing, we would respectfully submit that the PDPC should reconsider its proposal to introduce the increased financial penalty cap under the Bill, and even if PDPC decides to proceed to introduce the increased financial penalty cap, the PDPC may consider *inter alia*:

(i) reformulating the increased financial penalty to be capped in a tiered fashion, at 1 to 2% of the organisation's annual profit in Singapore, depending on the severity of the breach of the PDPA;

(ii) make it clear that consistent with the Competition Act (Cap. 50B), the proposed amendments under the PDPA should reflect that the financial penalty cap will be limited to 1 to 2% of the annual profits of the business of the organisation in Singapore;

(iii) applying an absolute monetary cap;

(iv) any increase in the financial penalty should not apply in relation to breaches of the PDPA before the inception date of the increased penalty regime; and

(v) clarifying that only the relevant subsidiaries' and/or business units' annual profits will be used to calculate the financial penalty in respect of breaches of the PDPA by its subsidiaries and/or business units.

5.3 Finally, in light of the unforeseen economic impact of the COVID-19 situation on businesses in Singapore and globally, we would further respectfully submit that the PDPC could consider deferring the introduction of such an increased financial penalty and/or providing for a graduated increase in the financial penalty so as to aid businesses to tide over this difficult period.

6. **CONCLUSION**

6.1 In conclusion, we agree that, in light of the emerging digital economy, there is a need to provide a balanced regulatory approach to ensure that Singapore's data protection framework continues to keep pace with evolving technological and business landscape whilst giving consumers effective protection of their personal data in the Digital Economy.

6.2 The driving vision for the proposed amendments under the Bill should be to enable Singapore's data protection framework to be in step with global regulatory trends and practices, as well as cater to the needs of businesses and individuals in the evolving digital economy.

6.3 However, the imposition of many of the requirements as proposed will likely also translate into significant business costs, and also raise other concerns in relation to the protection of intellectual property, confidentiality and cybersecurity.

6.4 Hence, we respectfully urge MCI/PDPC to take into account the concerns highlighted above, and provide greater clarity and guidance in connection with the proposed requirements as discussed above, as well as allow organisations more flexibility and leeway in the manner in which the obligations may be addressed.

WONGPARTNERSHIP LLP

28 May 2020