US-ASEAN Business Council
8 Shenton Way, #29-03,
AXA Tower,
Singapore, 068811
Tel +65 6339 8885

US-ABC Response to Public Consultation on the Draft Personal Data Protection (Amendment) Bill and Amendments to the Spam Control Act

The US-ASEAN Business Council ("**US-ABC**") and our members express our sincere gratitude to the Ministry of Communications and Information ("**MCI**") and the Personal Data Protection Commission ("**PDPC**") for this opportunity to provide comments on the Personal Data Protection (Amendment) Bill 2020 ("the **Bill**"). We welcome the opportunity for further discussion on the proposed Bill. Thank you again for your consideration of our comments, and we look forward to working with MCI and PDPC as the Bill is finalized and implemented. Should you have any questions or need clarification on any of the points addressed, please contact our Senior Director, Mr. Shay Wester at [Redacted], or our Manager for ICT, Natalie Tantisirirat [Redacted].

Summary of Major Points

- **Mandatory Data Breach Notification** – We encourage the introduction of Data Breach Notification (DBN) and suggest that the requirement outline a criterion for reportable breaches, provide clear guidelines on the items to be reported and extend the 3 calendar day timeline for notification. In addition, we propose the definition of "data breach" be revised to state when the DBN should be triggered, consistent with international practices (proposed Section 26A).
    - In the current Bill, the threshold for notification to be based on the likelihood of "significant harm" is unclear. This could result in the PDPC and individuals being inundated with numerous immaterial notices, resulting in "notification fatigue" and a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm.
    - The proposed 3 calendar days for notification to the PDPC imposes a significant burden on data controllers and supervisory authorities alike, especially where there are multiple intermediaries (or sub-intermediaries) which may require the organization to carry out multiple assessments of the nature and impact of the breach before it notifies the PDPC. We recommend notification should be encouraged "as soon as practicable" or "without undue delay" from the completion of all relevant assessments. Imposing a 3-day limit will divert valuable resources that should be focused on containing and remedying the breach to preparing and filing the notification within the deadline, possibly based on incomplete information in the absence of sufficient time for a thorough investigation.
    - A data classification approach or a "whitelist" of data categories (e.g. credit/debit card numbers being deemed as sensitive data for purposes of a data breach, or any unique identifiers) should be avoided for purposes of determining "significant harm" to individuals. Such a data classification approach has been adopted by other countries for other purposes (e.g. data localization) and this approach would work against Singapore's data hub strategy. A principles-based approach of relying on an appropriate threshold of harm (e.g. serious harm) is recommended instead.

  - Consent Requirement – The exceptions for consent requirement should be wide enough to cover other commercial purposes beyond market research. Examples include an intermediary providing data services or intermediary-developed data solutions. It is also important to clarify whether the legitimate interests and business improvement can be relied upon by an intermediary, and whether these exceptions only apply to the legitimate interests of, or business improvements by, the organization which has collected the data.
- **Data Portability Obligation** – Broad data portability requirements should not be mandated. A broad implementation of the data portability right may stifle competition and innovation and impose unnecessary burdens on organizations.
  - If MCI/PDPC proceeds with mandating data portability, this should be carried out in close consultation with the industry, given that the various facets of data portability, including the types of data involved, the industries involved and the responsibilities incumbent on such companies should be thoroughly assessed prior to the implementation of any mandatory data portability requirements.
  - The portability obligation should ensure a level playing field between the entities obliged to share the data (data transmitters) and those with whom the data should be shared (data receivers), so that information can port in both directions. An absence of bidirectional flows of data has the potential to create competition concerns and so it is key that the principle of reciprocity be embedded within the data portability framework.
  - We further recommend that:
    - The "whitelist" of data categories be narrowly scoped to meet the purpose of allowing individuals to switch to new service providers more easily.
    - Any direct service-to-service portability is limited to where it is "technically feasible".
    - The "whitelist" of data categories exclude types of data that provide no clear value to individuals' ability to switch providers, and/or take time for organizations to process, including (i) user activity data generated from the use of proprietary tools or features, (ii) user-generated content (such as voice recordings, videos, images, customer reviews and feedback), and (iii) unstructured data.
  - In support of global data portability and the Singapore digital economy, we support a risk-based approach in developing internationally-accepted data protection standards for operational environments. Alignment of the Bill to these efforts will further result in regulatory harmonization for the implementation.
- **Unsolicited messages** – While we support having improved controls for unsolicited messages, it is also important to include, in the new provisions to be inserted pursuant to proposed Section 27 of the Bill, and in the Spam Control Act, a presumption (similar to the one in Section 36(2) of the Personal Data Protection Act) that the unsolicited messages are not sent by those who merely provide the underlying services used to send the messages.
- **Increased financial penalty cap** – Civil penalties should not be tied to a regulated entity's turnover, and should be proportional to the harm caused to the data subjects and whether there are any aggravating or mitigating factors (including where part or most of the entity's turnover may be derived from jurisdictions where the PDPA does not apply). In our view, the

proposed penalty limit of "10% annual gross turnover" is excessive. Civil penalties frameworks should not impose undue hardship on an otherwise responsible entity. This potentially discourages companies from carrying out business activities in Singapore, including the setting up of any global or regional headquarters, or locating data hubs in Singapore, thereby potentially deterring innovation and investments by businesses in Singapore. Nonetheless, if PDPC imposes the revenue-based maximum financial penalty, then the Bill should clarify that the cap is based on turnover "in Singapore", which would reflect PDPC's intention as stated in the Public Consultation document. To avoid penalising organisations that act in good faith, PDPC should also consider introducing a provision that it may impose a financial penalty only if the infringement has been committed intentionally or negligently.

- **Implementation period and industry consultation for subsequent Regulations** – We appreciate the efforts of MCI/PDPC to consult with stakeholders in developing the Bill, thus far. We also request that MCI/PDPC commit to consulting with industry prior to the development of prescribed requirements in the subsequent Regulations. A clear timeline for implementation is important to allow organizations the time necessary to collect information, draft processes, policies, and protocols to address the requirements of the Bill. Without such lead time, organizations may not have enough time to put in place robust and well-designed processes, policies, and protocols.

Please find below our further detailed comments regarding the Bill for your consideration.

Statement of Interest

The US-ASEAN Business Council represents over 160 of the largest U.S. companies doing business in Southeast Asia. Our members span across all sectors and include leading technology companies in hardware, software, digital services, telecommunications, media, internet and financial services. Our members are deeply committed to taking part in the development of a data-driven digital economy in Singapore.

The Council strongly supports the Government of Singapore's dedication to a national personal data protection framework that strengthens accountability and consumer trust in personal data management, while simultaneously allowing flexibility for the usage of personal information to stimulate economic growth and recovery.

As such, the Council advocates for the implementation of legislation that promotes transparency of data collection and use; clear governance of the collection and use of personal data for legitimate business purposes; and the development of internationally-accepted data protection standards for operational environments, especially as it pertains to data portability.

COMMENTS ON THE PERSONAL DATA PROTECTION (AMENDMENT) BILL 2020

Section	Summary of Feedback and Recommendations
Amendment of Section 2	• *Definition of 'derived personal data':* Personal data may be derived from a combination of personal data about the individual together with aggregated or anonymised data. The current definition may not cover this use. We recommend that the definition should be extended to any other data elements and not just derived from other personal data about the individual or another individual. "Derived personal data" is defined in the Bill as "personal data about an individual that is derived by an organisation in the course of business from other personal data about the individual or another individual in the possession or under its control". We recommend that the definition include language such that the definition expressly rules out "user activity data" from the scope of "derived data" where there could be possible overlaps. For instance, user activity data is processed and analyzed immediately and could be kept together with or as part of the "derived data" that has been inferred from such analysis (for instance individual health profiles created by the organization could be kept with tracked health information, location, etc.) but that user activity data cannot be considered as derived. As such, we proposed that sub-clause (b) of the definition of "derived personal data" be amended: (b) does not include personal data **as a result of the individual's use of any product or service, or** derived by the organisation using any prescribed means or method;" • *Definition of 'user activity data':* We seek clarification on the definition of "user activity data". "User activity data" is defined in the Bill as "personal data about an individual that is **created** in the course or as a result of the individual's use of any product or service provided by the organisation". The distinguishing element of "user activity data" from "derived personal data" is that while the former is raw original data that is collected consequent to organization's product/service consumption by the individual, the latter (i.e. "derived data") is actually created by the organization on the basis of other personal data either held by the organization or under its control by conducting analysis or other methods, thus resulting in additional data that is not in the original form that was collected. However, the use of the word, "created" (which characteristically means to make something new, or invent something) in definition of "user activity data" can be taken to imply that organization is creating new data by virtue of individual's use of the product/service (which may unintentionally point towards data that is typically analyzed and derived pursuant to user activity).

	"Created" can be proposed to be replaced with "observed", or potentially "collected" or "generated". We note that the Working Party in their Data Portability Guidelines refers to user activity data as "observed data" and has differentiated the two concepts on the basis of data "provided by the data subject". The relevant excerpt below: *A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":* *- Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)* *- Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.* *In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject"* As such, we propose that "User activity data" is defined as "personal data about an individual that is observed in the course or as a result of the individual's use of any product or service provided by the organization".
Mandatory data breach notification requirement	We encourage the introduction of Data Breach Notification (DBN) and suggest that the notifications requirement clarifies the criteria for reportable breaches and provide clear guidelines on the items to be reported. *Notification criteria* • Recommendation: Revise the definition of "data breach" to more clearly state when the DBN should be triggered (proposed Section 26A). MCI/PDPC can consider revising the definition of "data breach" to be more consistent with international practices. For example, the EU General Data Protection Regulations (GDPR) states that " 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." • Recommendation: clarify the meaning of "significant harm" threshold (proposed Section 26B(1)(a)). o The threshold for notification to be based on the likelihood of "significant harm" is unclear. o "Significant harm" introduces a different nomenclature on mandatory reporting compared to existing global regimes (e.g. GDPR Article 35 speaks to notifying individuals if there is a "high risk" to the rights and freedoms of natural persons; Australia speaks to "serious harm"). It is important to clarify and/or define its meaning for compliance purposes. • Recommendation: Remove the notification requirement threshold based on the scale or the number of affected individuals (proposed Section 26B(1)(b)).

	○ Requiring notification of any instance where there is a breach of over 500 individuals could result in the PDPC and individuals being inundated with numerous immaterial notices, risking "notification fatigue" and a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm. For example, an email exposing 501 email addresses in the CC line would be reportable under this threshold. In assessing whether an organization's security practices constitute a "systemic issue within an organization", the PDPC should examine the nature of the security incident rather than the volume of individuals affected. For example, an employee of a company that mistakenly accesses a database of information about 1,000 customers on a single occasion would not suggest systemic issues with an organization. By contrast, the mistaken disclosure of a single patient's medical history through unencrypted channels might suggest systemic issues. In encouraging notification in both instances, PDPC will make it more difficult to distinguish security incidents that create no risk of harm from security breaches that may create a significant risk of harm. We are of the view that having a "significant scale" number arbitrarily defined does not necessarily contribute towards determining whether a data breach event results in "significant harm" to individuals, as should be the more relevant perspective to be considered. This default "significant scale" is also not commonly found in other privacy regimes such as GDPR or the Australia Privacy Act. ○ Moreover, in determining the scale of the breach, please clarify whether there is requirement to aggregate the number of affected individuals from a few separate incidents in different timeframes, if the root cause is the same/similar (e.g. evolved from the same issue). If so, we would suggest that there be a prescribed timeframe for purpose of aggregation of the numbers. • Recommendation: Revise Section 26(D) to make it clear that data intermediaries are not required to notify PDPC and individuals of a "notifiable data breach". While we support the requirement for data intermediaries to notify organizations of data breaches "without undue delay", it should however remain the responsibility of the organization to assess whether a data breach constitutes a "notifiable data breach" and notify PDPC and/or individuals, as the case may be. The current drafting of Section 26(D) is ambiguous as to whether such notification obligations would apply to data intermediaries. We therefore propose amendments to the language to make it clear that this obligation would not apply to data intermediaries. • Recommendation: Revise Section 26C(2) to make clear that data intermediaries do not have the obligation to monitor security breaches that are the responsibility of the main organization (proposed Section 26C(2)). As currently proposed in the Bill, the data intermediary is required to notify the organization without undue delay where it has "reason to believe that a data breach has occurred". The proposed language is overly broad and risks confusing the obligations of the data intermediary and the main organization. The data intermediary's obligation to notify should apply where the data

	intermediary has actual knowledge of a data breach and the breach extends to data or systems over which the data intermediary exercises control and has visibility into. • If intending to apply a "significant scale" criteria, in determining 'significant scale', please clarify whether there is requirement to aggregate the number of impacted individuals from a few separate incidents in different timeframe if the root cause is the same/similar (e.g. evolved from the same issue). If so, there should also be a prescribed timeframe for purpose of aggregation of the numbers. • Clarification is required on whether the requirement to notify the PDPC for any categories of data which are not "whitelisted" will only be triggered based on the scale of the breach (i.e. number of affected individuals). We further seek clarity on the categories of personal data that will deem a breach notifiable. • Clarification is required on the timeline potentially available to an organization to implement appropriate remedial action in order to not be required to notify affected individuals. We seek clarification on whether the requirement to notify individuals as soon as practicable be deferred while an organization determines and then implements remedial action. In addition, we seek clarification on the scope of the exceptions for notifying individuals, particularly the prescribed requirements for actions taken to render the harm unlikely. • We also seek clarification on whether the Bill would allow for partial notification or a withdrawal of a notification if a company does notify within the required timeframe but can withdraw the notification if it turns out that no breach worthy of notification under the PDPA in fact occurs. • 'Health insurance information' is mentioned in the consultation document as a potential category of personal data in future Regulations. 'Health insurance information' is a very wide term, e.g. premium, premium frequency, mode of payment, inception date, date of application, name, NRIC, mobile number, email address, claims incurred date, claims amount, treatment code, and name of healthcare provider. As the purpose of prescribing categories of personal data is related to 'significant harm' to individuals, please consider referring to 'medical information' instead. • "Credit/debit card numbers" is also included as a potential category of personal data that will by default be considered "likely to result in significant harm to individuals". We recommend adopting a principles-based approach and relying on the concept of an appropriate threshold of harm (e.g. serious harm) to the individual, instead of prescribing such default categories. Arguably, there may be circumstances where credit/debit card numbers would not result in "significant harm" to an individual (for example, where these are obsolete credit/debit card numbers). Further, transactions would not be enabled based on credit/debit card numbers alone, without the expiry date and CVV number of the card. As such the risk of unauthorized transactions, in a breach solely relating to credit/debit card numbers, is very low. • The above also sets a poor precedent for making card account data as sensitive data. Such a data classification approach or a "whitelist" of data categories has

	been adopted by other countries for other purposes (e.g. data localization) and this approach would likewise work against Singapore's data hub strategy. *Assessment and notification timeframes* • 3 calendar days may pose a challenge for organizations where there are multiple intermediaries (or sub-intermediaries) which may require the organization to carry out multiple assessments of the nature and impact of the breach before it notifies the PDPC. Requiring notice to any party within 3 days imposes a significant burden on controllers and supervisory authorities alike, especially where there are multiple intermediaries (or sub-intermediaries) which may require the organization to carry out multiple assessments of the nature and impact of the breach before it notifies the PDPC. • Hence, notification should be encouraged "as soon as practicable" or "without undue delay" from the completion of all relevant assessments. We recommend avoiding introducing arbitrary timelines, which may not be commensurate to the time and resources required for investigation and remediation of breaches, which vary in size, severity and complexity. • If a timeline is specified, then we encourage that this should be working days rather than calendar days, which is consistent with contracts between private sector companies (e.g. organizations and their intermediaries) and other regulatory reporting which usually use 'business days' requirements, for example: o Fraud notification to MAS (MAS Notice 123 Notice on Reporting of Suspicious Activities & Incidents of Fraud) provides for 5 working days after the discovery of the activity or incident by the registered insurer. o Suspicious Transaction Reporting to CAD (Guidelines to MAS Notice 314 Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Life Insurers, Guidelines to Notice FAA-N06 on Prevention of Money Laundering and Countering the Financing of Terrorism and Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism – Direct General Insurance Business, Reinsurance Business, and Direct Life Insurance Business) - A Suspicious Transaction Report (STR) should be filed within 15 business days of the case being referred by the relevant officer, employee or agent. • When considering subsequent Regulations as to "significant scale" of instances whereby notification to PDPC is necessary, as well as where notification to PDPC is required if such breach results, or is likely to result, in significant harm to individuals, PDPC should consider removing the requirement for notification where the remedial action or technological protection exceptions are applicable to minimize the risk of harm (i.e. the exceptions should apply to notification requirements to PDPC as well as individuals). This is to avoid "notification fatigue" to PDPC as described earlier, and to allow organizations to expend their time and resources for investigating and remediating the breach instead.

	• While a data intermediary is required to notify an organization without undue delay, to avoid uncertainty there should be further clarification (perhaps in the subsequent Regulations) as to what would be considered undue delay and whether an intermediary is permitted to conduct any internal assessment or remediation before notifying an organization. • Clarify the scope of the exceptions for notifying individuals, while maintaining flexibility for organisations (proposed Section 26D). The scope of the exceptions for notifying individuals of a data breach is not clear, especially in relation to the actions that the organisation must have taken, or the technological measures that the organisation had implemented, as to render it unlikely that the data breach will result in significant harm to the affected individual(s). We welcome additional clarity on these requirements and recommend that they are not overly prescriptive and technology agnostic to maintain flexibility for organisations operating under different circumstances and having different processes and resources. Further, it is recommended that the requirements are set out as guidance rather than legislative requirements in order to maintain flexibility over time. *Removal of exclusion for organizations acting on behalf of public agencies* • Recommendation: Sections 24 and 25 of the PDPA, should be further amended to make clear that where the relevant processing activity relates to a data intermediary acting on behalf of and/or for the purposes of a public agency, that such reasonable protection or retention should be in accordance with their contractual arrangements, and/or any other applicable law or regulation. • The removal of the exclusion for organizations acting on behalf of public agencies is confusing as it is unclear whether a data intermediary would reasonably be able to take on its relevant obligations (i.e. retention and protection), given that the organization it is acting on behalf for (i.e. public agencies), is not subject to the PDPA. *Offences relating to egregious mishandling of personal data* • The imposition of criminal sanctions on individuals requires careful consideration, particularly if it is based on wider criteria that includes "knowing" mishandling of data instead of just "reckless" mishandling of data. Criminal sanctions are out of step with global legislation such as the GDPR. A Personal Data Protection law should impose fines for violations of its provisions rather than criminal penalties. If such penalties are necessary, they should be added to the criminal code rather than the PDPA. • Clarification is required on why Section 35C(d)(ii) specifies individual gain or the causing of harm/loss to another as a factor in whether misuse of data is an offence given that this is not a factor in any unauthorized disclosure or re-identification of data under Section 35B or 35D. • The civil suits or other forms of dispute resolution may take a long time to complete or may be withdrawn (e.g. settlement between parties). This will prejudice the 'victims' where their personal data had been disclosed without

	their consent. PDPC should consider dealing with the PDPA offences separately, regardless of private law recourse. This will send a strong message to prevent egregious mishandling of personal data by individuals.

Enhanced framework for collection, use and disclosure of personal data	*Expanding deemed consent*
	
	• We support the proposals for deemed consent for contractual necessity and where notification is provided as they strike the right balance between allowing the use of personal data in the ordinary course of business and empowering individuals to control their data. Clear statutory language would also improve on the schedules contained in the current PDPA.
	• The opt-out requirement (in proposed Section 15A(3)(b)(iii)) should only be provided where feasible. Deemed consent by notification is likely to be relied on by organisations where it may not be practicable to obtain consent. Under the same circumstances it is likely that it also may not be practicable to provide the individual with an opportunity to opt out. Accordingly, organisations should only be required to allow individuals a reasonable time to opt-out, where it is feasible to do so. This is consistent with the PDPC's position in its Public Consultation for Approaches to Managing Personal Data in the Digital Economy, where it was proposed that "where feasible, organisations must allow individuals to opt out…".
	• We would welcome further clarification on the concept of "reasonable necessity", including its meaning and application in the Bill and subsequent Regulations and/or new Guidelines. Where global businesses are concerned, it is often necessary to rely on outsourced service providers and specialist services to benefit from economies of scale and leverage international best practices. It is respectfully submitted that the concept should be wide enough to embrace the various value/supply chain partners essential to the performance of the contract.
	
	New exceptions
	
	• We similarly support the exceptions to obtaining consent for legitimate interests and business improvement.
	• The exceptions for consent requirement should be wide enough to cover commercial purposes beyond market research such as:
	  ○ (1) Use Case 1- Intermediary providing Data Services: Organization provides consumer / transaction data with opt-in/opt-out details. Intermediary utilizes data (with applicable opt-in) or aggregated data to build data science solutions/dashboards for the organization.
	  ○ (2) Use Case 2 - Intermediary-developed data solutions: Intermediary uses customer transactional data to build a Data Science Model/Capability without access to personal data. Intermediary then uses this model to deliver behavioral/predictive scores for customers to the organization. In the absence of consent, organization relies on business improvement or research exceptions to deliver benefits to the customer based on the score/insight provided by the model.

	• Clarification is required on the extent to which the new exceptions for legitimate interests and business improvement can be relied upon by an intermediary, and whether these exceptions only apply to the legitimate interests of, or business improvements by, the organization which has collected the data. In some instances, the interests of the organization and the intermediary may be aligned e.g. both have a legitimate interest in trying to detect and prevent fraud. But could an intermediary rely on the business improvement exception to improve its own processes or develop new products? Similarly, can an intermediary participate in broader research efforts relating to personal data which do not include the collecting organization? • The "legitimate interests" exception to consent should include the legitimate interests of a third party (as proposed in Section 31 of the Bill). The proposed exception is limited to the legitimate interests of the organisation, and not of a third party. This should be broadened to include consideration of a third party's interests, for consistency with the position under GDPR. ○ Recommendation: Align the assessment for relying on the "legitimate interests" exception with the internal assessment for deemed consent by notification. To rely on legitimate interests as an exception to consent, organisations are required to conduct an assessment such that the benefit to the public (or a section thereof) of the collection, use or disclosure of personal data is greater than any adverse effect on the individual. The assessment must include the identification of any adverse effects on the individual, measures to eliminate the adverse effect or if not possible, to reduce or mitigate the effect. This appears to be a more stringent assessment than the assessment required for deemed consent by notification. Accordingly, we recommend that the same assessment is applied for both deemed consent by notification and for legitimate interests, so as to avoid confusion for organisations. • Recommendation: Clarify that the "business improvement" exception to consent applies across all group entities (as proposed in Section 32 of the Bill). The Public Consultation Document states that the exception applies to a group of companies, however this does not appear to be reflected in the Bill. • Clarification is also requested with respect to the need for organizations to "disclose their reliance on legitimate interests to collect, use or disclose personal data." We are of the view that for 'legitimate interests exception', it is not necessary to disclose this as long as the organization has sufficient justification. This would also be in line with the accountability approach. • Further, we recommend PDPC to provide practical examples in the upcoming guidelines to clarify situations which could be categorized as reliance on "legitimate interests" and "business improvement" exceptions respectively. For instance, an example on processing personal data for information security purposes and for fraud prevention would be a legitimate interest. We note that the GDPR provides a legal basis for processing personal data to ensure network and information security. This is a broadly recognized legitimate interest specifically called out in the GDPR Recital 49. • The amendments appear to require opt-in consent to the use of personal data for direct marketing. We would propose that this data be subject to opt-out.

	Businesses should be able to communicate with their customers about new products and offers, as this is an ordinary business function which presents low (if any) risk to individuals. An opt-out also seems more consistent with the proposals to improve controls for unsolicited commercial messages.

Data Portability Obligation	• Recommendation: Broad data portability requirements should not be mandated. A broad implementation of the data portability right may stifle competition and innovation and impose unnecessary burdens on organizations.
	  ○ If MCI/PDPC nonetheless proceeds with mandating data portability, we recommend that the "whitelist" of data categories be narrowly scoped to meet the purpose of allowing individuals to switch to new service providers more easily.
	  ○ Further, we recommend that any direct service-to-service portability is limited to where it is "technically feasible". This is because it may not always be technically feasible to provide data directly to other service providers, and is in line with the approach under GDPR. Nevertheless, it is worth noting that companies involved in the Data Transfer Project are working to address interoperability issues by creating an open source platform to allow users to more easily move their data between online service providers.
	  ○ We also recommend that the "whitelist" of data categories exclude types of data that provide no clear value to individuals' ability to switch providers, and/or take time for organizations to process, including (i) user activity data generated from the use of proprietary tools or features, (ii) user-generated content (such as voice recordings, videos, images, customer reviews and feedback), and (iii) unstructured data.
	  ○ The portability obligation should ensure a level playing field between the entities obliged to share the data (data transmitters) and those with whom the data should be shared (data receivers), so that information can port in both directions. An absence of bidirectional flows of data has the potential to create competition concerns and so it is key that the principle of reciprocity be embedded within the data portability framework.
	• The Bill should expressly state that the exceptions in the Fifth Schedule of the PDPA apply to the data portability obligation (i.e. an organisation is not required to comply with a data porting request in respect of the matters set out in the Fifth Schedule). This is stated in the Public Consultation Document, but does not appear to be reflected in the Bill. This will provide certainty and consistency in the implementation of the new provisions.
	• The subsequent Regulations should also allow flexibility for organisations to prescribe certain requirements themselves, for example in relation to data porting requests, technical and process requirements for porting, etc.
	• It would also be helpful if the Act, subsequent Regulations and/or new Guidelines could provide for, or clarify, the following:
	  ○ (a) A porting organization shall have no legal liability to the receiving organization for the personal data. This is because (i) there is no

	contractual nexus between the parties, and (ii) an organization that collects and uses personal data assumes responsibility for the personal data, including verification of the personal data and having to comply with the Accuracy Obligation under the PDPA. ○ (b) A transmitting organization reserves the right to reject a porting request "if the request is otherwise frivolous or vexatious". (This is similar to the Access Obligation and PDPC's current advisory guidelines on individual's access to their personal data) ○ (c) A receiving organization shall have a right to refuse ported data, if the personal data is (a) not necessary for the conclusion of an agreement, performance of an agreement or the relationship between the receiving organisation and the individual, or (b) not relevant for the purposes of the receiving organisation. This is because the receiving organization remains responsible for complying with the requirements under the PDPA when collecting personal data, including verification of consent or such other legitimate purposes and ensuring accuracy of the personal data from the relevant individual. • We also request that MCI/PDPC commits to consulting with industry prior to the development of prescribed requirements in the subsequent Regulations, and the new Data Portability Obligation coming into effect. The various facets of data portability, including the types of data involved, the industries involved and the responsibilities incumbent on such companies should be thoroughly assessed prior to the implementation of any mandatory data portability requirements. ○ For the financial services sector, there needs to be greater clarity around defined roles and obligations of data holders, data requesters and data intermediaries (e.g. data processors that conduct certain functions between data holders and data requesters). ○ In aligning cybersecurity requirements for data portability, we request industry consultation to support internationally-accepted standards for areas such as transfer protocol, authentication protocol, etc. • Clarification is requested regarding: ○ The basis on which the PDPC envisages extending data portability obligations to like-minded jurisdictions with comparable protection and reciprocal arrangements. ○ The extent to which the PDPC expects the data portability obligation to be applicable outside of Singapore (Section 26E indicates that this will be applicable to data porting requests regardless of whether the applicable data is stored or processed in, or transmitted from, Singapore or some other country). ○ Whether the PDPC expects to include, as part of any data portability obligation Regulations, more detailed requirements as to protection of such data (e.g. Australia's OAIC regulations in relation to CDR). ○ The extent to which intermediaries are required to comply with any data portability obligations, as well as further details on the potential role(s) which PDPC envisages that intermediaries play within the data porting process.

	○ Whether the subsequent data portability obligation Regulations will provide further details as to the scope of what will be excluded from the definition of "derived personal data" being added to Section 2.1(a) of the PDPA.
Improved controls for unsolicited commercial messages	• US-ABC supports the objective of providing consumers with greater control over the unsolicited commercial messages they receive, including through robocalls. This will provide consumers with confidence in using communications, messaging, email, and other cloud-enabled services. • Equally important, however, is to ensure that cloud services providers, whose services may be used by the parties sending the unsolicited messages, are not inadvertently presumed to have breached the improved controls the Bill would introduce for unsolicited commercial messages (as discussed in paragraphs 53 and 54 of the Consultation Paper). • We note that in the current Part IX of the PDPA, Section 36(2) of the PDPA expressly clarifies that "*[f]or purposes of this Part, a telecommunications service provider who merely provides a service that enables a specified message to be sent shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorized the message to be sent.*" We view this as an important clarification that must also be included in the proposed new Part IXA of the PDPA. If this clarification were not included in the proposed new Part IXA of the PDPA, then an ordinary statutory interpretation would lead to the conclusion that the policy intent is for the service providers, who would have been covered by the clarification in Part IX of the PDPA, not to be able to benefit from the same clarification for purposes of the proposed new Part IXA of the PDPA. • We also note that in the Spam Control Act (**SCA**), Section 12(2) of the SCA provides that "*[a] person does not contravene …[the prohibitions against sending, causing to be sent, or authorizing the sending of electronic messages in Sections 9 and 11 of the SCA] merely because he provides, or operates facilities for, online service or network access, or provides service relating to, or provides connections for, the transmission or routing of data.*" However, it would be preferable for an explicit clarification that the service providers in question are not presumed to have sent the messages in question. • US-ABC therefore recommends adding a new Section 48A(3) to the PDPA that reads as follows: "For the purposes of this Part, a telecommunications service provider who merely provides a service that enables an applicable message to be sent shall, unless the contrary is proved, be presumed not to have sent, not to have caused to be sent, and not to have authorised the sending of, the message." • We also recommend adding a new Section 12(3) to the SCA that reads as follows: "(3) Without affecting subsection (2), and for the purposes of Sections 9 and 11, a person who merely provides a service that enables the message or the messages to be sent shall, unless the contrary is proved, be presumed not to have sent, not to have caused to be sent, and not to have authorised the sending of, the message or the messages."

Increased financial penalty cap	• Recommendation: Deletion of "10% annual gross turnover".
	  ○ Civil penalties should not be tied to a regulated entity's turnover, and should be proportionate to the harm caused to the data subjects and whether there are any aggravating or mitigating factors. Civil penalties frameworks should also not impose undue hardship on an otherwise responsible entity.
	  ○ The suggested financial penalty cap also potentially discourages companies from carrying out business activities in Singapore, including the setting up of global or regional headquarters, or locating data hubs in Singapore, thereby potentially creating a chilling effect on innovation and investments by businesses in Singapore.
	  ○ If PDPC nonetheless imposes the revenue-based maximum financial penalty, then the Bill should clarify that the cap is based on turnover "in Singapore", which would reflect PDPC's intention as stated in paragraph 58 of the Public Consultation document. To avoid penalising organisations that act in good faith, PDPC should also consider introducing a provision that it may impose a financial penalty only if the infringement has been committed intentionally or negligently, similar to section 69(3) of the Competition Act.
	  ○ As an extension of the 'proportionate harm' argument, it should be noted that regulated entities may undertake activities outside Singapore where the PDPA may not apply. In such event, applying an entity turnover assessment would not be fair where part or most of the turnover is derived from such other jurisdictions.
	• Clarification is also required (presumably in the subsequent Regulations) on applicable penalties or other enforcement actions for any failure by (i) an organization to notify the PDPC and/or affected individuals and (ii) an intermediary to notify an organization.

Voluntary undertakings	• Recommendation: PDPC should further clarify that voluntary undertakings, are undertakings that are proposed by an organization or person, and such undertakings (including any variations) will not be imposed by the PDPC, without prior agreement from the relevant organization. • In addition, given the requirements that failure to "comply with an undertaking" could result in the voluntary undertaking being publicized and cost recovery (proposed Section 31A(5) – we also recommend that PDPC avoid mandating that organizations or persons be subject to the voluntary undertaking mechanism – and provide organizations or persons the ability to reject such a proposed undertaking, without prejudice.