PDPC'S PUBLIC CONSULTATION ON MANAGING UNSOLICITED COMMERCIAL MESSAGES AND THE PROVISION OF GUIDANCE TO SUPPORT INNOVATION IN THE DIGITAL ECONOMY

A RESPONSE
FROM
BSA | THE SOFTWARE ALLIANCE AND US-ASEAN BUSINESS COUNCIL

7 JUNE 2018

Contacts:

BSA | The Software Alliance
Darryn Lim,
Director, Policy - APAC
darrynl@bsa.org
300 Beach Road, #25-08 The Concourse,
Singapore 199555

US-ASEAN Business Council:
Shay Wester
Director, Trade & Industry
swester@usasean.org
100 Beach Road, #22-04/05 Shaw Tower
Singapore 189702

INTRODUCTION AND STATEMENT OF INTEREST

BSA | The Software Alliance ("**BSA**")[1] and the US-ASEAN Business Council ("**US-ABC**")[2] greatly appreciate the opportunity to provide comments to the Personal Data Protection Commission ("**PDPC**") on the Public Consultation on Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy issued on 27 April 2018 (the "**Consultation Paper**").

The members of our organizations are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things, among others. Our members remain deeply committed to protecting personal data across technologies and business models in order to ensure that consumers and businesses alike can trust in and reap the maximum benefits across such technologies and business models.

Our organizations have worked closely with governments around the world in relation to the development of national personal data protection policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively protect the privacy and civil liberties of citizens without hindering innovation and technological advancement.

To share learnings from this experience, BSA has published the BSA Personal Data Protection Principles ("**Principles**"), which set out a recommended model for a national personal data protection policy. US-ABC supports the Principles. A copy of the Principles is attached.[3]

We wish to commend the PDPC for its ongoing efforts in reviewing the Personal Data Protection Act ("**PDPA**") and the overall data protection regime in Singapore to ensure its relevance in the face of a changing digital landscape, and to provide greater certainty to organizations which are subject to its regulations.

In support of these efforts, and based on feedback from our members, we provide the following comments on the issues raised in the following parts of the Consultation Paper:

- Part III: Enhanced Practical Guidance
- Part IV: Second, Third and Fourth Schedules to the PDPA

A. COMMENTS ON PART III OF CONSULTATION PAPER: ENHANCED PRACTICAL GUIDANCE

We support the PDPC's proposal to introduce a new Enhanced Practical Guidance ("**EPG**") framework as set out in Part III of the Consultation Paper. Whilst we recognize the value of the

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations ("ASEAN"). Worldwide, the council's 150-plus membership generates over $6 trillion in revenue and employs more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The council has offices in Washington, DC; New York, New York; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

[3] The Principles can also be found at http://bit.ly/BSA-Data-Protection.

existing resources issued by the PDPC in the form of advisory guidelines and guides, we agree with the PDPC's observations in paragraph 5.3 of the Consultation Paper that there is a "gap for addressing complex compliance queries" with regulatory certainty.

Having reviewed the details of the proposed EPG framework, we would also like to make the following suggestions for further improvement.

A1. Greater clarity needed on the criteria for assessing requests for determinations

We request greater clarification on the proposed criteria for assessing requests for determinations, as set out in paragraph 6.2 of the Consultation Paper. In particular, we are concerned that the third criteria that "the query does not amount to a request for legal advice" may be confusing and could easily be interpreted too broadly.

We recognize that the PDPC is not a provider of legal services. However, the very nature of the EPG framework involves a determination by the PDPC on a matter of law, namely whether a particular business activity is in breach of the PDPA. While the PDPC has clarified that requests relating to the Protection Obligation will not be accepted, this is not an exhaustive list and still leaves some uncertainty over the parameters of this requirement.

Accordingly, we recommend that the PDPC remove this condition or provide further examples of what would constitute a "request for legal advice".

A2. Categories of those who may request determinations should be clarified

In paragraph 6.1 of the Consultation Paper, it is stated that requests for determinations must be from the organizations performing the business activity for which guidance is sought. **We request clarification from the PDPC on whether professional advisors, such as lawyers, may submit these requests for determinations on behalf of organizations.** In practice, we are aware that many companies would prefer to route these requests through their lawyers.

We also wish to understand if industry bodies such as BSA and US-ABC will be permitted to submit a request on behalf of their members. Our members often have queries in common, and a consolidated request for a PDPC determination by an industry body representing members' interests may be more efficient for the PDPC. In today's fast-paced world of innovation, questions relating to technology such as artificial intelligence may be sufficiently complex or novel enough to warrant a determination by the PDPC without necessarily being unique to any one organization.

Additionally, **we request clarification on whether requests for determinations can be submitted in respect of activities that organizations are *intending to* (but have yet to) perform.** Such determinations would provide regulatory certainty to organizations looking to implement novel business and/or technological initiatives that involve the handling of personal data, where the position under the PDPA and/or guidelines may be unclear. While this aligns with the objectives in paragraphs 5.3 and 6.5 of the Consultation Paper, in that the EPG framework is "intended to support organisations with innovative solutions", it is unclear if requests for such determinations would be precluded by paragraph 6.1 of the Consultation Paper, which states that the PDPC will not "provide determinations to queries relating to hypothetical situations."

A3. Risk of fragmented regulatory regime should be addressed

We support measures that reduce ambiguity for organizations, and we commend the PDPC's efforts at achieving this aim through the EPG framework. However, we recommend that clearer parameters on the nature and effect of determinations be set out.

As presently drafted, the EPG framework carries a risk that a fragmented regulatory regime may emerge with an imbalance of knowledge on what constitutes a breach of the PDPA. In paragraph 5.2 of the Consultation Paper, the PDPC has indicated that the determinations will have regulatory certainty. However, the determinations are also organization-specific and may not always be published, as set out in paragraph 6.7 of the Consultation Paper.

By way of example, an organization that has obtained a determination would know that its conduct is permitted, whereas another organization that may have interpreted such conduct as a breach of the PDPA and not proceeded with it would not have this knowledge available to it for as long as that determination remains unpublished.

We therefore recommend the following:

- **Determinations should be published unless specific, defined conditions are met.** Instead of publishing determinations on a case-by-case basis, we recommend that determinations only *not* be published where specific, defined conditions are met. For example, where such publication poses a material risk: (a) of a breach of confidential information; (b) of infringing and intellectual property rights (for example revealing details of a patent prior to filing); or (c) to national security. In all other situations, the default approach should be to publish each determination (with any commercially sensitive information redacted).

- **The PDPC should, as a minimum, commit to continuously update the practical guidance it publishes to take into account the salient points of each determination issued**. While we recognize the need to keep commercially sensitive information confidential, we also strongly advocate that regulations should be transparent to all to ensure fairness.

A4. Failure to seek a determination should not adversely affect subsequent investigations

We agree with the PDPC's proposal to not initiate investigations into an organization where it finds any non-compliance in the course of providing a determination. We also support the proposal that the PDPC will not use any information provided by the organization for the EPG assessment as part of its investigations. Such measures are important to foster trust and use of the EPG framework.

To further bolster confidence in the EPG framework, **we recommend that the PDPC clarify that no adverse inference will be drawn during any PDPC investigation from a prior failure by an organization to seek a determination.** As the EPG framework is entirely optional, the PDPA should not penalize organizations that do not avail themselves of it.

Without such an assurance, there may be an increase in the number of requests for determinations from organizations for whom the framework is not intended, simply as a risk-

mitigation strategy. We understand that such unintended consequences would not align with the goals of the framework.

B. COMMENTS ON PART IV: SECOND, THIRD, AND FOURTH SCHEDULES TO THE PDPA

We support the retention of the current exceptions to the obligation to obtain consent for the collection, use, and disclosure of personal data. We also recommend that the PDPC incorporate additional exceptions, as set forth below, to provide greater clarity and to reflect the realities of how companies operate in the digital economy.

B1. Existing exceptions in the Second, Third, and Fourth Schedules should be retained

We are in favor of retaining the existing exceptions set out in the Second, Third and Fourth Schedules of the PDPA.[4]

The flexibility offered by the existing exceptions has been key to ensuring that organizations are able to use the personal data they hold without incurring exorbitant compliance costs. The existing exceptions strike an appropriate balance to ensure that businesses and individuals in Singapore can avail themselves of the opportunities presented by the digital economy, whilst at the same time ensuring that their privacy is not ignored. For example, by allowing the collection of personal data without consent where it is publicly available, the PDPA facilitates the innovative use of the vast amounts of publicly available datasets for data analytics that power artificial intelligence solutions.

We recognize that data increasingly powers the modern, digital economy, and drives innovation in areas such as artificial intelligence and the Internet of Things. As such, a flexible data innovation policy is necessary to guard against privacy risks whilst ensuring Singapore maintains its competitive edge.

B2. Additional exception for performance of contractual obligations should be included

In line with the Principles and with other data protection laws around the world, such as Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and the European Union's General Data Protection Regulation ("**GDPR**"), **we recommend including in the Second, Third, and Fourth Schedules an exception to allow an organization to collect, use, and disclose personal data without consent to perform its obligations under a contract with the relevant individual or with a third party at the individual's request**.

We consider that, as this is a largely uncontroversial purpose that would benefit both individuals and companies, introducing an exception that applies under these circumstances would be appropriate. For example, this exception may apply where an individual makes an online purchase and the organization needs to use the individual's address in order to deliver the goods. Some processing of data is necessary in order to perform the contract.

[4] We nonetheless suggest clarifying the drafting in the Second, Third, and Fourth Schedules of the PDPA to remove circular references. For example, section 17 of the PDPA references the Schedules and the Schedules also contain references to section 17, creating some circularity in the PDPA.

At present, there is no clear exception provided for this situation or similar circumstances, and organizations are expected to obtain the individual's consent, unlike in relation to the transfer of personal data overseas (see regulation 9(3)(b) of the Personal Data Protection Regulations 2014). This commonly results in complex contractual provisions or privacy policy statements to ensure compliance with the PDPA.

This exception is also found in other personal data protection regimes, such as the GDPR, and is further supported by other laws, such as PIPEDA, that more broadly provide exceptions to consent obligations where the collection or use of the information is clearly in the individual's interests and consent is not available in a timely way.

We understand from the PDPC's earlier Response to the Public Consultation on Approaches to Managing Personal Data in the Digital Economy issued on 1 February 2018[5] that the PDPC is currently reviewing other bases for the collection, use, and disclosure of personal data and intends to include a new "legitimate interests" basis. We support the inclusion of the "legitimate interest" basis, as referenced in our comments of 4 October 2017 on the PDPC's Public Consultation for Approaches to Managing Personal Data in the Digital Economy,[6] and also wish to highlight that the PDPC could consider including the proposed "contractual obligation" exception above as an additional *basis* of collection, use, and disclosure of personal data rather than an *exception,* as the practical effect for organizations would be the same. Our primary interest is that Singapore's personal data protection regime remains sufficiently flexible so that it ensures proper safeguards for personal data while being conducive to innovation and the growth of the digital economy.

CONCLUSION AND NEXT STEPS

BSA and US-ABC once again express our support of the PDPC's efforts to continually review and update the personal data protection regime in Singapore to respond to the ever-evolving needs of the digital economy. We request that the PDPC consider the suggestions above to ensure that Singapore continues to protect the rights of individuals and their personal data whilst remaining a hub of cutting-edge technological development.

We remain open to further discussion with you at any time. Please do not hesitate to contact us for any further information on the contents of this submission. Thank you.

Yours faithfully,

BSA | The Software Alliance and **the US-ASEAN Business Council**

Attachment: BSA Personal Data Protection Principles

[5] Available at https://www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations#ACTR1.

[6] Our comments of 4 October 2017 are available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Responses-Received-as-at-5-October-2017/softwarealliancebsaandtheusaseanbusinesscouncilusabc.pdf. We also reiterate our encouragement for the PDPC to clarify, when amending the PDPA to include the "legitimate interests" basis, that the purposes for which personal data can be collected, used, disclosed, or otherwise handled under this basis includes, but is not limited to: (a) fraud detection and prevention; (b) administration and analyses within a group of affiliated organizations for internal purposes (including to improve operational efficiencies and provide internal training); and (c) ensuring network and information security. These clarifications are expressly provided for in recitals 47, 48, and 49 of the GDPR.

BSA PERSONAL DATA PROTECTION PRINCIPLES

BSA | The Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. Our member companies are at the forefront of data-driven innovation. BSA members have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models. We recognize the importance of fostering trust and confidence in the online environment. As a global organization, BSA actively follows privacy developments around the world. An effective privacy regime protects consumers without hampering innovation and leverages the power of the digital economy to support governments and businesses alike.

BSA provides these Personal Data Protection Principles to advance the development of effective privacy and personal data protection regimes internationally. The Personal Data Protection Principles rest on five Pillars of Personal Data Protection.

PILLARS OF PERSONAL DATA PROTECTION

1. Scope and Definition of "Personal Data"
2. Collection, Use, Processing, and Disclosure of Personal Data
3. Allocation of Obligations and Liability
4. International Data Transfers
5. Personal Data Breach Notifications

1. Scope and Definition of "Personal Data"

PRINCIPLE

Definition of "Personal Data" should be reasonably linked to an identified or identifiable natural person.

RATIONALE

As any government seeks to protect individuals' personal data, it should also ensure that the scope of information included within the definition of personal data is information that, if mishandled, would have a meaningful effect on an individual's privacy.

If the scope is not limited, and stringent legal obligations apply to a broad range of data regardless of its context and the risk of harm to users, the law is likely to have a chilling effect on data-driven innovation, negatively affecting economic growth.

Any proposed legislation should also recognize that anonymized data, which is not linkable to a specific individual and, therefore, does not implicate privacy concerns, should be excluded from the definition of personal data.

According to international best practices, the legal bases for handling personal data could include, among other things, the legitimate interest of the data controller or third party, the consent of the data subject, compliance with legal obligations, and performance of a contract with the data subject.

2. Collection, Use, Processing, and Disclosure of Personal Data

PRINCIPLE

The legal bases for collecting, using, processing, and disclosing (collectively, "handling") personal data should be sufficiently flexible so that they both ensure appropriate safeguards for personal data and allow businesses to continue to provide innovative services and stimulate economic growth.

RATIONALE

The legal framework for personal data protection should provide protections that meet, and are appropriate to, consumer expectations, without unnecessarily stifling economic growth through the data economy. According to international best practices, the legal bases for handling personal data could include, among other things, the legitimate interest of the data controller or third party, the consent of the data subject, compliance with legal obligations, and performance of a contract with the data subject.

Legitimate Interest

The legitimate interest legal basis for handling personal data would create the flexibility that companies need to carry out their business operations. For example, businesses may need to handle personal data as part of network security or fraud prevention efforts.

The legitimate interest legal basis also serves a particularly important role where it may not be suitable or practicable to obtain consent, or where it is premature to enter into a contract with the data subject. For example, if a financial institution is seeking to recover an outstanding debt and needs to collect, use, process, and/or disclose personal data as part of the debt-collection process (e.g., to debt-collecting agencies), it may not be suitable to request the data subject's consent to do so, but there is a legitimate interest that would justify the handling of the personal data.

As long as the data subject's fundamental rights and freedoms are respected, legitimate interest should be accepted as a valid basis for handling personal data.

Consent

Consent is another important basis for handling personal data. The standard for obtaining consent should be contextual to determine the level of consent that is appropriate.

In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate. In today's world, a large amount of data is created through individuals' interactions with Internet-connected devices, and express consent is not suitable or practical in all instances. For example, the future of public transportation services may be affected if an individual must provide express consent to allow an electronic gate to generate data every time he or she swipes a public transportation card. In other circumstances, such as the handling of sensitive health or financial data, affirmative express consent may be appropriate. Any proposed legislation should consider this context and allow sufficient flexibility for determining the timing, standard, and mechanism for obtaining consent.

Relying solely on explicit written consent as a legal basis for handling personal data would create two risks: (1) stymying growth and innovation in the digital economy; and (2) not meeting consumer privacy expectations by leading consumers to "click fatigue," where users simply accept whatever terms are presented to them without fully reviewing or understanding the information presented to them.

Compliance with Legal Obligations

Companies should also be able to handle personal data to comply with legal obligations. Businesses are subject to a wide range of legal obligations, including financial reporting rules, other regulatory requirements, and obligations arising from court proceedings. In some instances, companies must handle personal data to satisfy these legal obligations. Any privacy framework should ensure that companies can continue to comply with these requirements.

Contractual Performance

Similarly, companies should be able to handle personal data to perform contracts with the data subject. For example, a company may need to handle personal data to fulfill a product shipment ordered by an individual, or to open accounts at the request of the data subject.

The seamless transfer of data across international borders is critical to cloud computing, data analytics and other modern and emerging technologies and services. An effective personal data protection law should ensure that global data transfers continue.

Other Bases

In addition to the foregoing examples, there are several other potential circumstances that could serve as valid legal bases for handling personal data, including performance of tasks in the public interest and protecting the vital interests of data subjects. We recommend that governments adopt a flexible approach that both protects individuals' privacy and preserves companies' ability to carry out their legitimate business operations and provide innovative services to consumers.

3. Allocation of Obligations and Liability

PRINCIPLE

Responsibilities of "data controllers" and "data processors" should be clearly defined.

RATIONALE

The primary obligation for ensuring compliance with the applicable personal data protection law should fall on the "data controller." The "data processor" should only be concerned about complying with the instructions of the data controller, and to ensure the security of the data they process. The relationship between the data processor and data controller should be governed by contractual relationships they have formed.

This clear allocation of responsibility and liability is critical and ensures that the increasingly widespread practice of outsourcing does not insert confusion in the system. This allocation allows the data subject and the legal authorities to know who to turn to in case of a problem, and companies to have clarity on their roles and responsibilities.

Imposing direct, joint, or several liabilities or other obligations on data processors would have a range of unintended consequences, would undermine the relationship between these actors and would create an unjustified compliance burden. In addition, this could also have a negative effect on potential investments in data processing and outsourcing services.

In short, data controllers should have the primary obligation for ensuring compliance with applicable privacy law, whereas data processors should only be required through contractual mechanisms to comply with data controller instructions and to ensure the security of the data they process.

4. International Data Transfers

PRINCIPLE

The law should ensure the free flow of data across borders and avoid requirements that impose unnecessary or burdensome restrictions on global data transfers.

RATIONALE

The seamless transfer of data across international borders is critical to cloud computing, data analytics and other modern and emerging technologies and services that underpin the global economy. An effective personal data protection law should ensure that global data transfers continue.

The accountability model, first established by the OECD[1] and subsequently endorsed and integrated in many legal systems and privacy principles, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows.

The accountability model requires organizations that collect personal data to be responsible for its protection, no matter where or by whom it is processed. As such, any organizations transferring personal data must take steps to ensure that any obligations — in law, guidance or commitments made in privacy policies — will be met.

International data transfers are often made with commitments assumed in international cooperation agreements — including international industry codes of conduct or frameworks developed through open, multi-stakeholder processes — which provide additional assurances that companies will appropriately safeguard personal data.

Furthermore, as part of ensuring the free flow of data, the law should prohibit data localization requirements for both the public and private sectors, which can frustrate efforts to implement security measures, impede business innovation and limit services available to consumers.

1 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

5. Personal Data Breach Notifications

PRINCIPLE

Personal data breach notification requirements should be reasonable and appropriate and cover only situations where there is a material risk of harm to affected individuals.

RATIONALE

The creation of a personal data breach notification system applicable to all businesses and organizations would provide incentives to ensure robust protection for personal data, while enabling data subjects to take action to protect themselves in the event their data is compromised.

However, in creating such a system, it must be recognized that not all personal data breaches represent equal threats. In many instances, the breaches pose no actual risks to the individuals whose personal data was affected.

The notification requirements in the event of a personal data breach should therefore be carefully crafted to prevent the issuance of immaterial notices, principally by ensuring that notification is only required where there is a material risk of identity theft or economic loss to the user. Furthermore, it should also exclude from the notification obligation all instances where the personal data in question has been rendered unusable, unreadable, or indecipherable to an unauthorized third party through any practice or method that is widely accepted as effective industry practices or industry standards (e.g., encryption).

To ensure that data subjects receive meaningful notifications in the event of a personal data breach, it is also critical that data controllers and data processors are afforded adequate time to perform a thorough investigation to determine the scope and effect of the breach and prevent further disclosures. We recommend using a standard that is flexible such as "as soon as practicable" or "without undue delay" instead of specifying an arbitrary, fixed deadline for providing notification.

Data is now emerging as one of the most revolutionary forces for economic gains. We hope these Principles will assist governments worldwide in the development and implementation of effective personal data protection policies and privacy rules that protect consumers' personal data and also shape the growth of an emerging data-centric economy.

About BSA | The Software Alliance

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation and Workday.

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072
@BSAnewsAPAC

BSA Europe, Middle East & Africa

65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

+44.207.340.6080
@BSAnewsEU