

**PUBLIC CONSULTATION ISSUED BY
MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS**

PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

13 SEPTEMBER 2011

PART I: INTRODUCTION	Page 1
PART II: BACKGROUND A) Overview of Current Data Protection Regime B) Need for General Data Protection Regime	Pages 2 - 4
PART III: PROPOSED CONSUMER DATA PROTECTION FRAMEWORK A) Key Objectives and Principles B) Scope of Coverage C) Rules and Exclusions	Pages 4 - 23
PART IV: IMPLEMENTATION A) Penalty and Enforcement Regime B) Regulations, Codes of Practice and Guidelines C) Transitional Arrangements	Pages 24 - 28
PART V: NATIONAL DO-NOT-CALL REGISTRY	Pages 28 - 30
PART VI: SUBMISSION OF COMMENTS	Page 30

CONSULTATION PAPER

PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

PART I: INTRODUCTION

- 1.1 This Consultation Paper seeks views from the public on the proposed consumer Data Protection (“DP”) regime in Singapore.
- 1.2 DP concerns the regulation of the collection, use, disclosure, transfer and security of personal data. In general, a DP regime seeks to create a balance between the need to protect individuals’ personal data against an organisation’s need to obtain and process such data for legitimate and reasonable purposes.
- 1.3 The DP regime is intended to protect the interests of consumers and deliver economic benefits for Singapore. A DP regime will safeguard individuals’ personal data against misuse, at a time when such data has become increasingly valuable for businesses and more easily collected and processed with infocomm technology. The development of a general DP regime will put Singapore on par with other advanced economies that have introduced DP laws. This will strengthen and entrench Singapore’s position as a trusted hub for businesses, a key national economic strategy for Singapore.
- 1.4 The DP legislation is proposed to be a baseline law applicable to all organisations in Singapore, except organisations in the public sector, which are governed by an existing DP framework. The DP regime will operate concurrently with other legislative and regulatory frameworks that apply to specific sectors. The legislation will also provide for a Commission, referred to in this paper as the Data Protection Commission (“DPC”), to be set up to oversee compliance with the new DP legislation and to undertake DP education and awareness efforts.
- 1.5 MICA is seeking the public’s views on topics including the scope of coverage of the proposed DP law, the proposed data management rules involving: the collection, use, disclosure of personal data; transfer of personal data outside Singapore; data accuracy; protection and retention of personal data; and access to and correction of personal data; penalty and enforcement approach; and transitional arrangements for organisations to comply with the new law. In addition, to address the increasing volume of unsolicited marketing activities via telephone, fax and Short Message System (“SMS”), MICA is also seeking views on the proposed setting up of a National Do-Not-Call (“DNC”) Registry as part of the consultation exercise.
- 1.6 We invite all interested persons to comment on the proposed approach and issues highlighted in this Consultation Paper. Respondents are also welcome to surface any other related issues pertaining to the subject matter.

PART II: BACKGROUND

A) Overview of Current Data Protection Regime

- 2.1 There is no general law in Singapore governing DP today. Instead, Singapore adopts a sectoral approach towards DP by putting in place legislative safeguards within sector-specific frameworks to protect personal data. Common law, applicable to both the public sector and the private sector, also protects confidential information.
- 2.2 In addition, there are more than 150 Acts with statutory secrecy and disclosure provisions. Examples include the Official Secrets Act¹ and the Statutory Bodies and Government Companies (Protection of Secrecy) Act². Several of these Acts contain provisions that regulate the collection, use and disclosure of information³ obtained by public agencies and officials when carrying out their statutory functions, with penalties for contravention.
- 2.3 For the private sector, there are specific provisions in various sectoral laws to protect personal data, in particular sensitive data such as financial and health information. These provisions generally regulate the different types of actions relating to the collection, use, disclosure and transfer of personal data by sectoral licensees or for sector-specific uses. Some examples include the Banking Act⁴ and the Infectious Diseases Act⁵. There are also industry codes of practice governing DP, issued either by statutory/regulatory bodies or industry associations.
- 2.4 While there are DP safeguards in place for some sectors, many other sectors of the economy remain largely unregulated with respect to DP. For these sectors, there is the Model Data Protection Code for the Private Sector (“Model Code”)⁶, which was introduced in 2002 for *voluntary* adoption by the private sector. The Model Code has been adopted by the National Trust Council in the TrustSg initiative⁷, which seeks to enhance the electronic commerce environment in Singapore. However, there is a need to go beyond voluntary adoption of the Code to establish a mandatory baseline standard for DP across the private sector.

¹ See Official Secrets Act (Cap. 213), Long title and section 5.

² See Statutory Bodies and Government Companies Act (Cap. 319), Long title and section 3.

³ Not limited to personal data.

⁴ See Banking Act (Cap. 19), section 47 on “banking secrecy”.

⁵ See Infectious Diseases Act (Cap 137), section 25 on “protection of identity of person with AIDS, HIV Infection or other sexually transmitted disease”.

⁶ Developed based on the Organisation for Economic Cooperation and Development’s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines”), the Model Code provides a DP framework which organisations across sectors in Singapore can adopt to protect the personal data they hold. A copy of the Model Code is available at http://www.trustsg.sg/downloads/Data_Protection_Code_v1.3.pdf.

⁷ Under this programme, e-merchants seeking to acquire the TrustSg seal are required to comply with a stringent code of conduct, which incorporates the principles of the Model Code.

B) Need for General Data Protection Regime

2.5 The current sectoral approach to DP has served Singapore's needs in the past. However, recent international developments suggest that it may be timely to review our existing DP regime and establish a general DP regime in Singapore. For instance, major jurisdictions such as the European Union ("EU") and United States ("US") are putting in place measures to better protect consumers' online privacy⁸, and reviewing their existing DP regimes with the aim of strengthening protection for consumers.

Consumer / Public Interest

2.6 There is an increasing need to protect consumers' personal data, especially in an era where personal data is becoming more and more valuable to businesses. There is a growing concern that consumers' personal data is being sold or used without their consent. This is exacerbated by new technologies that create new potential for infringements of consumer privacy even as they develop new opportunities to improve everyday life. Moreover, with technology becoming more unobtrusive, intelligent and pervasive, individuals have less control over the collection and use of their personally identifying data⁹.

2.7 Under the current regime, the extent to which a private firm can be held responsible for the personal data it processes is not explicit. Whilst such firms may not necessarily be able to engage in irresponsible acts without loss to reputation or other negative outcomes, the burden lies disproportionately with consumers to ensure that their data is being protected and to pursue any suspected misuse – after the damage has already been done. There is also a negative impact on other businesses, as the irresponsible actions of a small group can undermine consumers' trust in the industry in general, and make consumers more reluctant to share their personal data even for legitimate purposes.

2.8 The Government recognises the increasing public concern over DP across multiple sectors and notes that a sectoral approach may not be able to adequately address them going forward. There is thus a need for a general DP legislation to ensure consumers' personal data is adequately protected.

Economic Interest

2.9 A general DP law will also strengthen Singapore's position as a trusted hub and create a conducive environment for the fast-growing global data management

⁸ The EU has introduced a directive to require a user's consent before a website can use a 'cookie' to store his/her browsing information. In the US, a Bill on a proposed 'Do-Not-Track' Online Act was introduced in the US Senate in May 2011.

⁹ For example, cookies are used to track a web user's online activities across many different visits and websites to build a comprehensive profile of the user, while invisible web bugs are embedded in websites, marketing e-mails and even newsgroup messages to track readers. More recently, concerns have been raised over iPhone, iPad and Android devices tracking users' locations without their knowledge and storing the data on the devices.

and data processing industries, such as cloud computing¹⁰, to thrive in Singapore. Singapore has many competitive advantages as a data hosting location, such as its telecommunications infrastructure, geographical location, safety from natural disasters and power reliability. However the lack of a general DP law in Singapore may increasingly be seen as a significant disadvantage that could deter some companies from choosing to host their data here. The development of DP legislation would thus support Singapore's future development as a global hub for data.

2.10 The lack of a general DP legislation could also be a potential hindrance to the flow of information between Singapore and other countries, and place Singapore businesses at a disadvantage in the global economy. DP legislation is increasingly seen as a basic feature in the legal framework for most economies. Sophisticated clients expect their personal data to be properly safeguarded regardless of geographical location. Having a general DP legislation in place may thus facilitate the cross-border flow of information and facilitate the growth of Singapore businesses.

PART III: PROPOSED CONSUMER DATA PROTECTION FRAMEWORK

A) Key Objectives and Principles

3.1 MICA recognises that building consumers' confidence in organisations' use and protection of their personal data is essential in today's data-centric global economy. With this in mind, the proposed DP framework seeks to achieve the following key objectives:

- a. To ensure there are adequate safeguards to protect consumers' personal data and promote greater consumer trust in the private sector; and
- b. To strengthen Singapore's overall economic competitiveness and enhance Singapore's status as a trusted hub and choice location for global data management and processing services.

3.2 The proposed DP framework is developed in support of these objectives, and is based on the following principles:

Manage Compliance Costs

3.3 Organisations may not necessarily incur high costs in order to comply with the proposed general DP regime. For example, organisations involved in global commerce would already be complying with the DP standards in other countries, and may not incur high incremental cost in order to comply with the new DP law. The impact on SMEs should also be minimal if they do not collect, process or retain large amounts of personal data.

¹⁰ Gartner forecasts that worldwide cloud services revenue will reach US\$68.3 billion in 2010, and grow to US\$148.8 billion by 2013.

- 3.4 Furthermore, the issue of compliance cost should be viewed in relation to the benefits of having such a regime. Based on the experiences of other jurisdictions, businesses, including small and medium sized enterprises (“SMEs”), have generally accepted the need for a DP law as a lack of clear DP rules meant that businesses could not be certain of their liabilities and might have to forego business opportunities¹¹. Compliance with the DP regime also sends a positive message and builds trust and credibility with customers.
- 3.5 Nevertheless, a key consideration in developing the DP regime would be to keep compliance costs manageable for businesses, especially SMEs. With this in mind, the proposed DP regime will be a baseline law to ensure that all private sector organisations put in place basic DP requirements. The DPC, which will be set up to oversee the new DP regime, will focus on educating businesses and the public on proper DP processes. A complaints-based approach rather than a more stringent audit-based regime, will be adopted. Organisations will not be regularly audited by the DPC, nor required to submit regular self-audit reports to the DPC on compliance with the DP rules. Rather, the DPC will investigate cases of non-compliance based on complaints. This would keep compliance costs for organisations manageable, reduce the resources needed to administer the regime and allow efforts to be focused on more significant data breaches.

Consistency with International Standards

- 3.6 Given that a key objective of the proposed DP regime is to enhance Singapore’s status as a trusted hub for global data management and processing services, it is important to ensure consistency with international standards, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines”) and the Asia-Pacific Economic Cooperation (“APEC”) Privacy Framework. The proposed DP framework is developed based on the principles of the Model Code, which was derived from the OECD Guidelines¹². Apart from the Model Code, the DP laws of key jurisdictions, such as the EU, the United Kingdom (“UK”), Hong Kong, Canada and New Zealand, as well as the APEC Privacy Framework are also used as references in developing the proposed DP regime.
- 3.7 It has been observed that the DP regimes in other key jurisdictions are becoming more stringent. There is growing interest in these jurisdictions in the protection of online privacy, as exemplified by the EU’s directive concerning the use of “cookies”, and the proposed “Do-Not-Track” legislation in the US. The proposed DP regime for Singapore seeks to balance this trend towards stricter regulation with the need to keep business costs manageable. This will be done by providing for the flexibility to comply with higher DP standards via an opt-in basis, if there is industry demand. The proposed DP regime also aims to be

¹¹ In Australia, where small businesses with annual turnover below A\$3 million are exempted from its DP regime, some SMEs asked not to be exempt from the law, as they felt that compliance would build up trust and credibility.

¹² The OECD Guidelines have been commonly used by countries as a basis for developing their DP laws.

technology-neutral as far as possible. This ensures that there is comprehensive protection of personal data even as new technologies emerge.

Facilitate Cross-Sector Data Flows

3.8 For a DP law to have a positive economic impact, it should facilitate data flow rather than impede it. This is best achieved by having a general DP law that applies the same baseline standard across all sectors. The general baseline law will apply concurrently with existing sectoral regulations, which could impose more stringent DP standards where necessary (for example, the banking sector). This approach is also observed in other jurisdictions¹³. It has the advantage of minimising confusion as to how the proposed DP regime will be applied, while assuring the public that there is a minimum set of DP rules applied consistently across all sectors. Such assurance will engender greater consumer trust in the private sector. This approach ensures a minimum standard of DP while providing flexibility for specific sectoral needs, and is a more balanced approach than enacting a DP law that either wholly supersedes or is superseded by sectoral regulations. Sectoral regulators may apply to the DPC to exempt their licensees from specific requirements under the general DP law where necessary. However, they will need to demonstrate that their sectoral framework will provide an equivalent, if not higher, standard of DP.

Questions in relation to objectives and principles of proposed DP framework:

Question 1: Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?

Question 2: With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations?

B) Scope of Coverage

Types of Data Covered

Definition of personal data

3.9 It is proposed that personal data be defined as follows:

“personal data” means information about an identified or identifiable individual; where “individual” means a natural person, whether living or deceased¹⁴.

¹³ For example, both Hong Kong and New Zealand have general DP laws that co-exist with specific sectoral regulations.

¹⁴ The coverage of personal data of deceased individuals will be discussed in paragraphs 3.15 and 3.16.

- 3.10 This definition takes reference from definitions of personal data adopted in DP legislations in other jurisdictions, such as Canada and the UK, as well as internationally-adopted guidelines such as the OECD Guidelines.
- 3.11 Under the proposed definition of “personal data”, information (whether a single piece of information or a group of information taken together) that relates to an identified or identifiable individual will be considered personal data. Based on the proposed definition, personal data refers not only to unique identifiers, i.e. attributes assigned to an individual which are guaranteed to be unique and hence can be used to accurately identify a person, for instance, a person’s National Registration Identity Card (“NRIC”) number, passport number or photograph, but extends to any information about an identifiable individual. For example, an individual’s mobile phone number can be considered as personal data if the individual is identifiable through his phone number.
- 3.12 The proposed DP law will not prescribe a fixed, or ‘hardwired’, list of personal data that should be protected. Under the proposed definition, certain types of information would clearly be considered personal data (e.g. a person’s NRIC number). Other types of information may be considered personal data only in specific contexts (e.g. when combined with other information). Because what constitutes personal data is context-specific, and also in view of technological developments that might bring about new types of personal data (e.g. the IP address of a device which can be linked to information about ownership or usage of the device), it is not feasible to have a definitive list of the types of personal data hardcoded into the DP law. Internationally, it is observed that none of the key jurisdictions with DP legislation prescribe a fixed list of personal data. Nevertheless, to provide greater clarity to organisations, the DPC may publish guidelines giving examples of information that may constitute personal data following the enactment of the DP law.

All forms of personal data

- 3.13 The DP law will cover all forms of personal data, including both electronic and non-electronic forms of personal data. Although data is increasingly collected, processed and stored electronically, much data is still collected, processed and stored using non-electronic means (for example, lucky draw forms). A homogeneous treatment of all forms of data is thus proposed as it is more effective in achieving the objective of protecting consumer interests.

Sensitive personal data

- 3.14 MICA recognises that there may be certain categories of information for which the level of DP required may be less stringent. It is noted that in some jurisdictions, certain types of information are excluded from the definition of “personal data” and hence fall outside the DP law in those jurisdictions. Examples include business contact information (e.g. the name, title, business address or telephone number of an employee of an organisation) and work

product information¹⁵. On the other hand, there are certain types of personal data that may require higher levels of protection than others. Some jurisdictions, such as the EU, have separately provided a definition for “sensitive personal data”, which are subject to more stringent DP requirements. The proposed approach is to have a general DP law that applies a minimal baseline DP standard to all sectors, with mechanisms, such as exemptions from specific clauses of the DP law to loosen the baseline requirements for certain requirements, and concurrent regulation, the proposed DP law will work together with sector-specific frameworks to address the specific concerns or needs relating to such data more effectively.

Personal data of deceased individuals

- 3.15 It is noted that there is no international norm as to whether personal information about deceased individuals is protected under DP laws. Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”) protects personal data of deceased persons who have been deceased for less than 20 years, whereas the UK’s Data Protection Act only covers personal data relating to living individuals. There are varying considerations in determining whether, and to what extent, the personal data of deceased individuals should be covered by the proposed DP law. On one hand, the unwarranted disclosure of the personal information of a deceased individual may have a negative impact on the living relatives of the individual. On the other hand, it would be administratively complex to extend the DP law to cover the personal data of the deceased. For instance, it would be difficult and costly for organisations to identify and verify the parties able to act on behalf of the deceased individual in relation to obtaining consent for the collection, use and disclosure of personal data about the deceased, or in relation to the access and correction of personal data about the deceased individual. It is also arguable whether the interests of the family of deceased individuals necessitate the same level of protection for the deceased’s personal data as living individuals’ personal data.
- 3.16 Given the complexity of this issue, MICA would like to seek views on whether the personal data of deceased individuals should be covered by the proposed DP law. In the event that such data is to be included, one possible approach is to accord the same level of protection to the personal data of deceased individuals as that of living individuals, only in relation to the safeguarding and disclosure of such personal data, and where the individual has been deceased for less than 20 years¹⁶. Such an arrangement will strike a balance between mitigating the impact of inadequate protection of the personal data of deceased individuals, which would be most pernicious in the event of disclosure without consent, and minimising compliance costs for organisations.

¹⁵ British Columbia’s Personal Information Protection Act, section 2, defines “work product information” is defined as “*information prepared or collected by an individual/group of individuals as a part of the individual’s/group’s responsibilities or activities related to the individual’s/group’s employment or business, but does not include personal data about an individual who did not prepare or collect the personal data*”.

¹⁶ This means that for the personal data of individuals that have been deceased for less than 20 years, organisations will have to comply with the provisions in the DP law governing the safeguarding of personal data and the conditions under which personal data may be disclosed; all other provisions in the DP law will apply only to the personal data of living individuals.

Questions in relation to the definition of “personal data”:

Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?

Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?

Types of Organisations and Activities Covered

Organisations in Singapore

- 3.17 In general (and subject to a few exceptions noted below), the proposed DP law will apply to all persons, companies and other organisations in Singapore, collectively referred to as “organisations” in this paper. This definition of “organisation” includes a natural person, a trust and any company or association or body of persons, corporate or unincorporated, but does not include a natural person acting in a personal or domestic capacity¹⁷, a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settlor, and public agencies.
- 3.18 The proposed DP law will put in place an overarching basic DP regime to govern all private sector organisations, similar to how the public sector as a whole is governed by a DP framework. The public sector in Singapore (including Government Ministries, Statutory Boards and Organs of State) is governed by its internal rules and regulations regarding DP. Like the proposed DP law, these public sector DP rules are consistent with the principles of the Model Code. While there may be some differences due to specific needs of the public sector (for example, the need to facilitate data sharing across public agencies), the public sector rules accord similar levels of protection for personal data as the proposed DP law. It should also be noted that separate regimes governing public and private sector handling of personal data is not uncommon internationally. In Canada, data protection by the public sector is governed by its Privacy Act while the private sector is governed by the PIPEDA. Malaysia’s Personal Data Protection Act, which was passed in 2010, is also a DP law that applies only to private sector organisations.
- 3.19 MICA also considered whether certain types of organisations should be excluded from the application of the DP law. For example, some jurisdictions

¹⁷ “Personal” refers to matters relating to the individual concerned, while “domestic” refers to matters relating to the home or family of the individual concerned. The exclusion of “personal” and “domestic” uses from the DP law is a common exclusion adopted internationally, including jurisdictions such as Canada, the UK and New Zealand.

do not apply their DP laws to small companies that have low annual turnover. In other jurisdictions, there are also specific DP laws that apply only to organisations engaged in commercial activities and exclude other organisations. The key consideration for excluding certain organisations is the cost of compliance for these organisations. However, based on the experiences of other jurisdictions, it is assessed that such measures increase the complexity of the regime, which in turn increase compliance costs. The regime that MICA is thus proposing is a “light touch” baseline legislation that applies to all private sector organisations to ensure a minimum standard of DP across the private sector.

Activities in Singapore

- 3.20 Besides organisations in Singapore, there are organisations outside of Singapore that engage in data collection and/or processing activities in Singapore. For example, overseas organisations may engage in data collection activities online and collect personal data from a person using a computer in Singapore. The question arises as to whether such activities should be covered by the DP law, even though the organisation is not in Singapore.
- 3.21 In some jurisdictions, such activities are covered under the DP law. The UK Data Protection Act, for example, covers entities established in the UK, as well as those that use “equipment” in the UK for data processing, such as UK based servers or cookies. This means that a company not in the UK installing cookies on UK users’ computers would be subject to the UK’s DP regime, and the UK courts would have jurisdiction over the company if its activities breached the UK Data Protection Act. The European Commission has similarly expressed views that with technological advancement, privacy standards for Europeans should apply independently of the location in which their data is being processed¹⁸.
- 3.22 However, while there are valid reasons for extending the coverage of Singapore’s DP law to all data collection and processing activities in Singapore, regardless of whether the organisation responsible is in Singapore, there are practical difficulties to implementing such a regime. In particular, where the organisation in question has no presence in Singapore, it would be difficult to carry out investigations into any complaint made in relation to an activity of the organisation, or to proceed with any enforcement action against the organisation. In practical terms, even if such activities are to be included in Singapore’s DP law, the limited ability to carry out investigation and enforcement may mean that consumer complaints against organisations outside of Singapore cannot be adequately addressed, and breaches by such organisations may remain uncorrected. MICA would like to seek views as to whether Singapore’s DP law should only cover organisations in Singapore, or

¹⁸ In a speech delivered on 16 March 2011, Viviane Reding, Vice-President of the European Commission, said “... *homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being processed. They should apply whatever the geographical location of the service provider and whatever technical means used to provide the service... for example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules.*”

whether coverage should also extend to personal data collection and processing activities in Singapore regardless of where the organisation is located, bearing in mind the practical difficulties of implementation.

Questions in relation to the organisations and activities covered by the DP law:

Question 5: Do you have any views / comments on the proposed organisations covered by the DP law?

Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations?

C) Rules and Exclusions

3.23 Under the proposed DP law, organisations will have obligations in the following four broad areas (described in greater detail in the following paragraphs):

- i) General rules, for example, relating to transparency of processes;
- ii) Rules on the collection, use and disclosure of personal data;
- iii) Rules on accuracy, protection and retention of personal data; and
- iv) Rules on providing access to and correction of personal data.

General Exclusions

3.24 There are certain circumstances under which some or all of the above areas of the DP Act should not apply. These exclusions take into account international practice and Singapore's context. For example, personal data recorded in a document of a court will be excluded from the application of the DP Act; personal data about an individual that is contained in a record that has been in existence for at least 100 years or under the control of a public agency, including personal data in the custody of a person acting as an agent of the public agency, will also be excluded from the DP Act.

3.25 There will also be circumstances where the DP Act will not apply to the collection, use or disclosure of personal data. One such circumstance is when personal data has been made available by a public agency to a specific organisation or to the public generally. The DP Act will also not apply to the collection, use or disclosure of personal data carried out by a news organisation¹⁹ in the course of a news activity²⁰, as well as the collection, use or

¹⁹ "News organisation" refers to any organisation whose business, or part of whose business, consists of a news activity and which has been declared to be a news organisation by the Minister-in-charge of the DP law.

²⁰ "News activity" refers to gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of

disclosure of an individual's business contact information²¹ if it is solely for the purpose of enabling the individual to be contacted in relation to the individual's employment, business or profession.

3.26 Some jurisdictions such as Canada also provide exclusions for the collection, use and disclosure of personal data solely for artistic or literary purposes (for example, biographies, plays, musical compositions, photography etc). While MICA recognises the underlying rationale for such exclusions, there is considerable practical difficulty defining such exclusions to meet legitimate needs. MICA would thus like to seek feedback on whether exclusions for artistic or literary purposes should be provided, and if so, how such exclusions should be defined.

3.27 In addition to the proposed general exclusions set out above, exclusions from specific provisions of the DP Act will also be provided for certain circumstances. These specific exclusions are discussed in subsequent sections.

Questions in relation to the general exclusions from the DP law:

Question 7: Do you have any views / comments on the proposed general exclusions from the DP law?

Question 8: With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?

Question 9: Are there any other exclusions that should be catered for under the DP Act?

General Rules

3.28 In some jurisdictions like the EU, a distinction is made between the DP rules applicable to data controllers and data processors. The proposed DP law does not distinguish between organisations as data controllers or data processors, but will hold an organisation *responsible for personal data under its custody or control, including personal data that is not in the organisation's custody but is under its control.*

3.29 An organisation that outsources the collection and/or processing of personal data is still responsible for the management of such personal data. However, this does not mean that an organisation that is merely in the business of

dissemination to the public or any section of the public, or the dissemination of news, to the public or any section of the public.

²¹ "Business contact information" refers to information to enable an individual to be contacted in relation to their employment, business or profession. Examples include the name, position name, title, business telephone number, address, email or fax number of the individual.

processing personal data on an outsourced basis is excluded from the DP Act. Such an organisation is likely to be deemed to have control over the personal data.

- 3.30 Generally, in line with international best practices, the regime prescribed by the proposed DP law is based on **consent, purpose and reasonableness**. An organisation may only collect, use or disclose personal data with the individual's consent, or where consent is deemed to be given under the DP Act, and for a reasonable purpose which the organisation has disclosed to the individual before collecting the data. The reasonableness of the purpose would be judged against what a reasonable person would consider appropriate in the circumstances. Exceptions will apply in certain circumstances, as discussed in the following sections, where the collection, use of the personal data without the individual's consent will not be in contravention of the DP law.

Consent

- 3.31 In general, an organisation is required to obtain the individual's consent for the collection, use or disclosure of his personal data. If the organisation attempts to obtain consent by providing false or misleading information with respect to the collection, use or disclosure of the information, or using deceptive or misleading practices, any consent provided in those circumstances is not validly given. In addition, an organisation may not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is necessary to provide the product or service.
- 3.32 Given that the type of consent could vary depending on the specific context of the collection, MICA does not propose to prescribe in detail the manner in which consent may be given in the DP Act. Consent obtained may be explicit or implied, depending on the circumstances. There will be situations where consent may be deemed to have been given, and it would be awkward for organisations to have to obtain explicit consent from the individual in such circumstances. If, at the time the consent is deemed to be given, the purpose is considered to be obvious to a reasonable person, and the individual voluntarily provides the personal data to the organisation for that purpose, then the individual would be deemed to have consented to the collection, use or disclosure of his personal data by an organisation for that purpose.
- 3.33 An example where this may apply is the case of an individual who seeks medical treatment in a medical facility such as a clinic or hospital. If such an individual voluntarily provides his personal data when registering or making an appointment with the facility, he would reasonably be deemed to have done so for the purpose of seeking medical treatment. He would also be deemed to have consented to the collection and use of his personal data by the medical organisation for that purpose. Generally, the imperatives of safeguarding public health and facilitating quick and effective medical treatment may sometimes override the requirement for consent. For example, the Infectious Diseases Act requires healthcare professionals to collect and disclose information from a patient to the Director of Medical Services in certain circumstances, such as for

the purpose of preventing the spread of an infectious disease. Such disclosure is notwithstanding any restriction on the disclosure of information imposed by other written laws, rules of professional conduct, contract etc²².

- 3.34 Consent may also be deemed to be given when the collection, use or disclosure of personal data is for the purpose of the individual's enrolment for or coverage under an insurance, pension, annuity, provident fund, benefit or similar plan, policy or contract, under which the individual is a beneficiary or has an interest as an insured under the plan, and is not the applicant for the plan, policy or contract. In such instances, requiring explicit consent could be onerous and detract from the objectives of including the individual under the plan, policy or contract.
- 3.35 Some jurisdictions such as British Columbia deem consent to be given when individuals are notified of an organisation's intent to collect, use or disclose their personal data, but do not register any objections within a reasonable timeframe. While such an "opt-out" approach may be more cost-effective for organisations, MICA notes that it may be unreasonable to place the burden of establishing consent on the individuals. MICA would thus like to seek views on whether the DP Act should also deem consent to be given in such situations.
- 3.36 An individual may, on giving reasonable notice to the organisation, withdraw his consent to the collection, use or disclosure of his personal data at any time, unless such withdrawal would frustrate the performance of a legal obligation or where consent has been given to a credit bureau to create a credit report. On receipt of such withdrawal notice, the organisation should inform the individual of the likely consequences of the withdrawal of consent. The organisation shall not prohibit the individual from withdrawing his consent to the collection, use or disclosure of personal data related to the individual. However, the organisation may set reasonable procedures for such withdrawal of consent. Where an individual withdraws consent to the collection, use or disclosure of personal data by an organisation, the organisation shall stop collecting, using or disclosing the personal data unless the collection, use or disclosure is permitted without consent under the DP Act or any other written law.

Representatives of individuals

- 3.37 The proposed DP Act provides an individual with several rights and powers, such as that of the provision of consent and access to his or her personal data. However, there may be instances where an individual may not be able to exercise such rights, such as when he or she is incapacitated. It is thus proposed that any right or power conferred on an individual under the DP Act may also be exercised by a representative of the individual in such instances. Such representatives could include a parent or guardian of the individual, if the individual is under 18 years of age, a guardian or trustee who has been appointed for the individual, an attorney appointed under a power of attorney

²² See Infectious Diseases Act (Cap. 137), section 10 on "Director may require information from healthcare professionals, etc".

that has been granted by the individual, or any person with written authorisation from the individual to act on the individual's behalf.

Accountability

3.38 Even as organisations seek to comply with the DP regime, it is important that they are open and transparent to customers in their policies and practices relating to the management of personal data. Organisations should designate one or more individuals to be responsible for ensuring that they comply with the DP Act. However, it should be noted that the designation of such an individual does not relieve an organisation of the obligation to comply with the provisions set out in the DP Act. The business contact information of the designated individual should be made known to consumers, so that consumers are able to contact the organisation easily in relation to queries about the organisation's data protection policies and issues related to the organisation's compliance with the DP Act, amongst other reasons.

Questions in relation to the general exclusions from the DP law:

Question 10: Do you have any views / comments on the proposed general rules under the DP law?

Question 11: With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?

Rules on the Collection, Use and Disclosure of Personal Data

3.39 Flowing from the general rules, the proposed DP rules governing the management of personal data throughout its "lifecycle", i.e., the collection, use/processing, disclosure, retention and deletion of personal data, are outlined in the following paragraphs.

Collection

3.40 In general, organisations may only collect personal data for purposes that a reasonable person would consider appropriate in the circumstances, and which fulfil the purposes that the organisation discloses in accordance with the DP Act, or are otherwise permitted under the DP Act or any other written law.

3.41 On or before collecting an individual's personal data from the individual, an organisation shall disclose to the individual, verbally or in writing, the purposes for the collection of the personal data. The organisation must also disclose the business contact information of an officer or employee of the organisation who is able to answer any questions the individual may have about the collection of his personal data. Where the organisation collects personal data from another

organisation without the consent of the individual, the collecting organisation shall provide the other organisation with sufficient information regarding the purpose of the collection on or before the collection, to enable the other organisation to determine whether the disclosure is in accordance with the DP law.

- 3.42 There may be situations where obtaining consent before collecting personal data about an individual may not be practical, which the DP law will allow for collection to occur without first obtaining consent from the individual. Examples include situations where the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way; where the collection is necessary for the medical treatment of the individual and the individual is unable to give consent; where the collection is necessary to respond to an emergency that threatens the life, health or security of an individual; or where it is reasonable to expect that the collection with the consent of the individual would compromise the availability or the accuracy of the personal data and the collection is reasonable for an investigation or legal proceeding. In addition, prior consent will not be required where the collection of personal data is required or authorised by law, or where the data was disclosed to the organisation without consent of the individual for purposes which the DP Act does not require consent for²³.
- 3.43 Another common situation where consent would not be needed is when the personal data is available to the public, or when the personal data is collected by observation at a performance, a sports meet or a similar event open to the public, at which the individual voluntarily appears. This provision recognises that it would neither be practical nor productive to prohibit the sharing of data in such circumstances. However, given that there are a multitude of data sources (for example, telephone directories and newspapers) that could be considered publicly available, the DPC will provide further guidance on the types of sources that would be considered as such.
- 3.44 Organisations may also need to collect employee personal data²⁴ for the purposes of establishing, managing or terminating an employment relationship between the organisation and the individual. It is proposed that the DP Act allows such collection without the need for consent, where the collection is reasonable for the specified purposes. However, before the organisation collects the employee personal data, the organisation should notify the individual that it will be collecting his personal data and the purposes for the collection. It is noted that such differential treatment for employee personal data is also adopted in some DP regimes internationally, such as the PIPA in Canada's British Columbia.
- 3.45 Organisations also typically collect personal data belonging to their members for identification purposes or for internal circulation. Examples of such personal

²³ Such purposes are further described in the section on 'Disclosure'.

²⁴ "Employee personal data" refers to personal data about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organisation and that individual, but does not include personal data that is not about an individual's employment.

data include photographs taken for identification passes, or for organisational newsletters. While there may be merit to protecting such personal data, requiring organisations to obtain consent for collection may be onerous relative to the benefits of protection, particularly if the data is intended for internal circulation. MICA thus seeks views on whether organisations should be required to seek consent for the collection of their members' personal data for such purposes.

- 3.46 The DP Act also recognises that the collection of personal data without consent may be necessary to enable certain organisations to perform their functions effectively. For example, when an individual has consented to organisations' disclosure of his or her personal data for a credit report, a credit bureau compiling the credit report would not need to obtain additional consent to collect the personal data. Similarly, where the personal data collected may be necessary to facilitate the collection of a debt owed to or the payment of a debt owed by the organisation, or for the organisation to provide legal services to a third party, consent would not be needed as it may impede the effective execution of these activities. Organisations under the purview of the National Council for Social Services providing financial assistance or social services to individuals or their families would also not need individuals' consent to collect personal data necessary for the purpose of determining eligibility for such financial assistance or social services.
- 3.47 Other situations where consent for data collection will not be needed under the DP Act includes situations where an individual acting in a personal or domestic capacity provides personal data relating to another party to an organisation, where the personal data is necessary for the organisation to provide services to the individual. In such instances, the organisation should also be allowed to collect this information without consent from the party with whom the personal data concerns. Another example is where the personal data is collected to determine the individual's suitability to receive an honour, award or similar benefit (for example, those granted by public bodies, professional associations, business federations etc), or to be selected for an athletic or artistic purpose.
- 3.48 In instances where an organisation outsources the collection or processing of personal data to another organisation, it will not be necessary to obtain the consent of the individual to transfer his personal data from one organisation to the other as long as the individual previously consented to the collection of his personal data by the organisation, and the sharing of personal data is solely for the purposes for which the information was collected and to assist the organisation outsourcing the work.

Use / Processing

- 3.49 Following from the rules governing the collection of personal data where in general, organisations should obtain the consent of the individual for the collection, use or disclosure of his personal data for specified purposes, the use or processing of such personal data by organisations must be reasonable and fulfil only the purposes for which the individual's consent was obtained. Unless consent is not required under the DP Act, fresh consent has to be obtained if

the personal data collected is to be used for a different purpose other than the purposes for which the individual has given consent.

3.50 There may be situations under which the individual's consent need not be obtained before the organisation may use the personal data, and the circumstances under which such exceptions apply are similar to those in relation to the collection of personal data without consent discussed above. In particular, exceptions in respect of use of personal data will be provided for situations contemplated in paragraphs 3.42 to 3.48.

Disclosure

3.51 Following from the principle that the collection and use of personal data should be done with the individual's consent for a specific purpose, disclosure of personal data collected must also be in line with the purpose for which the individual's consent was obtained, unless otherwise permitted under the DP Act or required under any other written law.

3.52 As with the collection and use of personal data, there are circumstances in which disclosure of personal data without the individual's consent may be allowed. These circumstances are similar to the exceptions applicable to collection and use discussed above. In particular, exceptions in respect of disclosure of personal data will be provided for the situations contemplated in paragraphs 3.42 to 3.48.

3.53 In addition, there are some unique circumstances which require specific exceptions in respect of disclosure of personal data. For example, disclosure of personal data does not require consent from the individual when it is to a public agency or a law enforcement agency in Singapore for the purpose of an investigation into an offence or other contravention under the laws of Singapore, or when the information to be disclosed relates to national security, defence, public security, the conduct of international affairs, or similar matters of national interest. Consent is also not needed when the purpose of the disclosure is to comply with a subpoena, warrant or order issued or made by a court, or the disclosure is made to an advocate and solicitor who is representing the organisation. Disclosures to police officers, or any other officers of the Ministry of Home Affairs authorised to collect personal data for the purpose of the officers' functions and duties under any written law can also be made without consent of the individual.

3.54 The DP Act will waive obligations to obtain consent to disclose personal data in cases where there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual. However, the individual should also be notified of the disclosure. Likewise, consent is not required when the disclosure is for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual.

3.55 Consent will also not be required for disclosure of personal data to prescribed archival institutions, such as the National Archives, if the collection of the personal data by the institution is reasonable for research or archival purposes.

Related to this is information disclosed to other organisations for research purposes, including statistical research. In situations when it is impracticable for the organisation to seek the consent of the individual for the disclosure, and the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form, organisations may disclose personal data for research purposes without consent, provided the personal data is not linked to other information that could be harmful to the individuals identified by the personal data, and the benefits to be derived from the linkage are clearly in the public interest. Conditions relating to the policies, procedures, security and confidentiality of the data would also need to be adhered to. In addition, the personal data must not be used to contact individuals to seek their participation in the research, and organisations using the personal data for research must remove or destroy individual identifiers at the earliest reasonable opportunity.

- 3.56 This exception will encompass research activities, including business analytics, which will support the drive to make Singapore a hub for such emerging industries. However, it should be highlighted that this exception is purely for the purpose of research, and does not permit organisations to collect, use or disclose the personal data for marketing purposes.
- 3.57 Another exception is in relation to the sharing and transfer of personal data when organisations are involved in a merger or an acquisition. Specifically for such cases, both the seller and the buyer may require the sharing of personal data about customers, employees, shareholders and other stakeholders in order to evaluate and complete the business transaction. A specific exclusion to facilitate such business transactions is thus proposed so that organisations may disclose personal data about their employees, customers, directors, officers or shareholders without their consent, to a prospective party, if the personal data is necessary for the prospective party to determine whether to proceed with the business transaction, and the organisation and prospective party have entered into an agreement that requires the prospective party to use or disclose the personal data solely for purposes related to the prospective business transaction.
- 3.58 If the organisation proceeds with the business transaction, the organisation may then disclose without consent the relevant personal data that relates directly to the part of the organisation or its business assets that is covered by the business transaction. The employees, customers, directors, officers and shareholders whose personal data is disclosed must also be notified that the business transaction has taken place and the personal data about them has been disclosed to the party. Likewise, the prospective party may collect and use the personal data without consent in such situations.
- 3.59 If a business transaction does not proceed or is not completed, a prospective party shall destroy or return to the organisation any personal data the prospective party collected about the employees, customers, directors, officers and shareholders of the organisation.

Transfer of personal data outside Singapore

- 3.60 While the proposed DP law will apply to organisations in Singapore, it is important for consumers to have the assurance that similar standards of protection are accorded to their personal data if the data is transferred outside Singapore. This is important to maintain the level of trust and confidence of consumers in Singapore, especially as cross-border data transfers become more commonplace with market developments like cloud-based computing.
- 3.61 Some jurisdictions like the EU impose stringent conditions on the transfer of EU data outside the EU. In particular, data may only be transferred to non-EU (or non-EEA²⁵) jurisdictions that have been found to have an adequate level of data protection, or where companies have adopted specific measures such as approved binding corporate rules or standard contractual clauses. Other jurisdictions impose alternative rules in relation to cross-border data transfers, such as APEC's proposed Cross-Border Privacy Rules system. For Singapore, the proposal is to adopt a "principle based" approach, as opposed to a more prescriptive approach of requiring adequacy rulings for foreign regimes or approving binding corporate rules. The onus will be on the organisation to ensure that appropriate measures are taken to protect personal data where such data is transferred outside Singapore, as the organisation is considered to have control over the data.

Questions in relation to the proposed rules on collection, use and disclosure of personal data:

Question 12: Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?

Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?

Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?

Rules on Accuracy, Protection and Retention of Personal Data

- 3.62 Besides the rules surrounding the need to obtain the individual's consent for the collection, use and disclosure of his personal data for specific purposes, DP regimes would also typically contain requirements for organisations to

²⁵ European Economic Area

safeguard personal data in their custody. There are three aspects of safeguarding that are typically catered for in DP regimes.

- 3.63 Firstly, it is important for organisations to ensure that the personal data they collect and use is as accurate as is practicable. However, it will be overly onerous on organisations to have a blanket requirement on the accuracy of the personal data, since organisations may incur costs in updating such personal data regularly. Instead, organisations will be required to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is reasonably accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, or is likely to be disclosed by the organisation to another organisation.
- 3.64 Secondly, it is important to ensure the security of personal data to prevent data breaches and inadvertent disclosure. Notably, there have been several widely publicised cases of data breaches internationally in recent years, either due to criminal activities like hacking or carelessness on the part of the organisation, which had led to the leakage of substantial amounts of personal data by organisations. The DP Act will thus require organisations to protect personal data in its custody or under its control, by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks.
- 3.65 Recognising that the manner of securing personal data would differ based on the sensitivity of the data, the nature of the data (for example, physical data as opposed to electronic data) and other factors, specific methods of securing personal data will not be prescribed in the DP Act. Nevertheless, when the DP law is implemented, guidelines may be issued on suitable methods of protection that can be considered by organisations.
- 3.66 Thirdly, it is important to strike the right balance between the need for organisations to retain personal data, where there are valid reasons to do so, and the requirement to delete personal data (or render such data anonymous such that the data is no longer personally identifiable). It is noted that organisations collect and use personal data for specific purposes, and where the data is no longer necessary to serve such purposes, organisations should not retain such personal data. To strike the balance, it is proposed that if an organisation uses an individual's personal data to make a decision that directly affects the individual, the organisation shall retain that information for a sufficient period of time after using it so that the individual has a reasonable opportunity to obtain access to it. Following that, an organisation shall then destroy its documents containing personal data, or make such data anonymous, when retention is no longer necessary for legal or business purposes, and as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data.
- 3.67 Ideally, individuals should be informed of the retention period for their personal data at the point of collection, as this would provide greater assurance to

individuals and encourage sharing of data. However, MICA recognises that the appropriate retention period may differ according to context, and it may not always be practicable for organisations to determine and specify a suitable retention period upfront. MICA would thus like to seek views on whether organisations should be required to specify the retention period at the point of collecting the personal data.

Questions in relation to the proposed rules on accuracy, protection and retention of personal data:

Question 14: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?

Question 15: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?

Rules on Access to and Correction of Personal Data

3.68 It is proposed that individuals will have the right to request access to their personal data held by an organisation. This will allow individuals to find out how organisations have used, or are using, the personal data collected, correct information that may be inaccurate, or seek redress for suspected breaches of the DP Act. Generally, upon the request of an individual, the organisation should take steps to assist the individual in obtaining access to his personal data, provide the individual with information about the ways in which the personal data has been and is being used by the organisation, and provide the individual with the names of the individuals and organisations to whom the personal data has been disclosed. Credit bureaus should also provide the individual with the names of the sources from which they received the personal data, unless it is reasonable to assume the individual can ascertain those sources.

3.69 Organisations should take steps to correct any inaccurate data at the request of the individual, if the data is about the individual and is under the organisation's control. Such corrected data should be also sent to any other organisations to which the personal data was disclosed during the year before the date the correction was made. Organisations notified of a correction of personal data by another organisation shall correct the personal data under their control. Even when no correction is made, organisations shall still annotate the personal data under their control with the correction that was requested but not made.

3.70 As organisations may need to incur costs in allowing individuals to access and correct their personal data, organisations will be allowed to charge a reasonable fee to recover any costs incurred in providing such access. In such situations, the organisation shall give the applicant a written estimate of the fee before providing the service, and can require the applicant to pay a deposit for all or part of the fee.

- 3.71 There are circumstances where it will be impractical for organisations to grant individuals access to certain personal data, and organisations will not be required to do so under those circumstances. For example, organisations will not be required to provide access to personal data if it is subject to legal privilege, or if it was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration. This exception also applies if the disclosure of the information would reveal confidential commercial information that if disclosed, could, in the opinion of a reasonable person, harm the competitive position of the organisation.
- 3.72 In addition, there are circumstances where the organisation would not be allowed to provide individuals access to their personal data or information about how the personal data has been or is being used by the organisation. In situations where personal data was collected or disclosed without consent as permitted under the DP Act for the purposes of an investigation, or for the purposes of national security, defence, public security, the conduct of international affairs or similar matters of national interest, the organisation shall not disclose such information to the individual, as this could compromise the investigations and operations of the relevant authorities. Organisations are also not permitted to provide individuals access to their personal data if the disclosure could reasonably be expected to threaten the safety or physical or mental health of another individual other than the individual who made the request, or to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request. When the disclosure would reveal personal data about another individual or the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to disclosure of his or her identity, the organisation would also not be allowed to provide access to the personal data.
- 3.73 The organisation may refuse individuals' access to their personal data where they face frivolous or vexatious requests, or where responding to the request would unreasonably interfere with the operations of the organisation due to the repetitious or systematic nature of the requests. This also applies if the information requested is trivial, not readily retrievable, does not exist or cannot be found, or the burden or expense of responding to the request would be unreasonable or disproportionate to the risks to the interests of the individual who made the request. Finally, organisations may also refuse access to a reference given for the purposes of an individual's education or employment if the individual had previously agreed to waive the right to view it.

Questions in relation to the proposed rules on access to and correction of personal data:

Question 16: Do you have any views / comments on the proposed rules on access to and correction of personal data?

PART IV: IMPLEMENTATION

A) Penalty and Enforcement Regime

- 4.1 The DPC will be set up to enforce the DP Act. It is envisaged that an independent Appeals Board²⁶ will be set up to hear appeals against the decisions of the DPC.
- 4.2 In many jurisdictions internationally, DP authorities are given the powers to serve enforcement notices on organisations that have been found to have breached their respective DP laws, requiring that organisations take specific steps or corrective measures to ensure compliance with the law. DP authorities may also be able to accept undertakings or settlements from organisations, which may include compensation to affected consumers resulting from non-compliance with the law. Where there are criminal offences involved, the relevant law enforcement agencies (including, where applicable, the DP authorities) may prosecute offending organisations.
- 4.3 In recent reviews of DP regimes in other jurisdictions, it is observed that DP authorities have sought greater powers in relation to the ability to impose financial or monetary penalties for non-compliance. In the UK, the Information Commissioner's Office has been given the power to issue monetary penalties in a review of its DP Act. In Hong Kong, the Privacy Commissioner for Personal Data ("PCPD") has also indicated in the 31 December 2010 "PCPD's Submission in response to Report on Public Consultation on Review of the Personal Data (Privacy Ordinance)" that *"in circumstances involving serious and blatant disregard of the personal data privacy rights, the issuance of an enforcement notice directing data user to take remedial steps is considered insufficient. Proposal 42 (Empowering the PCPD to impose Monetary Penalty on Serious Contravention of Data Protection Principles) will equip the PCPD with the power to impose monetary penalty on the data user to achieve the necessary deterrent effect."*
- 4.4 It is important to highlight that the penalty regime proposed for Singapore's DP Act seeks to secure ongoing compliance by organisations and at the same time, provide sufficient deterrence to ensure that organisations put in place appropriate measures to safeguard consumers' personal data. The proposed penalty regime is thus a tiered one that will enable the DPC to enforce remedies commensurate with the seriousness of the violation. Specifically, it is proposed that the DPC will have powers to issue orders for an organisation to rectify non-compliance with the DP law, and require the organisation to pay, within a specified period, a financial penalty of such amount not exceeding \$1 million. The financial penalty is notwithstanding any order already made by the DPC.
- 4.5 The proposed penalty regime recognises that the majority of contraventions would be minor or non-malicious in nature, and would be adequately addressed

²⁶ Members of the independent Appeals Board will be appointed by the Minister-in-charge of the DP Act.

by the issuance of orders for corrective action. However, there could also be violations that would warrant stiffer penalties, such as those that cause significant harm to individuals. In such instances, financial penalties could be imposed on top of any orders for corrective action. To enable the DPC to carry out its duties or powers effectively, criminal penalties will also be imposed on any organisation or individual that obstructs the DPC or an authorised delegate of the DPC in the performance of its duties or powers under the DP Act. Organisations or individuals who knowingly or recklessly make false statements, knowingly mislead or attempt to mislead the DPC, or fail to comply with an order made by the DPC under the DP Act, may also be subject to criminal penalties.

- 4.6 An independent Appeals Board will hear appeals against the DPC's decisions. The Appeals Board's decisions may be brought to court for appeal or review. In addition, the law will enable individuals to separately seek redress via civil proceedings in court.
- 4.7 Over and above the formal investigation and enforcement regime prescribed in the DP Act, it is expected that for many of the cases, the DPC will focus on early resolution of complaints by facilitating discussions between complainants and the organisations concerned. To this end, the DP law will enable the DPC to refer the contending parties for mediation.
- 4.8 The DPC may also initiate investigations, whether a complaint is received or not, into an organisation's compliance with any provision of the DP Act, if it is satisfied there are reasonable grounds to believe that the organisation is not complying with the Act. However, while the DP Act will provide the DPC with powers to investigate possible breaches and review organisations' decisions on DP matters, it may not be appropriate for the DPC to carry out such actions in all cases. The DPC may refuse to conduct or continue investigations or reviews in certain circumstances, such as when the written request for review or written complaint is frivolous or vexatious, is not made in good faith, or the circumstances warrant a refusal to conduct, suspending or discontinuing an investigation or review. Similarly, when the DPC requires an individual to attempt to resolve his dispute with the organisation in a way directed by the DPC before the DPC begins or continues an investigation or review, or when any party involved in the matter has commenced legal proceedings (other than proceedings to obtain interim injunctive relief) against another party, the DPC will be able to refuse to conduct or continue its investigations or reviews. The DPC can also choose not to interfere further in cases where the parties involved in the matter have mutually agreed to settle the matter.
- 4.9 Given that the DP Act is expected to operate concurrently with other sectoral regulations, there may also be cases where a particular incident may constitute a breach in both regimes. In such cases, it would be preferable that the organisation be subject to the investigative and enforcement actions of one regulator. The DP Act will therefore provide the DPC with the powers to refer an incident to another regulatory agency if necessary.

Questions in relation to the proposed penalty and enforcement regime:

Question 17: Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?

Question 18: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?

B) Regulations, Codes of Practice and Guidelines

4.10 MICA notes that it may be more appropriate for certain details of the DP regime to be explained in regulations or guidelines. These could include topics such as the definition of personal data, guidance on what constitutes deemed consent, and fee structures for processing requests to access personal data. It is proposed that the DP Act provides the power for the Minister-in-charge to amend the list of exclusions and make general exemptions, and for the DPC to issue regulations, codes of practices or guidelines to supplement the provisions of the DP Act.

C) Transitional Arrangements

“Sunrise” period

4.11 Many organisations with extensive personal data management activities should already comply with industry best practices in relation to data protection, such as those prescribed by the Model Code, and should not have to make significant adjustments to their practices to comply with the DP Act. However, recognising that some organisations, especially SMEs that collect and manage personal data, will need time to adjust their policies, processes and systems to comply with the new DP Act, there will be a “sunrise” period between the time the DP Act is enacted and the time its provisions take effect.

4.12 Internationally, “sunrise” periods from a few months to more than two years have been adopted. International practices have also differed on whether all provisions enjoy the same “sunrise” period, or whether certain provisions take effect sooner than others.

4.13 In Singapore’s case, MICA proposes to adopt a single “sunrise” period for all provisions in the DP Act for ease of compliance and administration. Given that it will be the first time organisations will need to comply with a general DP Act, a single “sunrise” period will create less confusion and be more easily communicated, understood and applied by organisations. It would also be more complex for the DPC to enforce certain aspects of the DP Act when other aspects might not have taken effect.

4.14 In relation to the appropriate “sunrise” period, MICA is considering a “sunrise” period of between one to two years, and would like to seek public and industry feedback on the appropriate length of a sunrise period. During the “sunrise” period, a transition team, which will eventually form the DPC, will be set up to conduct awareness-building activities for both businesses and consumers in relation to their rights and obligations under the DP Act. These activities will be targeted at enhancing organisations’ ability to comply with the DP Act when it comes into effect. Guidelines will also be published on various issues that may assist with organisations’ efforts to comply with the DP Act, and more information on these guidelines and awareness building activities will be available at a later stage of the development of the DP Act.

Questions in relation to transitional arrangements:

Question 19: Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?

Existing personal data

4.15 Up till the effective date of the DP Act, organisations may already control personal data previously collected (“existing personal data”). Such data may or may not have been collected or used in accordance with the provisions of the DP Act. There are several possible ways to cater to existing personal data. They include exempting such data from the DP Act (i.e., the provisions in the DP Act will not apply at all to personal data collected by organisations before the effective date of the DP Act), or requiring that all existing personal data controlled by organisations be compliant with the DP Act (i.e., organisations will have to check and ensure that all personal data under their control comply with the new rules, including deleting personal data of individuals where consent has not been obtained for the specific purpose).

4.16 While the former option would appear to lower the compliance costs of the DP Act for organisations, it will be complex to determine whether a particular piece of personal data was collected before or after the effective date of the DP Act, if a case of non-compliance with the DP Act was alleged. It may also cause organisations to incur some costs in auditing the existing personal data under their control.

4.17 As a balanced measure, MICA’s proposal is to deem that consent was already given by the individual concerned for the organisation to use and/or process existing personal data. This would however be restricted to reasonable existing uses, taking into account the nature of the organisation’s business. As such, the DP Act would not invalidate organisations’ existing contractual agreements on the use of customers’ personal data, nor require organisations to obtain explicit consent for the continued use and processing of their personal data.

4.18 After the effective date of the DP Act, however, fresh consent would need to be obtained if an organisation intends to use existing personal data for a new or

different purpose. As an example, if a company has been using its customer's personal data to provide after-sales customer support prior to the new DP Act, it can continue to do so after the DP Act comes into effect, even if it did not obtain explicit consent previously. However, if it now wants to use the same personal data for direct marketing where it had not done so previously, this would be considered a new use for which consent will need to be obtained. Similarly, organisations would need to obtain consent if they wish to disclose the existing data, if they did not previously obtain consent for the disclosure in a manner consistent with the DP Act.

4.19 While we recognise that the above approach may pose some implementation complexities, particularly in deciding what would constitute an "existing use", this approach achieves the best balance between protecting consumer interest in relation to their personal data, and the need to manage the compliance costs of organisations.

Questions in relation to transitional arrangements:

Question 20: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate?

Question 21: With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?

Question 22: Are there certain organisations that may require different transitional arrangements?

PART V: NATIONAL DO-NOT-CALL REGISTRY

5.1 A related issue to DP is the use of individuals' personal contact information (particularly telephone numbers) by organisations for unsolicited telemarketing purposes. Such personal contact information may have been collected by organisations directly from the individual for a different purpose (i.e., for the purposes of providing a service). However, unsolicited telemarketing calls are increasingly made by organisations that do not currently have or previously had a working relationship with the individual (i.e. the personal contact information was collected through other means).

5.2 Today, a form of industry self-regulation on telemarketers exists in the voluntary Code of Ethics put out by the Contact Centre Association of Singapore ("CCAS")²⁷. This Code of Ethics is a comprehensive list of guidelines to

²⁷ CCAS is an association formed in August 2005 and is developed from a sub-association of Direct Marketing Association of Singapore, and has the full backing of the Association of Banks of Singapore, General Insurance Association of Singapore, and Insurance and Financial Practitioners Association of Singapore. The CCAS comprises of members from the telemarketing community and promotes the interest of telemarketers in Singapore.

telemarketers in Singapore, which includes the setting up and maintenance of organisation-specific Do-Not-Call (“DNC”) lists. Consumers can request to opt-out of telemarketing calls by an organisation which has adopted the said Code, by listing their numbers on that organisation’s DNC list. In addition, for sectors which have in place sectoral frameworks that impose various requirements on telemarketing activities, organisations operating in those sectors will also be bound by these requirements²⁸.

- 5.3 As the Code of Ethics is a voluntary code, it does not contain an enforcement mechanism and is only applicable to members of the CCAS. There is thus a limit to the extent the current self-regulatory regime can address consumer expectations of compliance and enforceability. As such, the volume of unsolicited telemarketing and the level of public dissatisfaction with telemarketing have been increasing over the years.
- 5.4 MICA notes that several other jurisdictions have provided for a national DNC registry in addition to DP laws. While the latter prevents personal data from being used in a manner not consented to by the individual and allows for consent to be withdrawn, the former provides the individual a simple and effective way to opt-out of all telemarketing messages without having to manually withdraw consent from every organisation for the purposes of telemarketing.
- 5.5 MICA is similarly considering whether to set up a national DNC registry, where individuals will be able to register their phone numbers to opt-out of unsolicited telemarketing calls, SMS and fax messages²⁹ from all organisations in Singapore. With a national DNC registry, organisations will be required by law to check the registry and ensure that they do not make telemarketing calls or send SMS/fax messages to the numbers registered, unless the individual had specifically given their consent for the organisation to call/send them telemarketing messages. The proposed DNC registry will be administered by a new independent body set up specifically for this purpose.
- 5.6 While a national DNC registry may impose additional compliance costs on organisations engaging in telemarketing activities, telemarketers will benefit by being able to effectively target a genuine group of consumers who are interested in receiving information on the organisation’s products/services, and eliminate time and resources wasted on those who do not wish to be disturbed. This will also preserve the viability of telemarketing as a credible marketing medium.

²⁸ For example, the Council for Estate Agents recently published “Practical Guidelines on Ethical Advertising” which, among others, state that “*where a recipient has indicated not to receive future cold calls or SMS, the estate agent or salesperson shall cease to do so immediately. Such SMS advertising and cold calling shall also not be carried out between 10.00pm and 9.00am*”.

²⁹ Email messages are not likely to be included within the scope of the proposed DNC registry, as unsolicited emails can be mitigated through email filters, and cause less of a nuisance to delete when received, as compared to phone calls, SMS and fax messages, which are more difficult to filter off by the individual.

- 5.7 MICA would like to seek feedback on whether a national DNC registry should be set up in Singapore. Further public consultation will be sought with regard to the details of the proposed regime³⁰.

Questions in relation to proposed National Do-Not-Call registry:

Question 23: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?

PART VI: SUBMISSION OF COMMENTS

- 6.1 MICA would like to seek the views and comments on the above issues as well as relevant issues that may not have been specifically highlighted above.
- 6.2 Parties that submit comments on this consultation paper should organise their submissions as follows:
- a. Cover page (including particulars of the organisation and contact person);
 - b. Summary of major points;
 - c. Comments; and
 - d. Conclusion.
- 6.3 Supporting material may be placed in an Annex.
- 6.4 All submissions should be clearly and concisely written, and should provide a reasoned explanation for any proposed revisions. Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.
- 6.5 All submissions should reach MICA **before 25 October 2011, 5pm**. Comments should be submitted in soft copy (in Microsoft Word format), with the email header “**Public Consultation of the Proposed Consumer Data Protection Regime for Singapore**”, to the following e-mail address: MICA_DP_Public_Consultation@mica.gov.sg.
- 6.6 Commenting parties may request confidential treatment for any part of their submission that the commenting party believes to be confidential or sensitive. Any such information should be clearly marked within the submission.

³⁰ Such as the scope of activities that constitute telemarketing and the enforcement regime.