



**SINGAPORE TELECOMMUNICATIONS LTD**

**SUBMISSION TO THE PERSONAL DATA PROTECTION COMMISSION OF  
SINGAPORE**

**IN RESPONSE TO THE**

**PUBLIC CONSULTATION ON PROPOSED ADVISORY GUIDELINES ON  
SELECTED TOPICS IN THE PERSONAL DATA PROTECTION ACT (“ACT”)**

**DATE OF SUBMISSION: 1 APRIL 2013**



## **TABLE OF CONTENTS**

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>2</b>	<b>GENERAL COMMENTS</b>	<b>2</b>
<b>3</b>	<b>SPECIFIC COMMENTS</b>	<b>2</b>

## SINGAPORE TELECOMMUNICATIONS LTD

### SUBMISSION TO THE PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE IN RESPONSE TO THE PUBLIC CONSULTATION ON PROPOSED ADVISORY GUIDELINES ON SELECTED TOPICS IN THE PERSONAL DATA PROTECTION ACT (“ACT”)

#### 1 INTRODUCTION

- 1.1 Singapore Telecommunications Limited and its related companies (“**SingTel**”) are licensed to provide info-communications services in Singapore. SingTel is committed to the provision of state-of-the-art info-communications technologies and services in Singapore.
- 1.2 SingTel has a comprehensive portfolio of services that includes voice and data services over fixed, wireless and Internet platforms. SingTel services both corporate and residential customers and is committed to bringing the best of global info-communications to its customers in the Asia Pacific and beyond.
- 1.3 SingTel is also a leading Internet service provider (“**ISP**”) in Singapore and has been at the forefront of Internet innovation since 1994, being the first ISP to launch broadband services in Singapore. It is licensed to offer IPTV services under a nationwide subscription television licence granted by the Media Development Authority of Singapore (“**MDA**”).
- 1.4 SingTel welcomes the opportunity to comment on the Proposed Advisory Guidelines on Selected Topics in the Personal Data Protection Act (“**Act**”) (“**Proposed Advisory Guidelines**”).
- 1.5 This submission is structured as follows:
  - (a) Introduction;
  - (b) General comments; and
  - (c) Specific comments.

## 2 GENERAL COMMENTS

- 2.1 SingTel considers that the Proposed Advisory Guidelines provides the telecommunications sector and persons subject to the Act with a reasonable degree of guidance about the nature of some of their obligations under the Act and how these obligations are likely to be construed for compliance purposes. This guidance is particularly helpful at this point in time, as organisations take steps to implement the requirements of the new privacy regime under the Act.
- 2.2 SingTel also considers that there is merit in the PDPC increasing the level of detail in the regulations to be made under the Act to allow organisations to undertake more comprehensive planning and development of their internal processes and operations as part of the transition to the new regime, and to ensure clarity in both scope and operation of the regulations themselves.
- 2.3 SingTel submits its specific comments below.

## 3 SPECIFIC COMMENTS

### *Consent to collect and use personal data of job applicants (Ref p.5.5)*

- 3.1 The PDPC indicates that organisations would need to obtain consent (or else consent could be deemed to have been given) from job applicants to collect, use and disclose personal data. Paragraph 5.5 of the Proposed Advisory Guidelines in does not seem to exhaustively cover whether organisations are expected to permit withdrawal of consent as well. We seek confirmation that this is not required.
- 3.2 However, where withdrawal is expected to be facilitated or an individual does not provide the consent, the PDPC has separately highlighted (in the Proposed Advisory Guidelines on Key Topics) that organisations highlight to individuals the consequences, eg the contract may have to be terminated, the individual may have to pay termination charges etc. In the case of job applicants, it is only reasonable that where a job applicant refuses to provide details that are critical, eg whether they have any criminal records or any other important information, the organisation should have the right to reject or decline the application. We seek confirmation that this is the case.

***How long can an organisation keep personal data of job applicants who are not hired (Ref p.5.10)***

- 3.3. Section 25 of the Act state that an organisation must cease to retain personal data once the purpose for which the personal data was collected is no longer served and retention is not necessary for legal or business purposes.
- 3.4. It is highly likely that an organisation will want to retain personal data of job applicants for as long as possible given that it can review the application for future vacancies available within the company or even with related companies<sup>1</sup>. We seek confirmation that as long as the individual gives consent, an organisation is able to retain personal data of job applicants indefinitely for such a purpose.

***Personal data of employees (Ref. p. 5.15 – 5.22)***

- 3.5. Section 5.16 of the Proposed Advisory Guidelines says that employees can withdraw consent given to the use of their personal data. We therefor believe that in relation to employee data, the Act needs to provide for a more flexible approach towards the use of personal data of employees. The exception in Section 20(4) of the Act for example, covers the collection, use and disclosure of employee data for determining suitability, eligibility, qualifications of an employee for promotion, continuation of employment contract but do not extend to the collection, use and disclosure for ongoing operations to service that contract.
- 3.6. To overcome this, we suggest that the PDPC adopts a broader view of what constitutes maintaining and termination of employment, apart from determining suitability, eligibility, qualifications of an employee for promotion, continuation of employment contract.
- 3.7. To cite an example, organisations have intranet sites that house the information of various employees, ranging from the employee's qualifications to their photo images. All employees are encouraged to provide such information and in some cases, the information is mandatory, eg photo images of the employees are placed on the intranet site. It does not appear logical that an employee can withdraw consent for their photo image to be placed on the intranet site when this may even cause internal discord as to why one employee is treated differently from another. Another example would be

---

<sup>1</sup> These involves subsidiaries of a holding company or otherwise sibling companies.

where an employee is being investigated for disciplinary purposes; it is not clear whether this suffices as use of personal data for maintaining or terminating employment.

- 3.8. Using a strict reading of the Act, an individual cannot expect an organisation to use its personal data in the situations above and can in fact withdraw consent in which case an option is for the organisation to terminate the employment contract. This does not appear logical. We therefore urge that the PDPC reviews this and provides a better set of guidelines in relation to the exception in Section 20 (4) of the Act, ie adopt a broader view of what purposes and activities would qualify for the exception in Section 20 (4) of the Act.

***Personal data of ex-employees (Ref. p. 5.23)***

- 3.9. We refer to our comments above in relation to retention of personal data of job applicants not hired. It is also highly likely that an organisation will want to retain personal data of ex-employees for as long as possible given that it can review the application for future vacancies. We seek confirmation that as long as the individual gives consent, an organisation is able to retain personal data of ex-employees indefinitely for such a purpose.
- 3.10. This retention policy may even extend to ex-employees who had been dismissed for poor performance or disciplinary reasons. Their personal data, including the reasons for dismissal or termination of employment have to be retained for as long as possible, without the need for consent from the ex-employee so that the organisation can evaluate the individual properly in the event the individual applies to work with the organisation in future. We also ask that the access obligation not apply in such cases.

***Anonymisation (Ref. p. 4.9)***

- 3.11. We seek confirmation on the following - where an organisation applies anonymisation and the anonymisation logic / technique stays with the organisation / data owner who then shares the anonymised data with third parties, will the data still be considered as personal data for the purpose of the Act.