Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( ) Class: \_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_

**Lesson 1: Data Protection under PDPA**

**Instructional Objectives:**

By the end of this task, you should be able to:

* Understand the need for privacy of data.
* Explain how data in Singapore is protected under the Personal Data Protection Act (PDPA) to govern the collection, use and disclosure of personal data.

**What is data privacy?**

Data privacy is the requirement for data to be accessed by or disclosed to authorised persons only. It is important that unauthorised people do not have access to data they are not supposed to have. Unfortunately, in today’s digitised society, it is easier than ever to gather a person’s data and use it to obtain valuable insights, track his/her movements or to commit fraud.

For instance, data on which websites you visit often can reveal which products you are more likely to purchase as a shopper. This information can be highly valuable to an advertiser. As more services become available online, the risk of fraudent use of data increases. For instance, with a photo of your identity card, a person can impersonate you and register for a new phone line on a telco website. (Previously such a transaction would have required the person to personally register over the counter with the physical identity card.) As technology becomes increasingly powerful, machines can gather information on a person easily, like performing facial recognition on surveillance videos to track down the whereabouts of an individual in a particular area.

We want our personal data to be private so that unauthorised people cannot use our personal data for unauthorised use. In Singapore, personal data[[1]](#footnote-1) is protected under the Personal Data Protection Act (PDPA).

**Review:** Why is data privacy necessary?

**Think:**

Suppose you take a picture of yourself outside your home in your school uniform, and post it on social media to show everyone that you just returned home from school. What personal information can be gathered from the photo?

**What is the PDPA?**

The PDPA is a data protection law comprising various rules that govern the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, as well as the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

It takes into account the following:

* **Consent** – Organisations must obtain an individual's knowledge and consent to collect, use or disclose his/her personal data (with some exceptions).
* **Notification** – Organisations must inform individuals of the purposes for collecting, using or disclosing their personal data.
* **Appropriateness** – Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person under the given circumstances.
* **Accountability** – Organisations must make information about their personal data protection policies available on request. They should also make available the business contact information of the representatives responsible for answering questions relating to the organisations’ collection, use or disclosure of personal data.

To administer and enforce the PDPA, Singapore set up the Personal Data Protection Commission (PDPC) in 2013.

**Do Not Call Registry**

Have you received calls from unknown companies who seem to know your name and perhaps try to sell products to you? Your telephone number could have been gathered from unexpected sources, such as a lucky draw form that you filled up long ago. With technology, companies can easily gather and consolidate personal information. In fact, it can even automate the making of such calls.

To prevent you from getting unnecessary marketing calls, you can register in the Do Not Call (DNC) Registry to opt out of marketing messages and calls. The PDPA prohibits organisations from sending marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers that are registered with the DNC Registry.

There are three DNC registers that individuals can choose to register in:

* No Voice Call Register
* No Text Message Register
* No Fax Message Register

Registering the phone number in each register is to opt out of receiving marketing messages through voice calls, text messages and fax messages.

Note that organisations which have an ongoing relationship with a subscriber or user of a Singapore telephone number may send marketing messages on similar or related products, services and memberships to that Singapore telephone number via text or fax without checking against the DNC Registry. However, each exempt message must also contain an opt-out facility that the recipient may use to opt out from receiving such telemarketing messages. If a recipient opts out, organisations must stop sending such messages to his/her Singapore telephone number after 30 days. This means that, for instance, you can get a marketing message from your mobile phone company even if you listed the number in the DNC Registry. However, the message will include a link for you to opt out from receiving their marketing messages. Once you opt out, the mobile phone company can no longer send you marketing messages on that number.

**Use of NRIC**

The Singapore National Registration Identification Card (NRIC) number is a unique idenfier assigned to Singapore citizens and permanent residents. Similarly, the Foreign Identification Number (FIN) is a unique identifier that is assigned to foreigners. The NRIC/FIN contains personal information about the person, such as his/her date of birth and address. As unique identifiers like NRIC and FIN are permament, irreplaceable and used in a variety of government transactions, we need to be careful with such data.

Individuals should not readily provide their NRIC/FIN and personal particulars to companies/strangers. Consent is required before organisations can obtain a person’s data. Under the PDPA, from 1 September 2019, organisations[[2]](#footnote-2) are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC) except in the following circumstances:

* Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA applies); or
* Collection, use or disclosure of NRIC numbers (or copies of NRIC) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

For example, a medical clinic needs to see the NRIC of a patient to identify the person. The clinic will need to keep the name, address, NRIC and contact number of the person with the medical notes for future reference. The PDPA allows for that. However, a shopping mall cannot collect the photographs of NRICs of all the shoppers that want to participate in their lucky draw. It is unnecessary to collect the photographs to verify the lucky draw participant. Instead, the participants can be identified with their mobile number, or be asked to give the last 4 characters of the NRIC (i.e. partial NRIC) for verification purposes. This reduces the security risks if the data collected is unintentionally revealed.

**Ponder:**

1. When can a handphone company ask for your NRIC?
2. What should the company do to ensure that your data is protected?

**Data Obligations**

Organisations are required to abide by the following 9 main personal data obilgations:

**1. Consent Obligation**

Only collect, use or disclose personal data for purposes for which an individual has given his or her consent.

**2. Purpose Limitation Obligation**

An organisation may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

**3. Notification Obligation**

Notify individuals of the purposes for which your organisation is intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.

**4. Access and Correction Obligation**

Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been used or disclosed within a year before the request should be provided. However, organisations are prohibited from providing an individual access if the provision of the personal data or other information could reasonably be expected to cause harmful effects. Organisations are also required to correct any error or omission in an individual’s personal data that is raised by the individual.

**5. Accuracy Obligation**

Make reasonable effort to ensure that personal data collected by or on behalf of your organisation is accurate and complete, if it is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

**6. Protection Obligation**

Make reasonable security arrangements to protect the personal data that your organisation possesses or controls to prevent unauthorised access, collection, use, disclosure or similar risks.

**7. Retention Limitation Obligation**

Cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.

**8. Transfer Limitation Obligation**

Transfer personal data to another country only according to the requirements prescribed under the regulations, to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA, unless exempted by the PDPC.

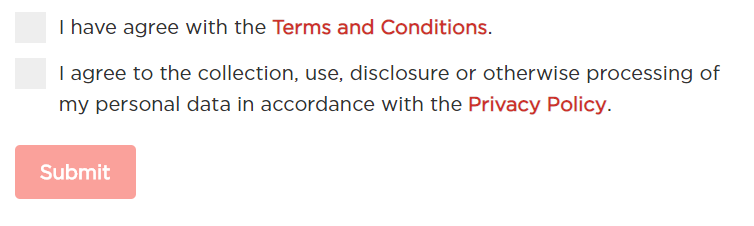
**9. Accountability Obligation**

Make information about your data protection policies, practices and complaints process available on request. Designate a Data Protection Officer to ensure that your organisation complies with the PDPA.

More information on PDPA are available at the PDPC website: <http://www.pdpc.gov.sg/>

**Protecting your Personal Data**

You can take various measures to protect your personal data. Don’t reveal your personal data to unknown sources. For phone calls, ensure that the caller is who he or she is before giving your personal information. For websites and applications, read the privacy or data protection policies of the website to understand how your data is used. Websites/applications require you to explicitly agree with the terms when you submit the data. An example is shown below.



Please note that once you agreed, the company can contact you, even if your number is listed in the Do Not Call Registry. If you have queries on personal data, or to withdraw consent, you can contact the data protection officer (DPO). Under PDPA, companies are required to appoint one or more persons to be DPO to oversee the data protection responsibilities within the organisation and ensure compliance with the PDPA.

Also be careful when throwing away paper containing your personal data such as application forms or letters from schools/banks. Tear or shred the paper so that people cannot use the paper to obtain personal data about yourself.

**References**

1. Burdett, A. (2016). *BCS glossary of computing*. BCS Learning and Development Limited.
2. LANGFIELD, S. D. (2015). *Cambridge International AS and A Level Computer Science Coursebook*. Place of publication not identified: Cambridge University Press.
3. Watson, D., & Williams, H. (2019, May 31). Cambridge International AS & A Level Computer Science. London: Hodder Education
4. Personal Data Protection Commission Singapore. (2018, August 7). Personal Data Protection Act Overview. Retrieved from <http://www.pdpc.gov.sg/Guidelines/Personal-Data-Protection-Act-Overview>.
5. Personal Data Protection Commission Singapore. (2019, September 26). Guide to Notification. Retrieved from <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Notification-260919.pdf>.
6. Personal Data Protection Commission Singapore. (2019, September 26). Data Protection and Your Organisation. Retrieved from <https://www.pdpc.gov.sg/Organisations/Organisations-Overview>.
7. Personal Data Protection Commission Singapore. (n.d.). [2019] SGPDPC 6. Retrieved from <https://www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases>

**For teacher’s reference: Possible Answers**

**Think**

The person’s home address and school can be inferred from the photograph.

**Ponder**

1. A handphone company can ask for your NRIC to verify your identify (e.g. to check that you are indeed the person registering for a new mobile phone). The company may obtain the NRIC number to run necessary checks. For example, by law, each person is allowed to register up to 3 prepaid cards. The company uses your NRIC number to check that you have not exceeded the limit.
2. The company should ensure that the data is stored securely, for example: encrypted and stored in an intranet rather than on the Internet. There should be user authentication required before someone is allowed to access the data.

**Apply**

1. Was the Personal Data Protection Act (PDPA) breached? If yes, in what ways? If no, why?

Yes. The teacher released the personal data of some parents to other parents without their permission.

1. Give examples of the personal data obtained by the teacher.

Name, contact number, identity number

1. What precautions can the teacher take to prevent a similar incident from happening?

The teacher shoud have messaged each parent directly to remind the parents of the school trip rather than messaging everyone in a group chat to minimise the possibility of accidental leakage of personal data.

1. What should the teacher do to the personal data obtained after the school trip?

The teacher should delete the personal data if they are not required after the school trip. Any printed copy of the data should be shredded to prevent leakage of personal data.

1. Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. [↑](#footnote-ref-1)
2. Note that PDPA does not apply to public agencies and organisations acting on behalf of them, thus, for example the police can collect your personal information, including NRIC/FIN. Data collected by public agencies are protected by other acts. See <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/2/mcis-response-to-pq-on-public-agencies-exemption-from-pdpa> for more information. [↑](#footnote-ref-2)