PERSONAL DATA PROTECTION COMMISSION SINGAPORE

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

Learners Guide

Name

Date

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Learner's Guide

Competency Unit	Facilitate Compliance with Legislative and Regulatory Requirements
Competency Category	Enterprise Risk Management
Competency Unit Code	BM-RM-301E-1
Version Number	2.0 Current 2.2
Effective Date	30 August 2016

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Version Control Record

Version	Effective Date	Changes	Author
1.0	2 April 2014	Original Version	PDPC
1.1	6 June 2014	▪ Changed appointment date to day to Para 2.11 on "Existing Data and Other Existing Laws" ▪ Added access and correction obligation and transfer limitation obligation	PDPC
1.2	14 Oct 2014	▪ Added photography as a new area under "Selected Topics" ▪ Removed duplicate question in updated Business Checklist	PDPC
1.3	10 July 2015	▪ Replaced '500' free credits with '1,000' free credits on page 88 ▪ Provided clarity on lucky draw example under Consent Obligation, Valid and Not Valid Consent – Example 2, page 23.	PDPC
2.0	30 Aug 2016	Added the following topics : ▪ Introduction to Data Protection Frameworks Around the World ▪ Enforcement ▪ Managing Data Breaches Updated the following topics: ▪ Consent Obligation (Withdrawal of Consent, Sample Clauses on Obtaining & Withdrawal Consent) ▪ Access & Correction Obligation (Guide to Handling Access Requests) ▪ Selected Topics – CCTV ▪ Ranamed course title to "Fundamentals of the Personal Data Protection Act"	PDPC

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Note

The contents herein are intended to give a general introduction to data protection law in Singapore and do not cover all information available on a particular issue. The contents herein are not intended to be an authoritative or complete statement of the law or a substitute for legal advice. Nothing herein modifies or supplements in any way the legal effect or interpretation of any laws including, but not limited to, the Personal Data Protection Act (PDPA) and any subsidiary legislation (such as regulations and rules) issued under the PDPA. The Personal Data Protection Commission (PDPC) makes no representations or warranties and disclaims any warranty, including but not limited to any representations or warranties as to the accuracy, completeness, correctness, reliability, currency, non-infringement, title, merchantability quality or fitness of the contents herein. To the fullest extent permitted by law, the PDPC, the Info-communications Development Authority of Singapore (IDA) and their respective members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind arising directly or indirectly as a result of any use of or reliance on this publication.

Nothing herein shall be construed to limit or restrict the PDPC's administration and enforcement of the PDPA. The contents herein shall not be relied on to claim or assert any form of legitimate expectation against PDPC, whether procedural or substantive in nature, in respect of any action that PDPC may or may not take in the exercise of its discretion as a public authority. PDPC reserves the right to change, modify, add to, derogate from or vary any position referred to in this publication at any time in PDPC's sole and absolute discretion without prior notice to you. Any party should obtain its own professional and/or legal advice relevant to its particular circumstances and conduct all necessary due diligence, including but not limited to making such other investigations or seeking clarifications as may be appropriate, as regards any decision or action that it intends to take in relation to any matter concerning the contents herein.

COPYRIGHT April 2014 – Personal Data Protection Commission Singapore and Infocommunications Development Authority of Singapore

The contents of this publication are protected by copyright, trade mark and other forms of proprietary rights. All rights, title and interest in the contents are owned by, licensed to or controlled by the PDPC and/or IDA, unless otherwise expressly stated. This publication may not be modified, reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Content

Competency Unit: Facilitate Compliance with Legislative and Regulatory Requirements (BM-RM-301E-1)	**7 - 11**
Course Overview	7
Course Lesson Plan	8
1. Introduction to Personal Data Protection Act (PDPA)	**12 - 36**
1.1 Objectives of Data Protection Regime	13
1.2 Key Terms – Personal Data, Business Contact Information (BCI), Individual & Organisations, Data Intermediary and Other Key Terms	16
1.3 Who will Not be Impacted	27
1.4 Introduction to Data Protection Frameworks Around the World	29
2. Data Protection Provisions and Do Not Call Provisions	**37 - 163**
2.1 PDPA 9 Key Obligations	38
2.2 Consent Obligation	39
2.3 Purpose Limitation Obligation	62
2.4 Notification Obligation	65
2.5 Access & Correction Obligation	70
2.6 Accuracy Obligation	83
2.7 Protection Obligation	86
2.8 Retention Limitation Obligation	94
2.9 Transfer Limitation Obligation	98
2.10 Openness Obligation	103
2.11 Existing Data and Other Existing Laws	105
2.12 Selected Topics – Employment, NRIC	109
2.13 Selected Topics – Photography, CCTV, Anonymisation, Research & Analytics, Online Activities	117
2.14 Do Not Call Provisions - DNC Registry – Specified Message and Examples - Exemption Order - DNC Operational Rules - Spam Control Act	131
2.15 Enforcement	150

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Content

3.	**Role of Data Protection Officer (DPO)**	**164 -173**
3.1	Appointment of DPO	165
3.2	Functions of a DPO	166
3.3	Governance Structures	167
4.	**Create An Organisation's Data Inventory Map (DIM) and Identify Possible Areas of Non-Compliance**	**174 - 177**
4.1	What is a DIM and How to Create One for the Organisation	175
4.2	Example of a DIM	176
5.	**Develop a Process for Dispute Resolution**	**178 - 188**
5.1	Typical Complaint Handling Process	179
5.2	What to Consider When Developing Process for Handling Complaints Relating to Data Protection	180
5.3	Example of Complaint Handling Process Relating to Data Protection	185
6.	**Training and Communications to Staff for Compliance to Data Protection Provisions**	**189 - 203**
6.1	Objectives and Outcomes of Staff Training and Communications	191
6.2	What to Consider When Developing a Training and Communications Plan	193
6.3	Example of a Training and Communications Plan	199
7.	**Managing Data Breaches**	**205 - 212**
7.1	What is a Data Breach and How Data Breach Could Occur	206
7.2	Responding to a Data Breach	207
	Annex A - Sample Access Request Form	**213 - 214**
	Annex B - Personal Data Protection Checklist for Organisations	**215 - 223**
	Annex C – Exceptions, Exemptions, Exclusions	**224 - 229**
	Annex D – Case Studies	**230 - 240**
	Other Resources	**241**

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Competency Unit: Facilitate Compliance with Legislative and Regulatory Requirements (BM-RM-301E-1)

Target Audience

The participants for this programme are likely to be:

- Compliance Managers or Data Protection Officers (DPOs); and
- Human Resource, Admin, IT personnel, Sales and Business Development Executive / Managers who need to be involved in data protection matters.

Assumed Skills and Knowledge

Participants are assumed to be able to:

- Understand relevant organisational strategies, objectives, culture, policies, processes and products / services;
- Have information gathering skills to gather and collate necessary data;
- Have analytical skills to assess policies and procedures;
- Have business writing skills to prepare management report;
- Have interpersonal and communication skills to interact with relevant stakeholders;
- Have facilitation skills to ask the right questions to elicit necessary information; and
- Be aware of compliance requirements of organisation.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Lesson Plan – Facilitate Compliance with Legislative and Regulatory Requirements (2 Days)

Time (Hours)	Lesson Plan – Day 1 – Lesson / Activities
0900 to 0930	Welcome Message • Self-Introduction for Trainer and Participants • Course Overview
0930 to 1015	**Chapter 1: Introduction to Personal Data Protection Act (PDPA)** 1.1 Objectives of the Data Protection Regime 1.2 Key Terms – Personal Data, Business Contact Information (BCI), Individual & Organisations, Data Intermediary , Definitions of exclusions, exemptions and exceptions and Other Key Terms 1.2 Who Will Not be Impacted? 1.3 Introduction to Regional Data Protection Frameworks Around the World
1015 to 1030	**Tea Break**
1030 to 1230	**Chapter 2: Data Protection Provisions and Do Not Call Provisions** 2.1 PDPA 9 Key Obligations 2.2 Consent Obligation 2.3 Purpose Limitation Obligation 2.4 Notification Obligation 2.5 Access & Correction Obligation 2.6 Accuracy Obligation 2.7 Protection Obligation 2.8 Retention Limitation Obligation 2.9 Transfer Limitation Obligation 2.10 Openness Obligation
1230 to 1330	**Lunch Break**
1330 to 1430	Chapter 2: Data Protection Provisions and Do Not Call Provisions 2.11 Existing Data and Other Existing Laws 2.12 Selected Topics – Employment, NRIC

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Lesson Plan – Facilitate Compliance with Legislative and Regulatory Requirements (2 Days)

Time (Hours)	Lesson Plan – Day 1 – Lesson / Activities
1430 to 1530	**Chapter 2: Data Protection Provisions and Do Not Call Provisions** 2.13 Selected Topics – Photography, CCTV, Anonymisation, Research & Analytics, Online Activities 2.14 Do Not Call Provisions - DNC Registry – Specified Message and Examples - Exemption Order - DNC Operational Rules - Spam Control Act 2.15 Enforcement
1530 to 1545	**Tea Break**
1545 to 1655	**Chapter 3: Role of Data Protection Officer (DPO)** 3.1 Appointment of DPO 3.2 Functions of a DPO 3.3 Governance Structures
1655 to 1740	**Learning Activity 1** • Group discussion & presentation on how a DPO can perform the following within their organisation: - Setting up policies and processes for compliance with the PDPA - Identify and document possible areas of non-compliance - Auditing for compliance
1740 to 1800	**Summary of Day 1**

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Lesson Plan – Facilitate Compliance with Legislative and Regulatory Requirements (2 Days)

Time (Hours)	Lesson Plan – Day 2 – Lesson / Activities
0900 – 1000	**Assessment Activity 1**
1000 – 1015	**Tea Break**
1015 – 1130	**Chapter 4: Create An Organisation's Data Inventory Map (DIM) and Identify Possible Areas of Non-Compliance** 4.1 What is a DIM and How to Create One for the Organisation 4.2 Example of a DIM
1130 – 1210	**Chapter 5: Develop a Process for Dispute Resolution** 5.1 Typical Complaint Handling Process 5.2 What to Consider When Developing Process for Handling Complaints Relating to Data Protection 5.3 Example of Complaint Handling Process Relating to Data Protection
1210 – 1310	**Lunch Break**
1310 – 1340	**Learning Activity 2 – Process for Dispute Resolution** Develop a Process for Dispute Resolution Arising From a Breach of One of the 9 Key Obligations
1340 – 1430	**Chapter 6: Training and Communications to Staff for compliance to Data Protection Provisions** 6.1 Objectives and Outcomes of Staff Training and Communications 6.2 What to Consider When Developing a Training and Communications Plan 6.3 Example of a Training and Communications Plan **Chapter 7: Managing Data Breaches** 7.1 What is a Data Breach and How Data Breach Could Occur 7.2 Responding to a Data Breach

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Lesson Plan – Facilitate Compliance with Legislative and Regulatory Requirements (2 Days)

Time (Hours)	Lesson Plan – Day 2 – Lesson / Activities
1430 – 1535	**Learning Activity 3 - Communications Plan and Management Report Writing** • Create a training and communications plan and a management report based on a given case.
1535 – 1545	**Tea Break**
1545 – 1745	**Assessment Activity 2**
1745 – 1800	**Sharing on "Case Studies from DPO Connect e-Newsletter"**
1800	**End of Course**

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 1:
INTRODUCTION TO PERSONAL DATA PROTECTION ACT (PDPA)

At the end of this chapter, participants will be able to have an overview of the PDPA, understand the key terms and the level of impact to organisations.

- *Objectives of the Data Protection Regime*
- *Key Terms – Personal Data, Business Contact Information (BCI), Individual & Organisations, Data Intermediary and Other Key Terms*
- *Who Will Not be Impacted?*
- *Introduction to Data Protection Frameworks Around the World*

For more information on the PDPA, please refer to Advisory Guidelines on the key concept in the Personal Data Protection Act (revised on 9 Jun 2016.)

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

1.1 OBJECTIVES OF THE DATA PROTECTION REGIME



Notes

Individual Interest

- Puts in safeguards to protect individuals' data from misuse by regulating proper management of personal data.
- Gives individuals greater control over their personal data.

Economic Interest

- Strengthens Singapore's position as trusted hub and choice location for data hosting and processing activities thereby enhancing Singapore's overall competitiveness.
- Facilitates cross-border transfer.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.1 OBJECTIVES OF THE DATA PROTECTION REGIME

Approach for the Data Protection Regime



- Protects individuals' personal data, while ensuring national interest, government functions & public service delivery not unduly impeded.
- Helps businesses gain consumer confidence through proper handling of personal data.
- Keeps compliance costs manageable, sufficient to address economic objectives.
- Takes into account international standards, to enhance Singapore's status as trusted hub for data management and processing activities.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.1 OBJECTIVES OF THE DATA PROTECTION REGIME

Overview of PDPA

Notes

The diagram below provides an overview of the various parts of the PDPA which may be relevant to organisations. Generally, there are 2 main sets of provisions that organisations are required to comply with - the Data Protection (DP) Provisions and Do Not Call (DNC) Provisions

Purpose of Act

"To govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances"



2 Main Sets of Provisions

Data Protection Provisions (Parts III - VI)				**DNC Provisions (Part IX)**
General Rules (Part III) - Compliance with Act - Policies and practices	Collection, Use and Disclosure (Part IV) - Consent - Purpose Exceptions: - 2nd, 3rd and 4th Schedules	Access and Correction (Part V) - Access - Correction Exceptions: - 5th and 6th Schedules	Care (Part VI) - Accuracy - Protection - Retention - Transfer outside Singapore	DNC Registry (Part IX) - Meaning of "specified message" - Application Exceptions: - 8th Schedule - Exemption Order

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Scope of Application – Personal Data

Notes

Eg. NRIC, photo.

Definition

"Personal data" refers to data about an individual who can be identified from that data; or from that data & other info that the organisation has or is likely to have access.

Covers *electronic & non-electronic* data;

Focuses on protection of personal data, regardless of whether data is *true or false*

Personal Data of Deceased Individuals	• Only disclosure & safeguarding rules apply • Protection for up to 10 years after death

* Whether data is correct or not, is immaterial. So long data can be used to identify a person, that is personal data.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Personal Data – Examples

Example 1: Unique identifiers

NRIC Number – "S1234567A"

Example 2: Set of data which when put together would identify an individual:

Name, age, occupation, address – "Jack Lim, 36 years old, civil servant, lives at Block 123 Bishan Street 23"

Example 3: Personal data may include the following:

- Full name;
- NRIC, FIN or passport number;
- Photograph or video image of an individual;
- Mobile telephone number;
- Personal email address;
- Thumbprint;
- DNA profile;
- Name and residential address; and
- Name and residential telephone number

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Business Contact Information (BCI)

Notes

Definition:

"Business contact information" is defined in the PDPA as "an individual's name, position name or title, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

- Parts III to VI (Data Protection Provisions) of the PDPA do not apply to BCI
- The definition of business contact information is dependent on the purpose(s) for which such contact information is provided by an individual

BCI:
Insurance Agent's name cards
Eg. Real Estate Agent's name cards
Taxi driver's name cards



Not Personal Data coz used for facilitating business / course of work

But if drop name card into fish bowl at restaurant ⇒ is personal data to register membership

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Business Contact Information – Examples

Notes

Example 1: BCI – Information Not Provided Solely for Personal Purposes

At the registration booth of a corporate seminar, Sharon drops her business name card into a glass bowl by the side of the registration booth as she wishes to be on the seminar organizer's mailing list for future invitations to similar seminars.

Example 2: Not BCI – Information Provided Solely for Personal Purposes

Sharon signs up for a gym membership. She provides her business name card to the gym staff so that they can record her name and contact details in order to register her for the membership.

The definition of business contact information is dependent on the purpose for which such contact information may be provided by an individual.

Depends on intention

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Individuals and Organisations

Notes

Individuals

- A natural person, whether living or deceased
- Not data relating to corporate bodies and other entities

Organisations

- Any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the law of Singapore, or resident, or having an office or a place of business, in Singapore.

Excluded Organisations

Parts III to VI (Data Protection Provisions) of the PDPA do not impose any obligation on the following organisations:

- Any individual acting in a personal or domestic capacity;
- Any employee acting in the course of his or her employment;
- Any public agency; and (govt agencies)
- Any organisation acting on behalf of a public agency in relation to the collection, use or disclosure

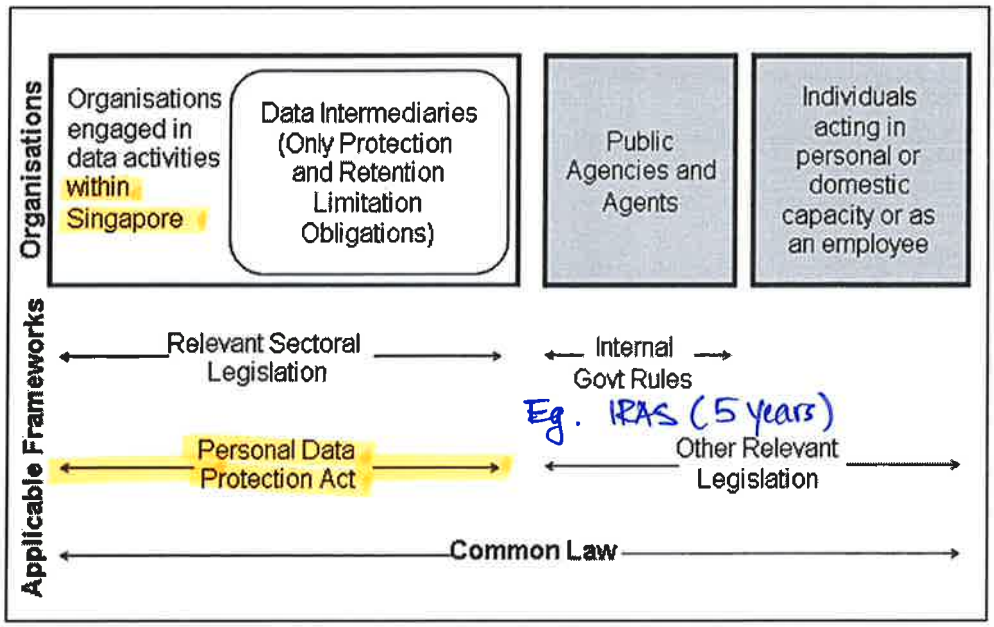


Schools are not under govt agencies. But they are affiliated to MOE, which is a govt agency.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Overview Organisations Covered



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Data Intermediary (DI)

Notes

Definition: (3rd Parties)

"Data Intermediary" refers to an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation.

Processing is the carrying out of any operation or set of operations in relation to the personal data, such as:

- Recording;
- Holding;
- Organisation;
- Adaptation or Alteration;
- Retrieval;
- Combination;
- Transmission;
- Erasure; or
- Destruction.

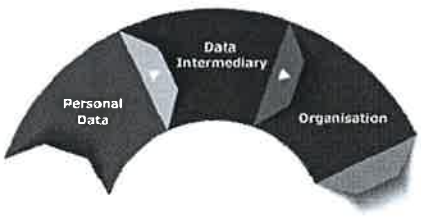
The other obligations are under the organisation which engaged the DI.

Only the Protection Obligation and Retention Limitation Obligation apply in relation to the processing of personal data by a DI –

- on behalf and for the purposes of another organisation,

pursuant to a contract which is evidenced or made in writing.

The other organisation has the same obligations under the PDPA in respect of personal data that is processed on its behalf and for its purposes by a DI as if the personal data were processed by the organisation itself.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Data Intermediary - Examples

Notes

Example 1:

ABC is a market research firm that has been engaged by XYZ. The written contract specifies that ABC has been engaged to collect personal data on behalf of XYZ and produce a report, exclusively for the use of XYZ.

All raw data collected is to be given to XYZ and ABC is not permitted to keep any copies of the data or use it for any other purpose.

Note: ABC is the data intermediary of XYZ and is only subject to the protection and retention provisions. XYZ has the same obligations under the PDPA in respect of the personal data processed by ABC.

Example 2:

XYZ undertakes payroll administration for other organisations, including organisations that belong to the same corporate group. XYZ processes personal data for the other organisations solely for the purpose of payroll administration pursuant to instructions contained within its written contacts.

Note: XYZ is considered a DI in this respect. Possible for an organisation that is part of a corporate group of organisations to act as a data intermediary for other members of the group.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Data Intermediary - Examples

Notes

Example 3:

Whether a professional photographer is a data intermediary processing personal data on behalf of and for the purpose of another organisation pursuant to contract evidenced or made in writing

Abel, a freelance photographer, is hired by Organisation ABC to be its photographer at its private function. Abel and Organisation ABC sign a contract that clearly states (among other things) that Abel will be taking photographs at the function on behalf of and for the purposes of Organisation ABC, and that Organisation ABC will obtain consent from the attendees. In such an instance, Abel will be considered a data intermediary processing personal data on behalf of and for the purposes of another organisation pursuant to a contract that is evidenced or made in writing, and Abel need not obtain consent from the individuals he takes photographs of at the event.

After the function, Abel selects some of the photographs and publishes them on his webpage to promote his work. Abel will not be considered a data intermediary and will be required to comply with the Data Protection Provisions, including obtaining consent from the individuals in the photographs in order to use or disclose the photographs for this purpose.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Agents and Data Intermediaries

- Certain organisations fall within the legal definition of agent, while others simply carry the title of "agent".
- In any case, an agent will have to be assessed as to whether it falls within the definition of "data intermediary", as with any other organisation.
- Thus, an agent that processes personal data on behalf of his principal would be a data intermediary of the principal (if he is not an employee of the principal).
- As good practice, organisations should ensure that their data intermediaries, including appointed agents, are made aware of and exercise proper data protection practices in relation to the handling of personal data.

Cycle & Carriage => An agent (of Mercedes)

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.2 KEY TERMS – PERSONAL DATA, BUSINESS CONTACT INFORMATION (BCI), INDIVIDUAL & ORGANISATIONS, DATA INTERMEDIARY AND OTHER KEY TERMS

Other Key Terms

- **Collection** – actions through which an organisation obtains control over or possession of personal data.
- **Use** – actions by which an organisation employs personal data (may involve collection or disclosure that is necessarily part of use).
- **Disclosure** – actions by which an organisation discloses, transfers or makes available personal data that is under its control or in its possession to any other organisation.
- **Purpose** – refers to objective or reasons.
- **Reasonable** – organisation should take into consideration the circumstances it is facing and determine what would be the appropriate course of action to take in order to comply with its obligations, based on what a reasonable person would consider appropriate.

Note: A "reasonable person" is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgment in the particular circumstances.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.3 WHO WILL NOT BE IMPACTED?

Data Protection Provisions (Parts III to VI) in the **PDPA do not apply to**:

- Any individual acting in a personal or domestic capacity;
- Any employee acting in the course of his or her employment with an organisation;
- Any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data; and
- Business contact information. (BCI)



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.3 WHO WILL NOT BE IMPACTED?

Assessment of Impact on Organisations – An Example

Notes

The diagram below shows how the level of impact is likely to differ from organisation to organisation depending on the type of organisations and its data activities.

Factors	Level of Impact		
	Low	Medium	High
Size of Organisation	Small ←		→ Large
Nature of Business	Don't Collect Personal data ←		→ Collect Large Amount of Personal Data
Existing DP Practices	Have Existing Practices ←		→ No Existing Practices
Transfer of Data Overseas	No Data Transfer ←		→ Huge Data Transfer
Conduct Telemarketing	No Telemarketing Practices ←		→ Heavy Use of Telemarketing Practices

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

Singapore Personal Data Protection Act

- In the development of the PDPA, Singapore took into account international best practices on personal data protection. References were made to the data protection regimes of key jurisdictions that have established comprehensive data protection laws, including the Australia, Canada, Hong Kong, New Zealand, UK, as well as the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the EU Data Protection Directive 95/46/EC and the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flow of Personal Data.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Notes

Background

- The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation.
- The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.
- On 11 July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.
- This revision is the first since the 1980 release of the Guidelines and arises out of a call by Ministers in the 2008 *Seoul Declaration for the Future of the Internet Economy* to assess the Guidelines in light of "changing technologies, markets and user behaviour, and the growing importance of digital identities".

Source: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Principle	Description
Collection limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
Data quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Purpose specification except with the consent of the data subject; or by the authority of law.
Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual participation	An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request made is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

APEC Privacy Framework

Background

- The APEC Privacy Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.
- It recognises the importance of:

i. Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;

ii. Recognising the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;

iii. Enabling global organisations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organisations for global access to and use of personal information;

iv. Enabling enforcement agencies to fulfill their mandate to protect information privacy; and,

v. Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

Source: APEC Privacy Framework

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

9 APEC Privacy Principles

S/N	Principle	Description
1	Preventing Harm	Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
2	Notice	Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.
3	Collection limitation	The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

Source: APEC Privacy Framework

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

9 APEC Privacy Principles

S/N	Principle	Description
4	Choice	Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.
5	Use of Personal information	Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.
6	Integrity of information	Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
7	Security safeguards	Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

Source: APEC Privacy Framework

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

9 APEC Privacy Principles

Notes

S/N	Principle	Description
8	Access and correction	Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.
9	Accountability	A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Source: APEC Privacy Framework

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

1.4 INTRODUCTION TO DATA PROTECTION FRAMEWORKS AROUND THE WORLD

EU Data Protection Directive 95/46/EC

Notes

- In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

Principles Relating to Processing of Personal Data

1. Member States shall provide for personal data to be:
    a) processed lawfully and fairly;
    b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
    c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
    f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
    a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
    b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.
    c) Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.
    d) The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Note: Article 1(1) states that the protection of natural persons in relation to the processing of personal data is a fundamental right.

Source: EU Data Protection Directive 95/46/EC

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 2:
DATA PROTECTION PROVISIONS AND DO NOT CALL PROVISIONS

At the end of this chapter, participants will be able to acquire knowledge for "Data Protection Provisions and Do Not Call Provisions".

- *PDPA 9 Key Obligations (Consent Obligation, Purpose Limitation Obligation, Notification Obligation, Access & Correction Obligation, Accuracy Obligation, Protection Obligation, Retention Limitation Obligation, Transfer Limitation Obligation and Openness Obligation)*
- *Existing Data and Other Existing Laws*
- *Selected Topics – Employment, NRIC*
- *Do Not Call Provisions*
- *Enforcement*

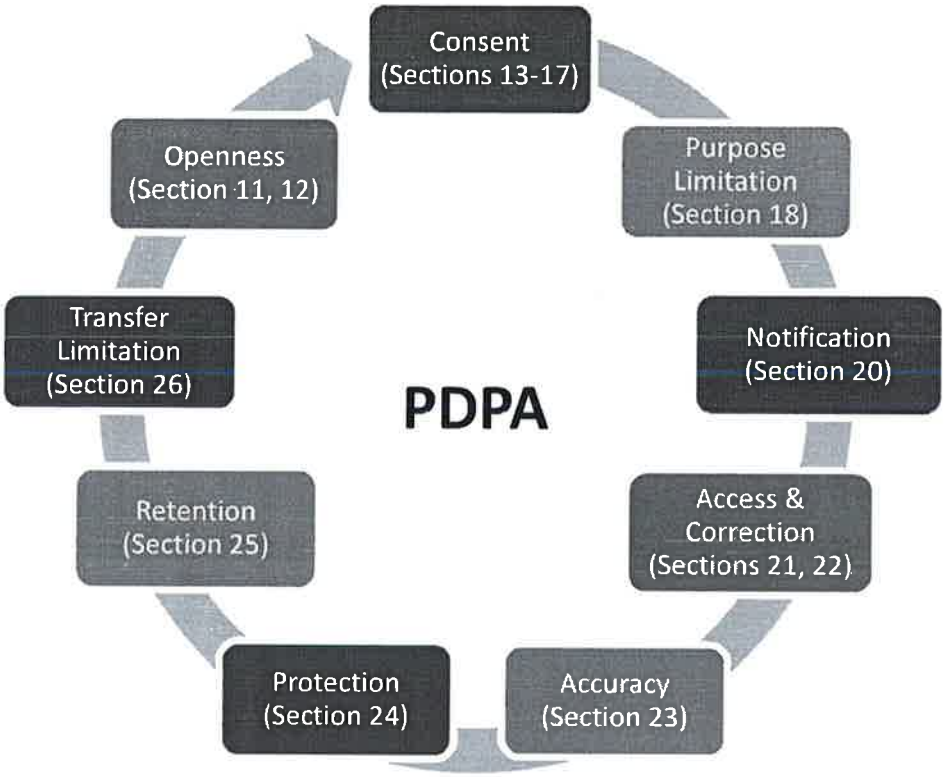
For more information on the 9 Key Obligations and DNC, please refer to Advisory Guidelines on the Do not Call Provisions (revised on 8 May 2015.)

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

2.1 PDPA 9 KEY OBLIGATIONS

The diagram below shows the 9 key obligations under the Data Protection Provisions.



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

① Valid & Not Valid
② Deemed Consent
③ Failure to Opt Out

- Organisation must obtain consent of the individual to the collection, use or disclosure of his or her personal data (PD).
- No consent unless the individual has been notified of the purpose (More details on the Notification Obligation are set out below in section 2.4).
- Consent can be obtained in a number of different ways. For example: verbal or written consent.
- As best practice, organisation should obtain consent in writing or recorded in a manner that is accessible for future reference.
- Deemed consent

  - When an individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would voluntarily provide the data.

  - 3 considerations:

    - Individual voluntarily provides personal data;
    - Individual aware of purpose;
    - Reasonable in the circumstances that the data would be provided.

Notes

For more information on the Consent Obligation, refer to Chapter 12 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Valid and Not Valid Consent – Examples

Notes

Example 1: Not Valid Consent: (Beyond what is reasonable)

Sarah signs up for a spa package. Sarah has to either agree to standard terms and conditions that allow the spa to share her personal data with 3rd parties for their marketing purposes, or not sign up for spa package.

Even if Sarah consents, consent is not valid.

Example 2: Valid Consent: (Eg. Lucky Draw)

Retailer ABC makes it a condition for every customer who wants to participate in its lucky draw to consent to the collection and use of his name and email address for the purpose of sending him marketing emails about ABC's products.

This may be a valid consent. The retailer may be able to require customers who want to participate in the lucky draw to consent to the collection and use of the personal data for the purpose of sending them marketing emails about ABC's products. Customers who do not wish to receive such marketing emails can choose not to participate in the lucky draw.

Note: The consent is not valid when:

An organisation providing a product or service to an individual requires the individual to consent to the collection, use or disclosure of his/her personal data beyond what is reasonable to provide the product or service

Or

An organisation provides false or misleading information with respect to the collection, use or disclosure or uses misleading or deceptive practices to attempt to obtain consent.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Deemed Consent – Examples

Notes

✓ **Example 1:** (Credit Card Payment)

Sarah visits a spa for facial treatment. After treatment, she hands over her credit card to the cashier for the purpose of making payment. The cashier processes payment and transmits credit card details to the bank for payment.

Sarah is deemed to have consented to the collection, use or disclosure of her credit card details for processing the payment.

✗ **Example 2:** Booking of taxi vs Receiving marketing info for about limousine service } No deemed consent

Sarah provides personal data to taxi operator's hotline when booking taxi. Taxi operator wants to use Sarah's personal data to market a limousine service to Sarah.

Sarah would not be deemed to have consented for purpose receiving of marketing information about the limousine service to the use of her personal data.

✓ **Example 3:** (Medical Checkup)

Sarah goes for a medical check-up at a clinic. For the purposes of the check-up, the clinic will be conducting a series of tests which include measuring her height and weight. Sarah is aware that such tests will be conducted as the clinic has provided this information on the registration form that Sarah filled out and submitted prior to the tests.

Sarah will be deemed to have consented to the collection of her personal data by submitting to the tests even though she did not directly provide the data to the clinic.

Failure to opt-out doesn't mean consent in all situations.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Failure to Opt Out

Notes

Failure to opt out will not be regarded as consent in all situations.

Example:

A retailer collected personal data from its customers to deliver products purchased by the customers. The retailer subsequently mails a flyer to an existing customer which states that a customer would have consented to the disclosure of his personal data to Company A to market the products of Company A unless the customer writes back to the retailer to opt out by a certain date. Retailer receives no response from the customer. In this case, customer's inaction is unlikely to signify consent since it may be due to other reasons not related to a desire to consent (e.g. not having opened the mailbox to read the flyer).

Failure to opt out will not be regarded as consent in all situations.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Other Consent Obligation Examples and Treatment

S/N	Example	Treatment
1	Signing up for a car cleaning service Ken would like to sign up for a car cleaning service with Organisation XYZ. Organisation XYZ makes it a condition of providing its service that it will share Ken's personal data such as his name, and residential address with third party marketing agencies in order for the agencies to mail Ken marketing information about products offered by Organisation XYZ.	In this case, requiring Ken to consent to the collection, use and disclosure of his personal data for such a purpose is likely to be beyond what is reasonable to provide the car cleaning service to Ken.
2	Using personal data in publicity materials Organisation XYZ conducts various educational and enrichment courses. Organisation XYZ makes it a condition for every student who enrols to provide consent for Organisation XYZ to collect, use and disclose his/her name, photograph and school examination scores in Organisation XYZ's publicity materials.	Requiring individuals to consent to the collection, use and disclosure of their personal data for such a purpose is likely to be beyond what is reasonable to provide the educational and enrichment courses to the individuals.
3	Offering a complimentary item Mary has enrolled in a weight management programme with Organisation ABC. Organisation ABC offers Mary the option of receiving a complimentary digital weighing machine on the condition that Mary consents to Organisation ABC's collection, use and disclosure of her photo, name and testimony in publicity materials to market Organisation ABC's weight management programme. Similar to lucky draw example.	In this case, Organisation ABC may be able to require Mary, who wishes to receive the digital weighing machine, to consent to the collection, use and disclosure of her personal data in publicity materials. If Mary does not consent to the collection, use and disclosure of her personal data for publicity purposes, she would still be able to sign up for the weight management programme and refuse the digital weighing machine.

Notes

In order to take free gift, must consent to collection, use & disclosure of data. Otherwise, refuse free gift.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Other Consent Obligation Examples and Treatment

S/N	Example	Treatment
4	Providing a free mobile application Organisation ABC releases a free mobile application in addition to a paid version. The terms and conditions of the application state that individuals who download the free application must consent to the collection and use of their name and email address for the purpose of sending them marketing emails about Organisation ABC's products and services.	In this case, Organisation ABC may be able to require individuals who wish to download the free application to consent to the collection and use of their personal data for the purpose of sending such marketing emails. Individuals who do not wish to receive marketing messages from Organisation ABC can choose not to download and use the free application, and select the paid version instead.
5	Redemption of complimentary parking coupon Shopping Centre ABC allows shoppers to redeem a 2-hour complimentary parking coupon with every $100 spent. A shopper who chooses to redeem the complimentary parking coupon must provide consent for Shopping Centre ABC to send SMSes about promotions by its shopping centre tenants to his Singapore telephone number.	In this case, Shopping Centre ABC may require shoppers who wish to redeem the complimentary parking coupon to consent to receiving such marketing SMSes. Shoppers who do not wish to receive such marketing SMSes can choose to decline the complimentary coupon.
6	Providing a voucher At Organisation ABC's road show, customers who spent more than $100 are offered a $20 storewide voucher on the condition that they consent to receiving, through their Singapore telephone numbers, marketing SMSes from Organisation ABC about its products.	In this case, Organisation ABC may require the customer who wishes to receive the storewide voucher to consent to receiving such marketing SMSes. Customers who do not wish to receive such marketing SMSes can choose to decline the voucher.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Other Consent Obligation Examples and Treatment

S/N	Example	Treatment
7	Offering a lucky draw Fashion Retailer ABC makes it a condition for every customer who wants to participate in a lucky draw it is administering to provide consent to the collection and use of his name and email address for the purpose of sending him marketing emails about Fashion Retailer ABC's products and services..	In this case, Fashion Retailer ABC may require customers who wish to participate in the lucky draw to consent to the collection and use of his name and email address for the purpose of sending them marketing emails about Fashion Retailer ABC's products and services. Customers who do not wish to receive such marketing emails can choose not to participate in the lucky draw.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Consent – 4 Things to Note

Notes

1) Obtaining consent from a person validly acting on behalf of an individual.

- The person should similarly have to be notified of the purposes for which the individual's personal data will be collected, used and disclosed
- Person gives consent for these purposes on behalf of the individual

2) Obtaining personal data from 3rd party sources with consent of the individual.

- Organisation obtaining personal data from 3rd party sources should exercise appropriate due diligence to check and ensure that the 3rd party source can validly give consent or has obtained consent and in the case of telemarketing, obtained clear and unambiguous consent in written or other accessible form. (More details on the Do Not Call Provisions are set out in section 2.14.)

Example:
Sarah provides the personal data of her friend Jane to the sales consultant at her spa as part of a member's referral programme the spa is running. Before recording Jane's personal data, the sales consultant asks Sarah a few questions to determine if Jane had been informed of the purposes for which her personal data is being disclosed to and used by the spa, and if Jane had indeed provided her consent. After obtaining verbal confirmation from Sarah in the affirmative to those questions, the sales consultant proceeded to collect Jane's personal data. The sales consultant is likely to have exercised appropriate due diligence in this situation.

As a best practice, when contacting Jane for the first time, the sales consultant should inform Jane that her personal data was disclosed by Sarah and verify that Jane had provided consent to do so.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Consent – 4 Things to Note

3) Exceptions to Consent Obligation – Second, Third and Fourth Schedules (Collection, Use and Disclosure of Personal Data without Consent)

- Necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual
- Necessary for any investigation or proceedings
- Publicly available data
- Necessary for evaluative purposes

"investigation", "proceedings" and "publicly available" are defined in the PDPA.

Notes

No need to obtain consent for collection, use & disclosure.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Obtaining Personal Data without the Consent of the Individual

Publicly Available Data Exception (1/2)

- Publicly available – The PDPA defines "publicly available" as personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

- Generally, personal data is generally available to the public if any member of the public could obtain or access the data with few or no restrictions. In some situations, the existence of restrictions may not prevent the data from being publicly available.

Example 1:

Allan is a member of an online social network that is open to the public. His membership profile which is publicly searchable lists his name, date of birth and the university at which he is currently enrolled.

The data which Allan has shared on this online social network is likely to be personal data that is publicly available, where any other user of the social network would be able to gain access to the data even if they accessed his profile page by accident and any member of public may join the online social network.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Obtaining Personal Data without the Consent of the Individual

Publicly Available Data Exception (2/2)

- Publicly available personal data also includes personal data observed in public.
- For this to apply, there are two requirements relating to how and where the personal data is observed:
  - the personal data must be observed by reasonably expected means;
  - the personal data must be observed at a location or event at which the individual appears and that is open to the public.

Example 2:

Jeff enters Store ABC to make a purchase. It would be reasonably expected that his image would be captured by CCTVs installed by Store ABC for security reasons. However, as best practice, store ABC should put up relevant notices to inform their customers about the CCTVs in operation.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

Consent – 4 Things to Note

Notes

4) Withdrawal of Consent

- Individual may at any time withdraw consent given.
- Individual must give reasonable notice for withdrawal.
- Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law (section 16(4)).
- Organisation must not prohibit withdrawal of consent, although this does not affect any legal consequences arising from such withdrawal.
- Organisations must allow an individual who has previously given (or is deemed to have given) his consent to the organisation for collection, use or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice.
- In this regard, considerations for whether the individual has given reasonable notice would include the amount of time needed to give effect to the withdrawal of consent and the manner in which notice was given.
- As a general rule of thumb, the Commission would consider a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice, to be reasonable notice.
- Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take effect.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

Notes

To enable and facilitate withdrawal, organisations are advised to make an appropriate consent withdrawal policy that is clear and easily accessible to the individuals concerned. This withdrawal policy should:

- advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;
- indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and
- distinguish between purposes necessary and optional to the provision of the products/services (that may include the service of the existing business relationship). Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes.

An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself.

Where relevant, organisations should consider how the withdrawal notice impacts both consent obtained under the Data Protection Provisions and the Do Not Call Provisions.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

Notes

Example: (Eg. Early termination of telco contract)

An individual wishes to obtain certain services from a telecom service provider, Operator X and is required by the telecom service provider to agree to its terms and conditions for provision of the services.

Operator X can stipulate as a condition of providing the services that the individual agrees to the collection, use and disclosure of specified types of personal data by the organisation for the purpose of supplying the subscribed services.

Such types of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data.

The individual provides consent for those specified types of personal data but subsequently withdraws that consent.

The withdrawal of consent results in Operator X being unable to provide services to the individual.

This would in turn entail an early termination of the service contract. Operator X should inform the individual of the consequences of the early termination, e.g. that the individual would incur early termination charges.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

Notes

Effects of a Withdrawal Notice

- In determining the effect of any notice to withdraw consent, the Commission will consider all relevant facts of the situation. This could include but is not limited to matters like the actual content of the notice of withdrawal, whether the intent to withdraw consent was clearly expressed, and the channel through which the notice was sent.

- In cases where an organisation provides a facility for individuals to withdraw consent (e.g. by clicking on an "unsubscribe" link within an e-mail), the organisation should clearly indicate the scope of such withdrawal. The organisation is also encouraged to inform individuals of how they may withdraw consent for matters outside the scope of such withdrawal.

- Typically, where the withdrawal notice for marketing contains a general withdrawal message, i.e. it is not clear as to the channel of receiving marketing messages for which consent is withdrawn, the Commission will consider any withdrawal of consent for marketing sent via a particular channel to only apply to all messages relating to the withdrawal sent via that channel.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

(Withdrawal of consent is NOT a blanket withdrawal.)

Notes

Example:

Organisation ABC has obtained consent from Sally to send her marketing messages via e-mail and fax.

ABC sends Sally an e-mail informing her of the latest in-store promotion, and included a link for her to unsubscribe:

"If you wish to stop receiving marketing messages from ABC, please click on the link 'unsubscribe'."

Sally clicks on the 'unsubscribe' link and is directed to a website which states:

"You have unsubscribed successfully."

As the withdrawal notice is general and does not specify the channel of receiving marketing messages for which consent is withdrawn, Sally would be considered to have withdrawn consent to receive marketing messages sent by e-mail only.

PDPA controls :

1. Phone calls
2. Fax
3. SMSes

SPAM Control Act :

1. Email
2. Social media

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

Notes

Actions Organisations Must Take Upon Receiving a Notice of Withdrawal

- Once an organisation has received from an individual a notice to withdraw consent, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent, even if these consequences are set out somewhere else, e.g. in the service contract between the organisation and the individual

- Although an individual may withdraw consent for the collection use, or disclosure of his personal data, section 16 does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in its documents and records in accordance with the Data Protection Provisions. For more information on this, please refer to the section on the "Retention Limitation Obligation".

- Upon receipt of a notice of withdrawal of consent, the organisation must cease to collect use or disclose the individuals personal data and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

- An organisation is not required to inform other organisations to which it has disclosed an individual's personal data of the individual's withdrawal of consent. This does not affect the organisation's obligation to provide, upon request, access to the individual's personal data in its possession or control and information to the individual about the ways in which his personal data may have been disclosed. Hence the individual may find out which other organisations his personal data may have been disclosed to and give notice to withdraw consent to those organisations directly.

→ Different from Data Intermediary. Data intermediaries are under the umbrella of the organization.

- Organisations may retain personal data in its documents and records in accordance with the Data Protection Provisions.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

WITHDRAWAL OF CONSENT

Notes

Actions Organisations Must Take Upon Receiving a Notice of Withdrawal

Example:

Andy had previously given his consent to Y Electronics to collect, use and disclose his contact details (which form part of his personal data) for the purpose of providing him with marketing information and promotional offers on computers and other IT products. Y Electronics discloses Andy's contact details to its outsourced marketing agent and some other third party companies offering computers and other IT products to fulfil that purpose. Andy changes his mind and submits a notice to withdraw the consent he gave to Y Electronics for the purpose of marketing computers and other IT products.

Y Electronics is required to notify Andy of the consequences of his withdrawal, for example, that:

- Y Electronics and its marketing agents will cease to send information on computer and IT products to Andy;
- Y Electronics will cease to disclose Andy's personal data to any third party; and
- Y Electronics will cease using Andy's contact details for marketing computer and IT products and will instruct its outsourced marketing agent likewise (so that it will cease sending marketing information to Andy).

However, Y Electronics will not be required to inform the third party companies to which it disclosed Andy's contact details, and Andy will have to approach those companies to withdraw consent if he wishes to do.

The withdrawal of consent also does not affect Y Electronics' ability to retain Andy's personal data that it requires for legal or business purposes. For example, Y Electronics may still retain Andy's personal data in its database for the purpose of servicing an ongoing warranty, or records of his purchases that are necessary for audit purposes.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

SAMPLE CLAUSES ON OBTAINING AND WITHDRAWING CONSENT

Notes

A. Sample Consent Clause for Membership Application

Set out below is a sample clause for obtaining consent from an individual for the collection, use and disclosure of his personal data in the context of a membership application.

By signing this membership application form, you agree that <organisation name> may collect, use and disclose your personal data, as provided in this application form, or (if applicable) obtained by our organisation as a result of your membership, for the following purposes in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>):

(a) the processing of this membership application; and
(b) the administration of the membership with our organisation.

Please visit our website at <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.

Name:
Signature:
Date:

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

SAMPLE CLAUSES ON OBTAINING AND WITHDRAWING CONSENT

Notes

B. Sample Consent Clause for the Sending of Marketing Material

Set out below is a sample clause for obtaining consent from an individual to collect, use and disclose his personal data for the purpose of sending him marketing material.

You agree that <organisation name> may collect, use and disclose your personal data, which you have provided in this form, for providing marketing material that you have agreed to receive, in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>).

Please tick the relevant boxes below if you agree to receive the following: Explicit consent

□ Our organisation's monthly Newsletter (sent by us via email)

□ Information sent by our organisation about our organisation's products and services, including updates on our latest promotions and new products and services, via the following channels:

- □ Email
- □ Text Message
- □ Phone Call

□ Information sent by our organisation on selected third parties' products and services, such as updates on their latest promotions and their new products and services, via the following channels:

- □ Email
- □ Text Message
- □ Phone Call

□ Information sent by our business partners* on their products and services, via the following channels:

- □ Email
- □ Text Message
- □ Phone Call

*Please note that information will be sent directly by our business partners, and we shall disclose the relevant contact information to them for that purpose.

Please visit our website at <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.

Name:
Signature:
Date:

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

SAMPLE CLAUSES ON OBTAINING AND WITHDRAWING CONSENT

Notes

C. Sample Consent Clause for Lucky Draws

Set out below is a sample clause for obtaining consent from an individual for the collection, use and disclosure of his personal data for the purposes of lucky draws.

> By submitting this lucky draw entry form, you agree that <organisation name> may collect, use and disclose your personal data, as provided in this entry form, for the following purposes in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>):
> (a) to administer this lucky draw, including to contact you for the administration of prizes in relation to this lucky draw.
>
> Please visit our website at <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.
>
> Name:
> Signature:

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

SAMPLE CLAUSES ON OBTAINING AND WITHDRAWING CONSENT

Notes

D. Sample Clause for Withdrawal of Consent in Relation to Receiving Marketing Material

Set out below is a sample clause for an individual to withdraw consent to the use and disclosure of his personal data for the purpose of sending him marketing material.

I withdraw my consent to the use and disclosure of my personal data for receiving marketing material as follows*:

*Please tick the relevant boxes below to indicate the categories, and corresponding medium of communication, of the marketing material for which consent is withdrawn.

□ Your organisation's monthly Newsletter (sent via email)

□ Information about your organisation's products and services, including updates on the latest promotions and new products and services, via the following channels:
- □ Email
- □ Text Message
- □ Phone Call

□ Information sent by your organisation on third parties' products and services, such as updates on their latest promotions and their new products and services, via the following channels:
- □ Email
- □ Text Message
- □ Phone Call

□ The use of my contact details by third parties** to send me information on their products and services, via the following channels:
- □ Email
- □ Text Message
- □ Phone Call

** Third parties that our organisation has disclosed your personal data to for this purpose will be informed of your withdrawal of consent and your personal data will no longer be disclosed to any third parties by the effective date of your withdrawal.

Please visit our website at <webpage URL> for further details on our data protection policy, including any consequences arising from your withdrawal of consent and the period within which your withdrawal of consent will take effect.

Name:
Signature:
Date:

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.2 CONSENT OBLIGATION

SAMPLE CLAUSES ON OBTAINING AND WITHDRAWING CONSENT

Notes

E. Sample Messages for Opting Out of or Withdrawing Consent in Relation to Receiving Telemarketing Material

Sample Message 1

Organisation ABC has obtained clear and unambiguous consent from an individual to send him telemarketing text messages to his mobile telephone number as well as marketing e-mails. Organisation ABC sends him the following text message to market its upcoming workshop:

"<ADV> You are invited to ABC's workshop. Call us at 12345678 for more details. If you do not wish to receive telemarketing text messages from ABC, please SMS "UNSUB" to 76543."

By sending "UNSUB", the individual would be withdrawing consent to receive further telemarketing text messages from Organisation ABC via his mobile telephone number. Organisation ABC may continue to send him marketing e-mails. To be clear, Organisation ABC must facilitate any withdrawal of consent from the individual to receive marketing e-mails.

Sample Message 2

Store ABC has an ongoing relationship with an individual. Store ABC sends to his mobile telephone number telemarketing text messages that are exempt messages with the following opt-out statement:

"<ADV> ABC storewide discounts of 20% for all members from 20-25 June. To opt-out of receiving telemarketing text messages from ABC, SMS "UNSUB" to 76543."

By sending "UNSUB", the individual would be opting-out from or otherwise withdrawing consent to receiving further telemarketing text messages from Store ABC to the mobile telephone number. To be clear, Store ABC must facilitate any withdrawal of consent from the individual to receive any other forms of marketing messages.

Sample Message 3

Organisation ABC has an ongoing relationship with an individual. Organisation ABC sends him exempt messages via facsimile, with the following opt-out statement:

"<ADV> ABC storewide discounts of 20% for all members from 20-25 June. To opt-out of receiving messages from ABC via fax, please inform us via fax at 12345678 or via e-mail at abc@abc.org."

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.3 PURPOSE LIMITATION OBLIGATION

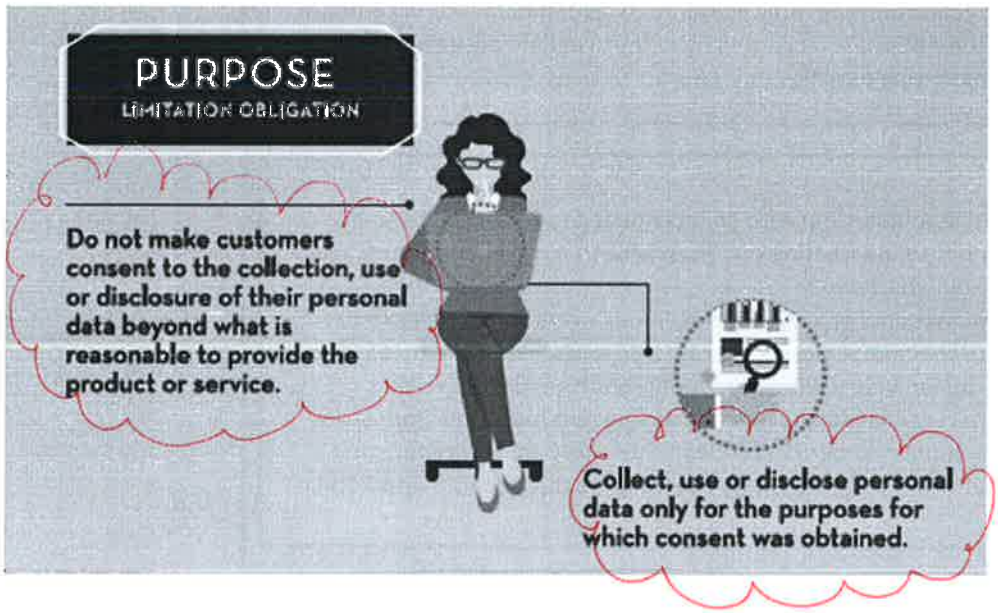
Publicly Available Data Exception (2/2)

Notes

Organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned.

Purpose limited to:

- ✓ What a reasonable person would consider appropriate in the circumstances; and
- ✓ The individual has been informed by the organisation.
- ✗ "For any other purposes that the organisation deems fit".



For more information on the Purpose Limitation Obligation, refer to Chapter 13 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.3 PURPOSE LIMITATION OBLIGATION

Purpose Limitation Obligation – Examples

Notes

Example 1: Activities are part of the purpose of servicing existing business relationship for which consent has been obtained.

Sarah signs up for a spa membership with ABC Pte Ltd. ABC Pte Ltd wants to use her personal data for the purposes of sending greeting cards and reminders to use the remaining credits in her account before her spa membership expires.

Example 2: Purpose unlikely to fall within consent obtained for purpose of servicing existing business relationship.

ABC Pte Ltd wants to send her material promoting its affiliate company's hair salon.

Note: When specifying its purposes relating to personal data, an organisation is not required to specify every activity which it may undertake, but its objectives or reasons relating to personal data.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.3 PURPOSE LIMITATION OBLIGATION

Other Purpose Limitation Obligation Cases

Notes

Case
A fashion retailer is conducting a membership drive. It states in the membership registration form that the purposes for which it may use the details provided by individuals who register including providing them with updates on new products and promotions and any other purpose that it deems fit. In this case, providing updates on new products and promotions may be a reasonable purpose but the fashion retailer's unqualified reference to 'any other purpose that it deems fit' would not be considered reasonable. (As noted in the section on the "Notification Obligation", this may also be an inadequate notification to the individual of the purposes for which his or her personal data will be collected, used and disclosed.)

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.4 NOTIFICATION OBLIGATION

Organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

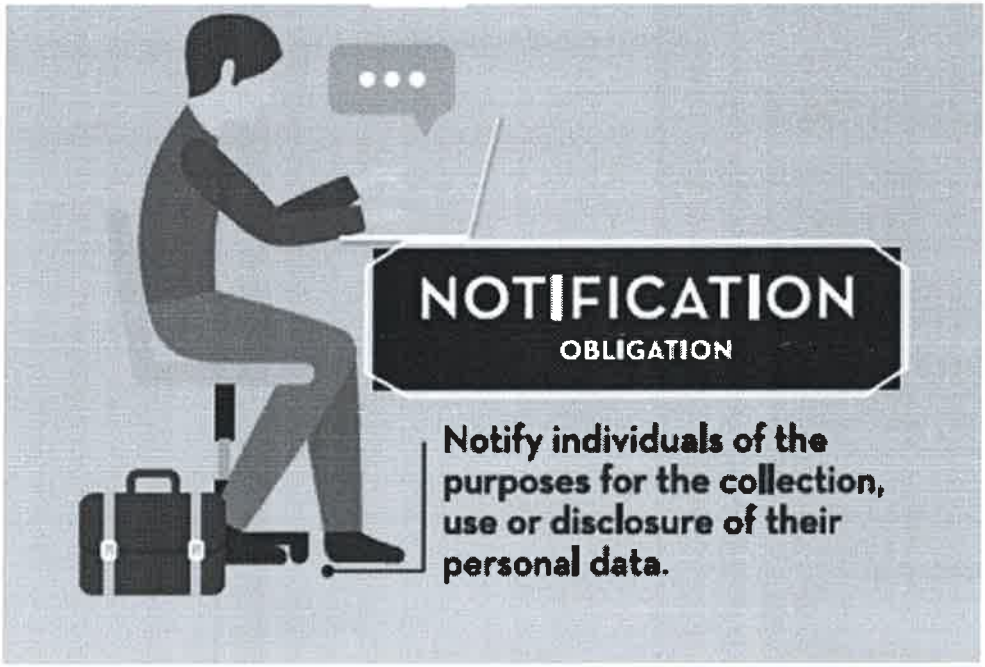
Notification Obligation does not apply: EXCEPTIONS

- Deemed consent
- In circumstances specified in the Second, Third and Fourth Schedules (Collection, Use and Disclosure of Personal Data without Consent)

Note: Notification obligation applies for managing or terminating employment relationship exception.

Notes

No need to notify individuals of the purposes for collection, use & disclosure.



For more information on the Notification Obligation, refer to Chapter 14 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.
'A Guide to Notification' is accessible from the link:
https://www.pdpc.gov.sg/docs/default-source/other-guides/a-guide-to-notification-v1-0-(110914).pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.4 NOTIFICATION OBLIGATION

Notification Obligation – 3 Things to Note

Notes

1) When organisation must specify its purposes

- Notification of the purpose(s) for collection, use or disclosure to be on or before such collection, use or disclosure of the personal data. For example, this could be:
  - When an individual is entering into a contract
  - Before an individual enters into a contract (e.g. Insurance)
  - Before collecting, use or disclosing personal data on a periodic basis

2) The manner of stating purposes and obtaining consent

- Data Protection Provisions do not specify the manner or form.
- Organisation should determine the appropriate form and manner. Some considerations may include :
  - Amount of personal data collected;
  - How the personal data is collected;
  - Frequency at which personal data collected;
  - Using a "layered notice" where appropriate;
  - Whether purpose may be of special concern and thus highlighted to individual;
  - Easy to understand and appropriate to the intended audience.

3) Information to be included when stating purposes

- Appropriate level of detail for understanding of the organisation's purposes. Information should also include:
  - Whether purpose is necessary for provision of products or services or optional
  - Whether will be disclosed

Note: New purpose will need "new" notification and consent.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.4 NOTIFICATION OBLIGATION

Notification Obligation – Examples

Notes

Example 1: Sufficiently specified purpose

Organisation sells products online. It informs individual purchasing products through its website of the purposes for which it will be collecting, using and disclosing personal data, including disclosure to other companies in the corporate group and its outsourced marketing company for the purpose of marketing their products to the individual from time to time.

Example 2: Insufficiently specified purpose

Real estate agency places a guest book at reception counter in a show flat. However it is unclear if individual who voluntarily provide their personal data did so for the purpose of being contacted in relation to their visit to the show flat, to receive information about other properties or for other purposes.

Example 3: Verbal

Individual signs up for a certain service with a service provider over the telephone. The service provider requests for the individual's consent to the collection and use of his personal data for the service provider's purposes and obtain personal data from the individual over the phone.

(For accountability)

Good practice to document verbal consent. Organisations should remember that they may have to demonstrate later that consent was actually given.

Example 4: Online

Sarah signs up for a spa membership over the internet. The notifications on website explain how Sarah's personal data will be used and disclosed. Sarah clicks on "Accept" button at the bottom of the notification page.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.4 NOTIFICATION OBLIGATION

Other Notification Obligation Cases

S/N	Cases
1	Sarah signs up for a membership at a gym. The application form contains an extract of the most relevant portions of the Data Protection Policy in a physical document. For example, it states that Sarah's address details will be used for sending her a gym membership card and other communications related to her gym membership. The sales representative of the gym informs her that the full Data Protection Policy is available on the gym's website and provides her with relevant information to locate it. In this case, the gym has informed Sarah of the purposes for which her personal data will be collected, used or disclosed.
2	An electronics store sells products online through its website. It informs individuals purchasing products through its website of the purposes for which it will be collecting, using and disclosing personal data, including that the contact details provided by the customers will be disclosed to other companies in the electronics store's corporate group and outsourced marketing company for the purposes of marketing the products of the various companies in its corporate group from time to time. In this case, the electronics store would be considered to have stated a sufficiently specific purpose. In another case, the electronics store informs individuals purchasing products through its website that the personal data provided may be used and disclosed for valid business purposes. In this case, the electronics store would not be considered to have stated a sufficiently specific purpose

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.4 NOTIFICATION OBLIGATION

Other Notification Obligation Cases

S/N	Cases
3 ✓	A supermarket surveys a group of shoppers on its premises to find out ways to improve customer experience. It collects personal data such as the names and contact details of the shoppers through a survey form which it hands to shoppers. The first line of each survey forms clearly and legibly states that "Your personal data will be used by the supermarket or its appointed survey company for analysis of survey responses to find out ways to improve customer experience at our supermarket, or to contact survey respondents for follow-up queries on the survey responses for such analysis." The supermarket would be considered to have provided appropriate notification in this scenario.
✓	An estate agent places a guest book at the reception counter in a show flat. Individuals who visit the show flat are asked to provide their name, address and income information in the guest book. The receptionist greets every individual who enters the show flat and explains verbally that his personal data is collected for the estate agent's market research and product planning purposes and that it would not be used to contact individuals after they leave the show flat. The real estate agency would be considered to have provided appropriate notification in this case.
4 ✓	Sarah currently has a membership with a spa. Her spa wants to use her personal data for the purposes of sending her greeting cards and the spa's annual newsletter in the post while her spa membership is still active. These purposes would fall within sub-paragraph (a) above, as part of the organisation's servicing of the existing business relationship with the individual, for which consent would have been previously obtained.
✗	Sarah's spa wants to send her information about an affiliate company's hair salon promotions. The spa would need to obtain Sarah's consent before sending information promoting new services that Sarah has not signed up for, as that is unlikely to fall within sub-paragraphs (a) to (c) above.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Can impose a reasonable fee

Cannot charge any fee

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

2.5 ACCESS AND CORRECTION OBLIGATION

1. Making access request channels available

Your organisation should allow an individual to submit an access request, and to state the available channels clearly. For example, an access request may be submitted in person, through email or post. Please refer to ANNEX A for a sample access request form.

If the personal data requested can be retrieved by the individual himself, your organisation may wish to inform him how it can be done. For example, the individual can log into his account online to access his own personal data.

2. Obtaining specific information

The individual does not need to provide a reason for making an access request. However, your organisation may request for the individual to provide more details to enable your organisation to identify the individual making the request and to locate the requested personal data. For example, if the individual is able to specify the type of personal data requested, and provide the date and time the personal data was collected, this would help your organisation narrow down the search.

Eg. Request to view video footage.
— Must provide date & time & location at store

Notes

For more information on the Access and Correction Obligation, refer to Chapter 15 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act. 'Guide to Handling Access Requests' is accessible from the link: https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-handling-access-requests-v1-0-(090616).pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Responding to access requests:

Organisation should provide **complete set of personal data requested:**

- Where personal data contained in a document, the organisation may provide only the personal data (or sections of document containing the personal data) if feasible.

In providing **info on use/disclosure over past year**, organisation:

- May provide information on purposes rather than specific activities.
- May develop a standard list of all possible third parties to whom personal data may have been disclosed. In many cases, an organisation may provide this standard list as an alternative to providing the specific set of third parties to whom the personal data has been disclosed.

Organisation may charge a **reasonable fee** to recover incremental costs of responding to access request.

- Premature for PDPC to prescribe benchmark fees at the outset.
- If your organisation would like to charge a fee for the access request, a written estimate of the fee must be provided to the individual.
- If the final fee to be charged is higher than the original written estimate, your organisation must inform the individual in writing of the increased fee.
- The PDPA does not prescribe a standard fee or range of fees applicable to access requests.

Organisations must upon request:

Provide an individual with his PD in the possession or under the control of the organisation and information about the ways in which the PD has been or may have been used or disclosed during the past 1 year.

Notes

Determining response timeframe

- Your organisation must provide access to the requested personal data as soon as reasonably possible.
- If your organisation is unable to provide access within 30 working days, inform the individual as soon as possible of the time your organisation will be able to provide access.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Access Obligation – Examples



Example 1:

A shopping centre receives a request from an individual to view all CCTV footages of him recorded at the shopping centre over the past year.

The burden of providing access would likely be unreasonable to shopping centre and disproportionate to the individual's interests

Responding to access requests:

Example

- Mary makes an access request with Organisation ABC for CCTV footage of herself at a particular date and time. Organisation ABC has a CCTV recording system which typically keeps the CCTV footage for 30 days before the footage is overwritten.

- As Mary submitted her access request before the scheduled deletion of the specific CCTV footage, the organisation should search for the requested CCTV footage as soon as reasonably possible before the footage is overwritten by the CCTV system.

Organisations must upon request:

(a) If Organisation ABC assesses the access request and provides Mary access to the requested personal data contained in the CCTV footage, Organisation ABC must delete the footage thereafter if the purpose for collecting the personal data is no longer served by retention and it has no other business or legal purpose to retain the footage in accordance with the PDPA16.

(b) If, however, Organisation ABC determines that it is to reject Mary's request to access the personal data contained in the CCTV footage, Organisation ABC should preserve the footage for a reasonable period, minimally 30 days or longer, to allow Mary the opportunity to exhaust any recourse under the PDPA.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Access Obligation – Examples

Example 2:

A shop receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently. The individual provides shop with sufficient information to determine when the event was held.

The provision of access would be reasonable.



EXCEPTIONS

Organisations must not provide access if doing so:

a) Threatens the safety or physical or mental health of another individual;

b) Causes immediate or grave harm to the safety or physical or mental health of the individual who made the request;

c) Reveals personal data about another individual;

d) Reveals the identity of an individual who provided personal data about another individual; or

e) Contrary to national interest.

Notes

No need to provide access to personal data.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Access Obligation – Examples

Notes

Example 3:

Company ZYX receives an access request from a customer to view his personal data stored in a format that is readable only by a special machine. The company owns two such machines but both are faulty. In order to respond to the customer's request in a timely manner, Company ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounted to $50,000.

Under the PDPA, this would not be considered a reasonable fee as ZYX is expected to have the general means to comply with its customers' access requests.

Example 4:

An individual requests from Company TUV a paper copy of his personal data. TUV charges a fee of $50 for the information printed out on 50 pages of paper, based on the incremental cost of producing the copy.

The fee is reasonable as it reflects the incremental cost of providing the personal data.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Ascertaining identity

- When processing an access request, it is important to establish and verify the identity of the individual making the request. Your organisation should set out standard operating procedures to conduct verification when processing access requests (e.g. verification questions to be asked to establish the identity of the requestor).

- If the requestor is making an access request on behalf of another individual, your organisation should ensure the requestor is legally authorised to act on behalf of the individual.

- If your organisation receives an access request from two or more individuals (e.g. husband and wife) for their respective personal data captured in the same set of records, your organisation may obtain consent from the respective individuals to disclose their personal data to each other. In such a circumstance, your organisation can provide the individuals access to a common data set containing their personal data, without having to exclude the personal data of the other individuals. If such consent cannot be obtained, your organisation may provide access to the individuals separately, for example, by masking the personal data of the other individuals before providing the individual access to his own personal data, and vice versa.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Keeping a record of all access requests

- Your organisation should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected. Proper documentation may help your organisation in the event of a dispute or an application to the PDPC for a review. As part of your organisation's documentation process, you may wish to consider using an acknowledgement form (please see ANNEX B for a sample form).

- Your organisation should also put in place an appropriate retention policy for the keeping of such records, including the duration for which they will be retained. Organisations should cease to retain records containing the individuals' personal data where retention is no longer necessary for any legal or business purposes.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Preservation of personal data

- If an organisation has scheduled periodic disposal or deletion of personal data (e.g. the CCTV system deletes the footage every X days, or physical documents containing personal data are shredded every X days), the organisation is to identify the requested personal data, as soon as reasonably possible after receiving the access request, and ensure the personal data requested is preserved while the organisation is processing the access request

- However, organisation should not unnecessarily preserve personal data "just in case" to meet possible access requests. Organisation should not retain personal data indefinitely when there is a no business or legal purpose to do so.

After rejecting an access request

- Should the organisation reject an access request, the organisation should continue to preserve the requested personal data for a reasonable period - minimally 30 days or longer after rejecting the request, as the individual may seek a review of the organisation's decision.

- In the event the individual submits an application to the PDPC to review the organisation's rejection of the access request, the organisation should continue to preserve the requested personal data until PDPC's review is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Responding to correction requests:

- Send corrected personal data to every other organisation which personal data was disclosed to within a year before the date the correction was made, unless other organisation does not need the corrected personal data.
- May send corrected personal data only to specific organisations, with consent of individuals (unless organisation is a credit bureau).
- Organisation is not entitled to impose a charge for complying with the correction obligation

Organisations must upon request:

Correct an error or omission in an individual's PD that is in the possession or under the control of the organisation.

Notes

Example :

An individual disputes his performance evaluation records kept by his ex-employer, Organisation ABC. In anticipation of background checks to be conducted by his new employer, an individual requests that Organisation ABC amend his performance track record to something he considers to be more favourable and accurate compared to the one kept by Organisation ABC.

Organisation ABC is not obligated to make the correction to the extent that the individual's performance evaluation records constitute or contain an opinion.

- Evaluation purpose
- Investigation purpose

} No need to obtain consent

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Correction Obligation – Examples

Example :

An online retailer receives a request from a customer to update his address. The retailer decides that there are no reasonable grounds to reject the customer's request and proceeds to correct the data.

The retailer also sends correct address to its affiliate responsible for servicing customer's warranty. The affiliate determines that it does not require the corrected address for any legal or business purpose as the customer's warranty has expired. It makes a note that it has not made the correction.

The retailer does not send the corrected address to a courier company which it had previously used to deliver products to customer.

EXCEPTION

If an organisation is satisfied upon reasonable grounds that a correction should not be made, organisation is required to annotate the correction that was requested but not made. (Section 22(5)).

Organisation is not required to correct or alter an opinion, including a professional or an expert opinion (Section 22(6)).

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Other Access and Correction Obligation Cases

Notes

S/N	Cases
1	Organisation ABC receives a request from John seeking to know what personal data relating to him was disclosed in Organisation ABC's correspondence with Organisation DEF in a specified month within the last one year. Assuming that the request does not fall under any relevant exception (for example, it is not opinion data kept solely for an evaluative purpose), Organisation ABC is required to provide John with his personal data even if its correspondence with Organisation DEF had not been archived in a formalised system such as a database. To be clear, Organisation ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in their possession or control, and it is not necessarily required to provide John with copies of the actual correspondence with Organisation DEF.
2	Sarah makes an access request to her spa, requesting for information relating to how her personal data has been used or disclosed. The request was made on 5 December 2015. The spa is only required to provide information on how her personal data has been used or disclosed within the past year – that is, the period from 6 December 2014 to the date of the request, 5 December 2015.
3	An individual sends an email providing feedback to Organisation XYZ. The form contains his personal data including his full name and contact number. A day later, he requests access to the personal data in the form while having full knowledge of the information he is requesting. Such a request is likely to be considered frivolous or vexatious, unless it can be shown otherwise.
4	An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Other Access and Correction Obligation Cases

S/N	Cases
5	Mary makes an access request with Organisation ABC for footage of herself captured by Organisation ABC's CCTV system on a particular date and time. Organisation ABC looks for the requested CCTV footage, and finds that the requested footage contains personal data of Mary and two other individuals. Organisation ABC then assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data (e.g. by masking the images of the other individuals in the same footage).
6	John applies to School ABC for access to CCTV footage of himself in a classroom when he was having a discussion with another classmate, Peter. Peter provides consent to the school to disclose his personal data (that is part of the CCTV footage requested by John) to John. School ABC is able to provide John access to the requested CCTV footage without masking Peter's image.
7	Betty applies to Shopping Centre ABC for access to CCTV footage of herself walking through the aisles of the shopping centre on a specific day and time. The CCTV footage contains images of other individuals. Since the images of the other shoppers are recorded in a public area, the data is considered to be publicly available. Shopping Centre ABC does not need to obtain the consent of the other shoppers in the CCTV footage nor mask their images before providing access to Betty.
8	An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests.

Notes

Always better to mask instead of obtaining consent.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.5 ACCESS AND CORRECTION OBLIGATION

Exceptions to Access and Correction Obligation:

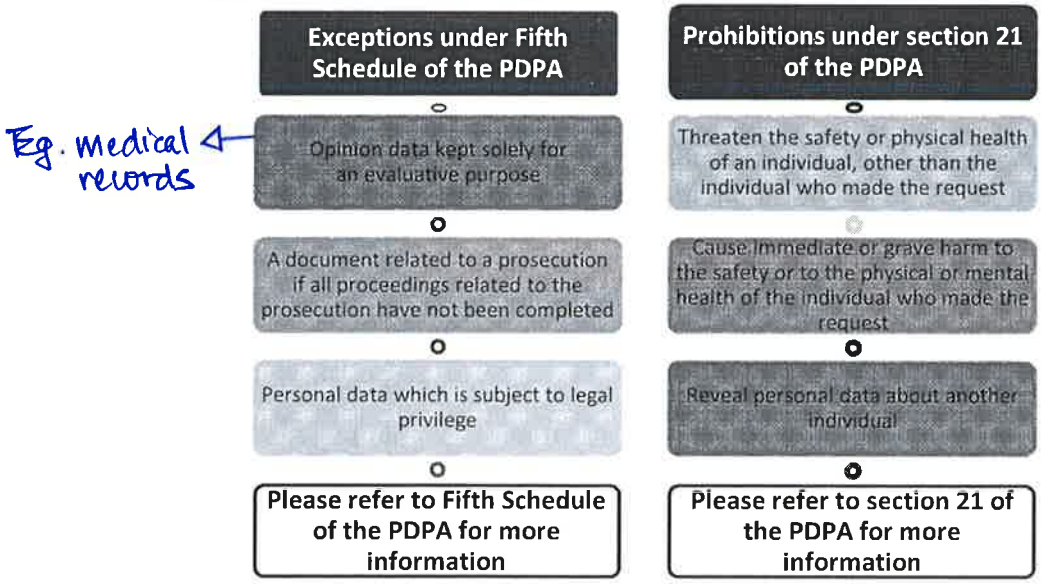
Notes

Assessing exceptions and prohibitions

• Under the PDPA, there may be circumstances where your organisation does not need to provide access to the personal data requested. Some of these circumstances include : (refer to diagram).

• When assessing whether any exceptions or prohibitions apply, your organisation should also consider if it is able to provide the individual with the requested personal data or information without the personal data or information excluded under sections 21(2), (3) and (4) of the PDPA. If your organisation is able to do so, it must provide the individual access to the personal data without the personal data or information excluded. For example, if personal data requested by the individual also contains personal data of another individual, and your organisation is able to mask out the personal data of the other individual, your organisation must provide access to the requested personal data without the personal data of the other individual.

• If any exception or prohibition under the PDPA applies such that your organisation may reject the access request, as good practice, inform the individual of the relevant reason(s) so that he understands the reason(s) behind your organisation's decision.



Eg. medical records

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.6 ACCURACY OBLIGATION

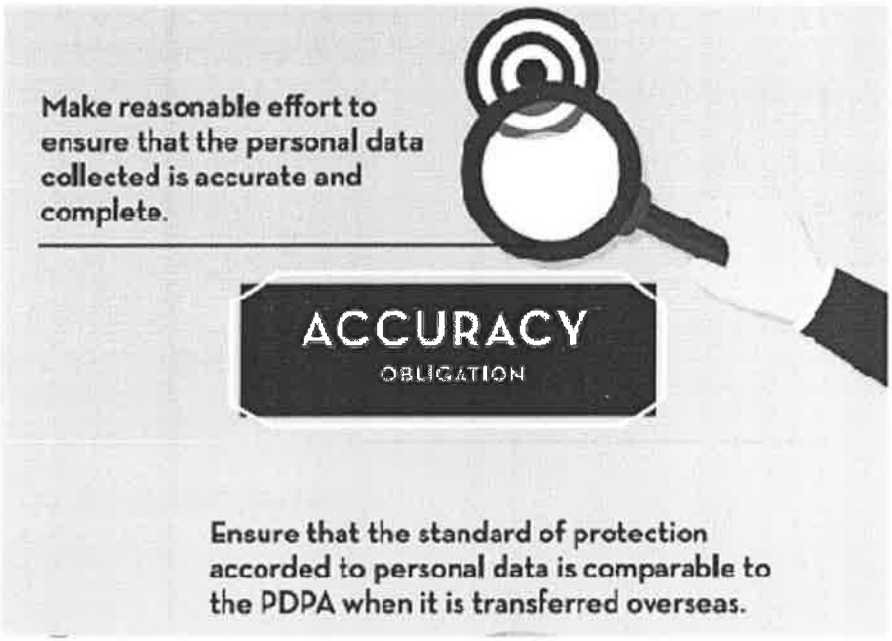
Organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be:

a) Used by organisation to make a decision that affects the individual concerned; or

b) Disclosed by the organisation to another organisation.

Organisation must make reasonable effort to:

- Accurately record personal data which it collects;
- Collect all relevant parts of the personal data (so that it is complete);
- Take appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness; and
- Consider whether it is necessary to update the information.



For more information on the Accuracy Obligation, refer to Chapter 16 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.6 ACCURACY OBLIGATION

Accuracy Obligation – Examples

Example:

Nick applies for a home loan from a bank. To assess whether to provide loan to Nick, Bank asked for relevant supporting documents to verify the information provided by Nick, including identity document and his most recent pay slip. Bank also asks Nick to declare that the information he has provided is accurate and complete.

Bank is likely to have made a reasonable effort to ensure that personal data collected from Nick is accurate and complete.

Note: Not all types of personal data require updates e.g. historical data.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.6 ACCURACY OBLIGATION

Other Accuracy Obligation Cases

S/N	Cases
1	Nick will be attending an adventure camp for his company's team-building purposes. The adventure camp operator obtains relevant health check-up records from his company to determine whether Nick is sufficiently fit to participate in the adventure activities. The records were dated eight years ago, when Nick first joined the company. In this scenario, the adventure camp company should consider asking Nick for a more recent health record.
2	A company is considering whether an existing employee, John, should be transferred to take on a different role in its IT department. One of the criteria for the transfer is the possession of certain qualifications and professional certifications. The company has information about John's qualifications and professional certifications that was provided by John (which form part of his personal data) when he joined the company five years before. The company asks John to update them with any new qualifications or certifications he may have obtained in the last five years since joining the company but does not ask him to re-confirm the information about the qualifications he provided when he joined the company. In this scenario, the company is likely to have met its obligation to update John's personal data.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

cost ↑

No harm over-protecting but do not over-collect.

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Administrative Measures
Physical Measures
Technical Measures

2.7 PROTECTION OBLIGATION

Need to encrypt data

Organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

In practice, organisations should:

- Design its security arrangements to fit the nature of the personal data and the possible harm that might result from a security breach;
- Identify reliable and well-trained personnel responsible for ensuring information security;
- Implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- Be prepared and able to respond to information security breaches promptly and effectively.

Notes

Data Intermediaries only take care of protection & retention obligation.

For more information on the Protection Obligation, refer to Chapter 17 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.
'A Guide Securing Personal Data in Electronic Medium' and 'Guide to Managing Data Breaches' are accessible from: https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-handling-access-requests-v1-0-(090616).pdf
https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Protection Obligation – Examples of Administrative Measures

- Requiring employees to be bound by confidentiality obligations in their employment agreements; (Non-Disclosure Agreements)
- Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;
- Having regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data; and
- Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Protection Obligation – Examples of Physical Measures

- Marking confidential documents clearly and prominently;
- Storing confidential documents in locked file cabinet systems;
- Restricting employee access to confidential documents on a need-to-know basis;
- Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops;
- Proper disposal of confidential documents which are no longer needed, through shredding or similar means;
- Implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security (e.g. registered post instead of normal post);
- Providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and
- Confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Protection Obligation – Examples of Technical Measures

- Ensuring computer networks are secure;
- Adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate); Eg. Setting up of rights
- Encrypting personal data to prevent unauthorised access;
- Activating self-locking mechanism for the computer screen if the computer is left unattended for a certain period; Eg. Screen saver
- Installing appropriate computer security software and using suitable computer settings;
- Disposing of personal data in IT devices which are to be recycled, sold or disposed;
- Using the right level of email security settings when sending and / or receiving highly confidential emails;
- Updating computer security and IT equipment regulatory; and
- Ensuring that IT service providers are able to provide the requisite standard of IT security.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Disposal of Personal Data on Physical Medium

Notes

Physical medium refers to paper, posters and photographs read-only storage media like CDs, DVDs, etc.

Re-writeable media like hard disks, USB memory sticks, etc. would be considered as "electronic media" as they allow for nearly unlimited overwriting of data, so that personal data may be disposed from these types of media without the need to dispose of the medium itself.

Disposal refers to the overall process of transforming or destroying information in a way that renders it unreadable (for paper records) or irretrievable (for electronic records). Incomplete disposal can lead to data breaches, such as:

- Deleted electronic files or improperly shredded paper may be restored (in full or partially); and
- Uncontrolled disposal of paper without destruction may lead to recovery of documents through 'dumpster diving' (e.g. sifting through physical waste or recycling containers for items that have been discarded, but are still of value or covered by regulation).

For personal data stored on paper, proper disposal or destruction usually refers to putting the paper through one or more of the following processes, e.g. shredding of paper followed by recycling:

- Incineration (or burning): reduces paper to ashes;
- Shredding: cuts paper in a way that makes it reasonably difficult, or even impossible, to reassemble the pieces in order to reconstruct (a substantial part of) the information;
- Pulping: paper is mixed with water and chemicals to break down the paper fibres before it is processed into recycled paper.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Typical Disposal Mistakes and Issues

It is a common mistake to neglect personal data where:

- It is only part of a whole data set (e.g. just the first page of a completed form);
- There are mistakes in some fields (therefore data is deemed inaccurate); or
- It contains printing errors (e.g. letter to customer printed with errors in the title or date).

Typical problems involving printouts containing personal data include:

- Recycling of paper is encouraged by the organisation, and without rules in place, paper meant for shredding is recycled without first destroying it;
- Staff is not sufficiently trained or aware about protecting personal data even when it is 'not used' anymore in the current form or has become obsolete;
- Staff not checking on the reverse page of waste/recycled paper whether it contains any personal data and that piece of paper is just simply discarded or left unattended;
- Containers meant to collect confidential documents are not sufficiently marked and differentiated from common collection containers, e.g. for recycling; or
- Confidential documents are left in an unsecured area.

Good Practices

To address typical issues and problems in destroying paper documents, the following best practices should be considered for implementation:

- When in doubt whether the paper document contains personal data, shred the document; and
- Encourage staff to shred paper documents containing personal data regularly to build up a habit. Shredded paper can still be sent for recycling, encouraging environmental sustainability.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Checklist of Good Practices for Disposal of Physical Media		
1.	If your organisation recycles used paper, are the staff reminded to check whether there is personal data left on the recycled paper? (If there is, those recycled paper should disposed of properly)	☐
2.	Are your staff aware that they should check if wastepaper (e.g. extra copies, wrong copies, unused copies) contains personal data and how to dispose of them properly?	☐
3.	Does your organisation leave wastepaper outside its premises unattended? If so, does your organisation first check that there are no confidential documents or documents containing personal data of individuals?	☐
4.	Is the paper shredding machine regularly cleared and serviced?	☐
5.	If your organisation has outsourced its document disposal, was there a review on how the third party disposes of the paper and whether such practises comply with the PDPA?	☐
6.	Has your organisation nominated a data protection officer, who is overall in charge of personal data protection, and to whom staff can refer to when they need further clarification on personal data protection and disposal?	☐
7.	Does your organisation have disposal policies in place, which determine how the different data must be disposed of, and are they regularly reviewed?	☐
8.	Does your organisation have retention policies in place, which determine when certain type of data should be disposed of or how long they should be archived for business reasons?	☐

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.7 PROTECTION OBLIGATION

Other Protection Obligation Cases

S/N	Cases
1	Breach of Protection Obligation by 'M' Company On 21 April 2015, the Complainant, Ms C, complained to the Personal Data Protection Commission that she had been receiving calls from unknown numbers, and that when she conducted a search on Google, she discovered that her personal data and those of her family members were posted online on http://siph0n.net ("Siph0n website"). The Complainant had attributed the posting on the Siphon website to a data "leak" on the Respondent's part. A warning was issued to the company for failing to make reasonable security arrangements to prevent unauthorised access to personal data held in M Company's IT systems. Source: https://www.pdpc.gov.sg/docs/default-source/enforcement-data-protection-cases/grounds-of-decision---metro-(210416).pdf?sfvrsn=2
2	Breach of Protection Obligation by 'F.H.' Communications The Complainant, [Redacted] (Replaced with Mr L), submitted a complaint to the Personal Data Protection Commission (the "Commission") on 4 March 2015 in respect of the way that the Respondent had collected and protected personal data at a lucky draw redemption counter operated by the Respondent. The specific matters that were raised in his complaint were as follows: Should not be enabled. a. The auto-fill function was enabled for the forms on the Respondent's laptops that a participant had to fill up to register for the lucky draw. This allowed a user to view from drop-down box the historical entries containing the personal information of the previous registering participants. b. The Respondent's laptop screens were in plain view of customers waiting in line behind the Complainant, which allowed them to view the personal information that was being entered into the laptop. c. The page containing the form was accessed through an unsecured Mozilla Firefox browser at the site: http://localhost/coupon/finish.php. d. The Respondent's staff did not appear to be adequately trained to ensure the protection of personal data collected at the redemption counter. A warning was issued to 'F.H.' Communications for failing to make reasonable security arrangements to prevent unauthorised disclosure of personal data on its computers at a furniture fair, which collected the data for a lucky draw Source: https://www.pdpc.gov.sg/docs/default-source/enforcement-data-protection-cases/grounds-of-decision---full-house-communications-(210416).pdf?sfvrsn=2

Notes

Eg. KBOX

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.8 RETENTION LIMITATION OBLIGATION

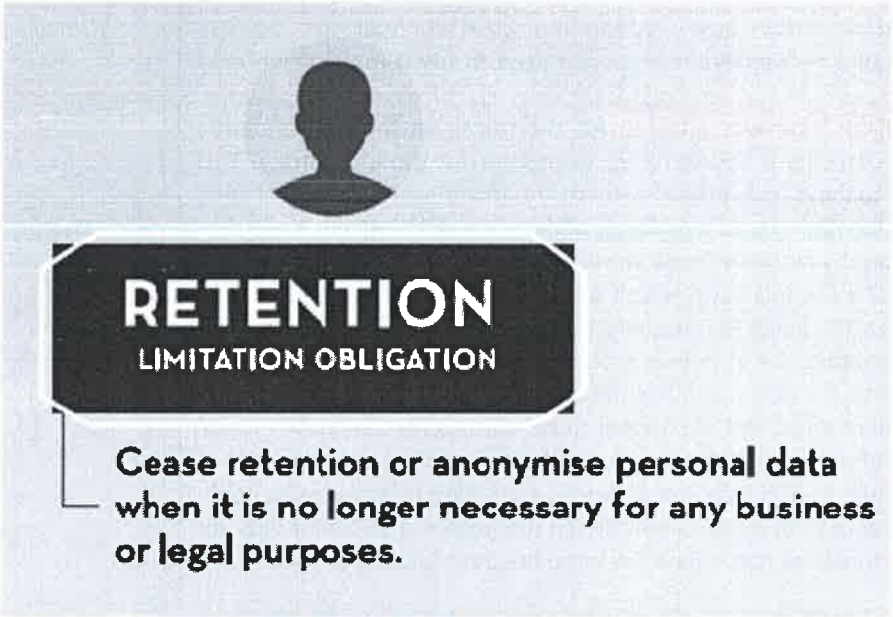
Organisation must cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that:

a) Purpose for which the personal data was collected is no longer being served by retention of the personal data; and

b) Retention is no longer necessary for legal or business purposes.

Retention period may depend on the following:

- The purpose(s) for which personal data was collected:
  - If one or more of the purposes for which it was collected remains valid;
  - Personal data should not be kept for "just in case".
- Other legal or business purposes e.g. legal action, required under other applicable laws or regulations, needed for generating annual reports, or performance forecasts, etc.



For more information on the Retention Obligation, refer to Chapter 18 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.8 RETENTION LIMITATION OBLIGATION

Retention Limitation Obligation – Examples

Notes

Example 1:

A dance school collects personal data of its tutors and students for purpose of maintaining an alumni network where the tutor or student is no longer with the school (with consent of the individual).

As this is a valid purpose, dance school is not required to cease to retain the data.

Example 2:

An interior design firm is engaged in a legal dispute with a former customer over the renovation of his home several years ago.

Interior design firm may retain records pertaining to the contract with its former customer for the purpose of legal proceedings.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.8 RETENTION LIMITATION OBLIGATION

Retention Limitation Obligation – Examples

Notes

Example 3:

A retailer retains billing information, including personal data, collected from its customers beyond the Point of Sale for the purposes of accounting and billing administration.

As the retailer is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation.

Example 4:

Under the Limitation Act (Cap. 163), actions founded on a contract (amongst others) must be brought within 6 years from the date on which the cause of action accrued. Hence an organisation may wish to retain records relating to its contracts for 7 years from the date of termination of the contract and possibly for a longer period if an investigation or legal proceedings should commence within that period.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.8 RETENTION LIMITATION OBLIGATION

Ceasing to Retain

For example, an organisation ceases to retain personal data when documents are:

- Destroyed;
- Disposed of in an appropriate manner;
- Returned to the individual concerned;
- Transferred to another person on the instructions of the individual concerned; or Eg. Car ownership, title deed (HDB Flat)
- Anonymisation – process of removing identifying information, such that the remaining data does not identify any particular individual. (The topic on Anonymisation will be covered in greater details in Chapter 2.13)

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

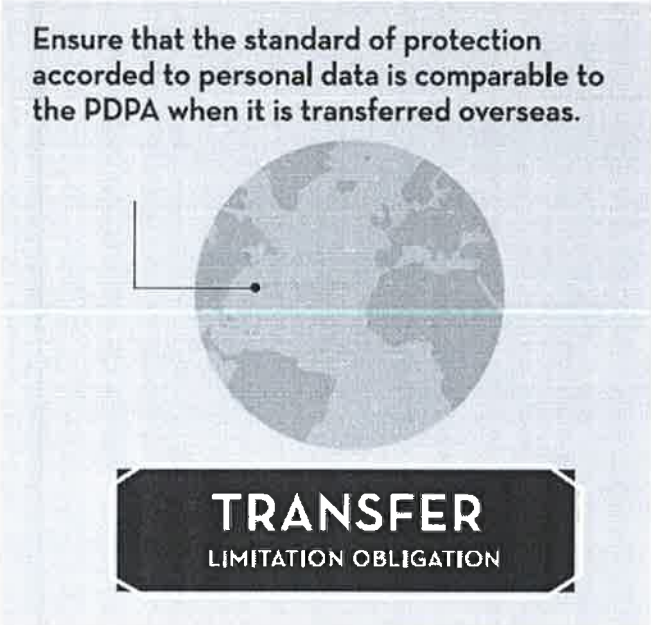
2.9 TRANSFER LIMITATION OBLIGATION

Transferring organisations that retain possession or control of personal data that is transferred out of Singapore must take steps to ensure its compliance with the DP Provisions.

Transferring organisation is taken to have satisfied the above requirements where the personal data is in transit or publicly available in Singapore.

For example:

- Implement appropriate security policies and measures to safeguard personal data while it is overseas.
- Implement policies and measures to ensure personal data is only used in accordance with the PDPA while it is overseas.



For more information on the Transfer Obligation, refer to Chapter 19 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.9 TRANSFER LIMITATION OBLIGATION

Transferring Personal Data Out Of Singapore

When transferring to a recipient outside Singapore, the transferring organisation must ascertain and ensure that the recipient is bound by legally enforceable obligations that provide a standard of protection that is at least comparable to the PDPA.

Legally enforceable obligations include:

- Any law
- Contracts*
- Binding corporate rules*
- Any other legally binding instrument

(*Must meet the prescribed requirements)



Transferring organisation is taken to have satisfied the requirements in certain circumstances.

Circumstances include:

- Individual is informed about how his personal data will be protected and **provides consent** (subject to conditions).
- Transfer is necessary for the **performance of a contract** between the transferring organisation and the individual.
- Transfer is necessary for the use/disclosure **where certain exceptions to consent for use/disclosure apply** (e.g. necessary to respond to an emergency that threatens individual's safety) and reasonable steps taken to ensure personal data will not be used/disclosed by recipient for any other purpose.
- The personal data is in **transit or publicly available in Singapore**.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.9 TRANSFER LIMITATION OBLIGATION

Transferring Limitation Obligation – Examples

Notes

Example 1:

Organisation ABC is transferring personal data of its customers to its parent company overseas via the group's centralised customer management system. The conditions of the transfer, including the protections that will be accorded to the personal data transferred, are set out in binding corporate rules that apply to both Organisation ABC and its head office. Organisation ABC has reviewed these binding corporate rules and assessed that they comply with the conditions prescribed under the regulations and would provide protection that is comparable to the standard under the PDPA.

In this case, Organisation ABC's transfer of the personal data overseas would be in compliance with the Transfer Limitation Obligation.

Example 2:

Karen purchases an overseas tour with travel agency DEF. In order to perform its obligation under its contract with Karen to make the necessary hotel reservations, travel agency DEF is required to transfer her personal data (such as her name, nationality and passport number) overseas to the hotels that Karen will be staying at during the tour.

Travel agency DEF's transfer of Karen's personal data in this case would be in compliance with the Transfer Limitation Obligation as it is necessary for the performance of the contract between travel agency DEF and Karen.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.9 TRANSFER LIMITATION OBLIGATION

Transferring Limitation Obligation – Examples

Notes

Example 3:

Cedric is a client of Organisation GHI. Organisation GHI notifies Cedric in writing that it is adopting a cloud-based solution to store and analyse its client data, which includes personal data such as clients' identification details, address, contact details and income range, and asks for Cedric's consent to move his client data to the cloud-based solution. Organisation GHI also provides Cedric with a written summary of the extent to which Cedric's personal data will be protected to a standard comparable to that under the PDPA, in the countries and territories that it will be transferred to.

Should Cedric provide his consent, Organisation GHI would be able to transfer his personal data in compliance with the Transfer Limitation Obligation.

Example 4:

John is injured in an accident while travelling overseas. To aid John's treatment, his family doctor in Singapore transfers some of his medical records (including personal data such as his identification details, blood type, allergies, and existing medical conditions) to the hospital where John is receiving medical attention, after confirming with the hospital that the personal data will only be used for John's medical treatment.

In this case, the transfer of John's personal data would be in compliance with the Transfer Limitation Obligation as the disclosure to the overseas hospital is necessary to respond to an emergency that threatens John's life, health or safety, and John's family doctor has taken reasonable steps to ensure that the personal data transferred will not be used or disclosed by the recipient for any other purpose.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.9 TRANSFER LIMITATION OBLIGATION

Transferring Limitation Obligation – Examples

Notes

Example 5:

Company JKL films a commercial at a location open to the public in Singapore. The commercial captures images of individuals who pass by the filming location. Company JKL wishes to transfer the commercial to its overseas partners for use in an advertising campaign.

In this instance, Company JKL's transfer of the commercial would be in compliance with the Transfer Limitation Obligation as the personal data in the commercial would be publicly available to the extent that the filming of images would be reasonably expected at that location.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

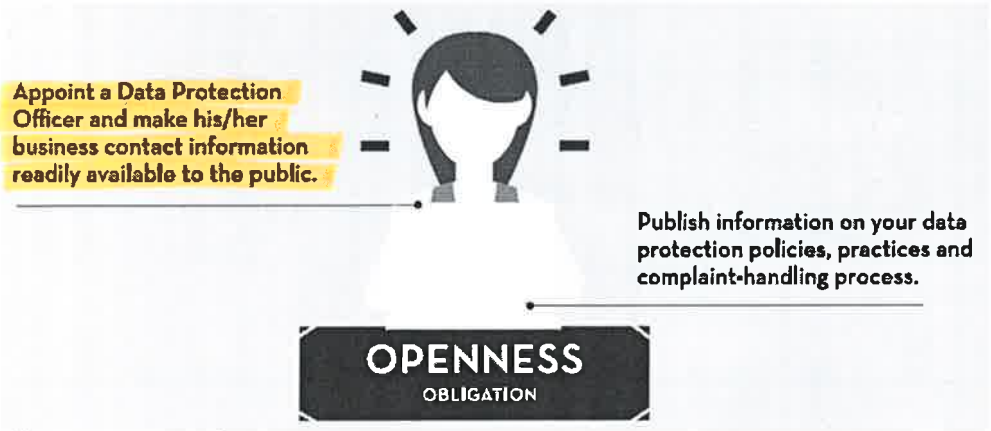
2.10 OPENNESS OBLIGATION

Organisation is required to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and to make information about their data protection policies and practices available.

In particular, organisation is required to designate at least one individual (data protection officer or "DPO") to be responsible for ensuring its compliance:

- Appoint one or more individuals;
- Designated individual may delegate responsibility conferred to another individual;
- Designation of individual does not relieve organisation of any of its obligations under the PDPA; and
- Make available BCI of a DPO or an individual to whom the DPO's responsibility has been delegated to.

This obligation will be discussed further in Chapter 3 on the role of Data Protection Officer.



For more information on the Openness Obligation, refer to Chapter 20 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.10 OPENNESS OBLIGATION

Accountability

- Individuals may request for access to their personal data;
- Individuals may submit a complaint to the Commission;
- Commission may give directions to the organisation to ensure compliance, (including amongst others) imposing a financial penalty of up to $1 million; (per offence)
- Individuals who suffer loss or damage directly as a result of a contravention of any provisions in:
  - ❖ Part IV – Collection, use and disclosure of personal data
  - ❖ Part V – Access to and correction of personal data
  - ❖ Part VI – Care of person data of the PDPA have a right of action for relief in civil proceedings.

Notes

Eg. Zest Tuition ($33,000)

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.11 EXISTING DATA AND OTHER EXISTING LAWS

Other Rights, Obligations and Uses

- Data Protection Provisions will not affect any authority, right, privilege, immunity, obligation or limitation by or under the law, except that performance of a contractual obligation shall not be an excuse for contravening the PDPA;

- Other written laws shall prevail over the Data Protection Provisions to the extent of any inconsistency between them; and

- Organisation may continue to use personal data that was collected before the appointed day for the purposes for which it was collected unless consent is withdrawn under the PDPA or the individual has otherwise indicated that he does not consent to such use.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.11 EXISTING DATA AND OTHER EXISTING LAWS

Other Rights, Obligations and Uses

Notes

Example 1:

A retailer has entered into a contract with a data aggregator under which it has agreed to sell certain personal data about its customers to the aggregator. The personal data involved includes the customers' names, contact details and certain information on products they have purchased from the retailer.

However, the retailer did not obtain the consent of the customers to disclose their personal data. With effect from the appointed day, the retailer must comply with the Data Protection Provisions and cannot assert its contractual obligations to the aggregator as a reason that it does not need to obtain the consent of its customers.

Example 2:

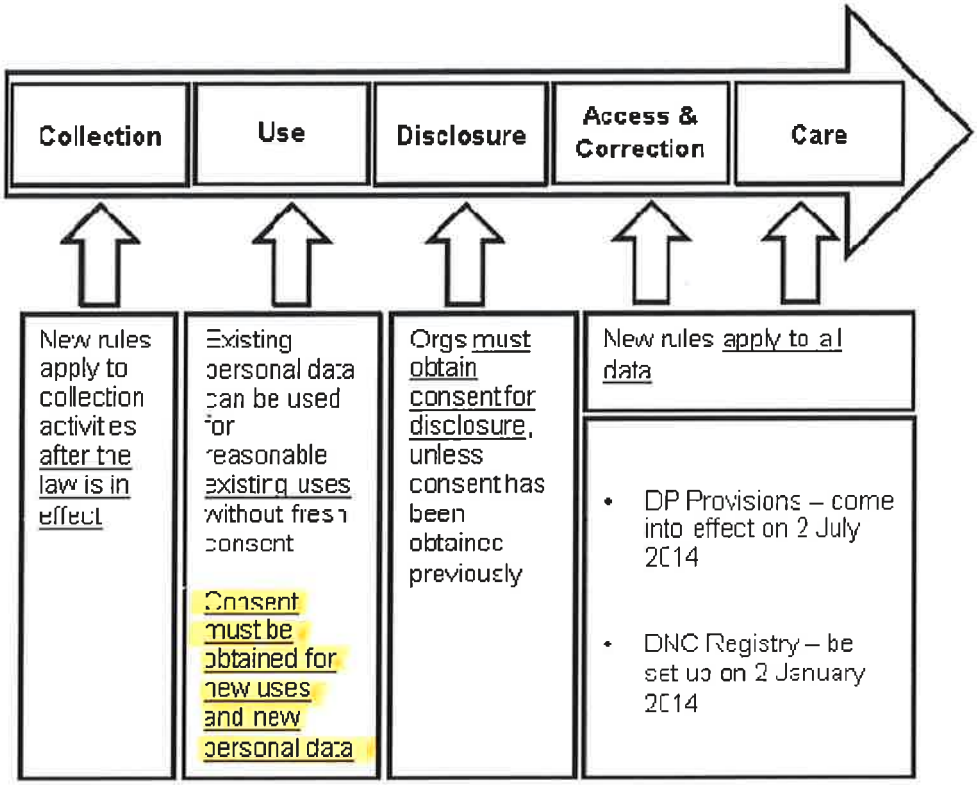
Organisation ABC has been using the personal data of their customers to send them desktop calendars once every year. This would be considered a reasonable existing use So long as their customers have not indicated to ABC that they no longer wish to receive these calendars (i.e. withdrawing their consent for the purpose of receiving calendars once every year), ABC can continue to do so without obtaining fresh consent after the appointed day.

Organisation XYZ has been selling databases containing personal data. This would be considered a disclosure of personal data and not a reasonable existing use under section 19. After the appointed day, XYZ needs to ensure that consent has been obtained before selling these databases again.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.11 EXISTING DATA AND OTHER EXISTING LAWS

Treatment for Existing Data (Collected before Appointed Day)



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.11 EXISTING DATA AND OTHER EXISTING LAWS

Existing Data – Examples

Notes

Example 1:

Organisation ABC has been using personal data to send customers desktop calendars annually before appointed day.

As personal data was collected before the appointed day and sending desktop calendars was a purpose for which the personal data was collected, ABC can continue to do without obtaining fresh consent, as long as customers had not indicated otherwise.

Example 2:

Organisation XYZ has been selling databases containing personal data.

This would be disclosure of personal data, XYZ needs to seek consent before selling the database.

Organisations may consider:

a) How the activity relates to the original purpose of collection;

b) Whether it would be clear to the individual concerned that the activity falls within the scope of the original purpose.

Not necessary that purpose have been notified to individuals.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

Notes

- PDPA applies to personal data of employees
- PDPA defines "employee" to include a volunteer, and "employment" to include working under an unpaid volunteer work relationship.
- Generally, organisations should obtain consent, unless an exception applies

Exceptions:

- Managing and terminating an employment relationship – no consent is required but requirements for notification of purpose and to provide BCI of person who is able to answer questions about such collection, use or disclosure
- Evaluative purpose

For more information on Employment, refer to Chapter 5 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

Notes

The definition of "evaluative purpose" in the PDPA includes:

a) For the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates;

(i) For employment or for appointment to office;

(ii) For promotion in employment or office or for continuance in employment or office;

(iii) For removal from employment or office;

(iv) For admission to an education institution;

(v) For the awarding of contracts, awards, bursaries, scholarships, honours, or other similar benefits;

(vi) For selection for an athletic or artistic purpose; or

(vii) For grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

Notes

Recruitment

- Job application – When an individual voluntarily provides his personal data in his job application to an organisation, his consent is deemed to be given to the organisation for collecting, using and disclosing the personal data for the purpose of assessing his job application. If the organisation wishes to use the personal data for other purposes, then the organisation must inform him and obtain his consent, unless relevant exceptions apply.

- Reference checks (ex-employers, other sources) – The evaluative purpose exception allow organisations to collect, use or disclose personal data without consent if it is for the purposes of determining the suitability, eligibility or qualifications of the job applicant for a job. For example, an organisation is not required to obtain consent to collect information about the job applicant from his ex-employers, if such collection is necessary for the organisation to evaluate the job applicant for employment.

- Use of BCI – If the individual provides his "Business Contact Information" in his business card for purposes other than solely for personal purposes, then the organisation is not required to comply with the Data Protection Provisions in respect of such contact information set out in the business card.

- Recruitment agencies – Recruitment companies, employment agencies, head-hunters and other similar organisations are subject to the Data Protection Provisions of the PDPA. Accordingly, unless an exception under the PDPA applies, recruitment agencies will have to inform job applicants of the purposes for which they are collecting, using or disclosing their personal data, and obtain consent before doing so.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

Notes

Employees

- Performance assessment – the collection of the personal data of an employee that is necessary for determining the suitability, eligibility or qualifications of the employee for promotion, continuing their employment contract, or for terminating their employment contract is an exception to the requirement for consent. An organisation may obtain information about its employee without the consent of the employee, if such collection is necessary for such evaluative purposes.

- Under the PDPA, the collection by organisations of personal data about their employees for the purpose of managing or terminating their employment relationships, and the use or disclosure of such personal data for consistent purposes would not require the consent of their employees. Using the employee's bank account details to issue salaries, or monitoring how the employee uses company computer network resources are possible purposes which may fall under this exception. However, the PDPA requires organisations to inform their employees of the purposes of such collection, use or disclosure, even though their consent is not required.

Former Employees

- Even after the employee is no longer working with the organisation, the organisation may continue to retain personal data about the former employee that was collected during his employment period if the purpose for which the personal data was collected is still being served by retention or if retention is necessary for other business or legal purposes.

Check:
1. ACRA
2. IRAS
3. MOM



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

Notes

Example:

An employer collects information about the projects an employee has worked

on to determine whether to promote him (an evaluative purpose), and to conduct audits on his finance claims (a purpose for managing and terminating an employment relationship).

The employer need only notify the employee that his personal data is being collected for audit purposes. The employer does not need to obtain consent from the employee for the collection of his personal data or inform him that he is being evaluated for promotion to a higher job grade.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – Employment

- Can organisations collect and use personal data on the job applicant from social networking sources (e.g. Facebook or Twitter)?
- What is the difference between the exception for evaluative purposes and the exception for the purpose of managing and terminating an employment relationship?
- Can organisations use the information in business cards for recruitment? Yes for BCI.
- How long can organisations continue to hold personal data of former employees?
- Are organisations responsible if their employees do not comply with the PDPA? Are volunteers considered employees? No.
- Do the exceptions to the Consent Obligation for the collection, use and disclosure of personal data of employees also apply to individuals that may act on behalf of an organisation, but are not the organisation's employees?

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – NRICs

Notes

- Collection and retention of the physical NRIC card are not governed by the PDPA. However, NRIC cards contain personal data which would be subject to the PDPA.
- Under PDPA, individuals have to be informed of and consent to the purposes for which their personal data, including NRIC numbers, are collected, used, and disclosed by organisations.
- As a best practice, organisations should avoid over-collecting personal data, including NRIC numbers, where this is not required for their business or legal purposes. Organisations should consider whether there may be alternatives available that address their requirements.
- Organisations may publish NRIC numbers if consent had been obtained from the individual(s) concerned. However, as a good practice, organisations should only publish the amount of personal data necessary to fulfil the relevant purpose. For example, when publishing personal data of the winners of a lucky draw, organisations are advised to reveal only a portion of the NRIC number such as the last three digits and the letter. Organisations should use the full NRIC number only when necessary, for example to confirm the identity of someone who is coming forth to receive the winning prize.



For more information on NRIC, refer to Chapter 6 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.12 SELECTED TOPICS – EMPLOYMENT, NRIC

Selected Topics – NRICs

Notes

Example 1 :

John calls his service provider to make some queries concerning the services he has subscribed for. Instead of asking for John's NRIC number, the service provider could ask for other information such as John's account number or mobile number to verify his identity, if the service provider would already have such other information about John in the course of providing the service.

Example 2 :

Jane is visiting her friend who lives in a private condominium. The security guard asks for Jane's full name and NRIC number, for the purpose of checking it against the guest list provided by the residents. In this situation, the security guard is collecting Jane's personal data for a reasonable purpose. The security guard should make reasonable security arrangements to protect Jane's personal data – for example, to prevent unauthorised disclosure to subsequent visitors.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – Photography

Notes

An image of an identifiable individual captured in a photograph is personal data. Among other obligations, the Data Protection Provisions require consent from the individual to be obtained for the purposes of collection, use or disclosure of the personal data.

Exceptions to this Consent Obligation may apply, for e.g.

- Where the photographer is acting in personal or domestic capacity, such as when an individual takes photographs for his own personal uses at a family gathering; or
- Where the photograph is taken at an event or location that is open to the public.



For more information on Photography, refer to Chapter 9 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – Photography

Notes

Example 1: What are some ways organisations can obtain consent from guests for photo taking at private functions?

Organisation ABC holds a private function for a select group of invited clients. ABC wishes to take photos of attendees for its internal newsletter with their consent.

Organisation ABC can obtain consent by:

- Stating on the registration form that photographs will be taken, and requiring individuals who wish to attend the function to sign and return the form.

If Organisation ABC intends to rely on deemed consent, it can better ensure that the individuals voluntarily provided their personal data for the purpose by:

- Putting an obvious notice at the reception or entrance of the function venue to inform attendees that photographs will be taken at the event for publication in its internal newsletter.

Example 2: What should organisations do when an individual in a group photo withdraws consent?

Organisation ABC obtains consent to take a photograph of a group of individuals at a corporate event, for publication in its internal newsletter. One of the individuals, John, subsequently withdraws his consent.

Organisation ABC should give effect to John's withdrawal by ceasing future publication of the photo or publishing it without John's personal data (e.g. masking John's image), unless disclosure without consent is required or authorised under the PDPA or other written law.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Other Photography Cases

S/N	Cases
1	Submission of photographs for a competition Alan is a professional photographer. He takes a photograph of his aunt Betty at a family event, and subsequently submits it for a competition for professional freelance photographers organised by Organisation ABC. The winner of the competition will receive a contract to provide services as the official photographer at an event conducted by Organisation ABC. Alan is unlikely to be considered to be acting in a personal or domestic capacity, and the Data Protection Provisions will apply to his use or disclosure of the personal data unless any other exceptions apply. Alan submits the same photograph of his aunt Betty for a photography competition organised by Social & Recreational Club DEF on the club member's favourite family member. The competition is open to all members of the social and recreational club and the prize is a free holiday for the winner and his favourite family member. Alan is likely to be considered to be acting in a personal or domestic capacity, and the Data Protection Provisions will not apply to his use or disclosure of the personal data.
2	Collection in breach of Data Protection Provisions Jessie informs Organisation XYZ that it had collected her personal data without her consent by taking an identifiable photograph of her, and asks it to destroy the photograph. Organisation XYZ determines that its collection (and any subsequent use or disclosure) of Jessie's personal data may have been in breach of the Data Protection Provisions. In this case, Organisation XYZ should cease any further use or disclosure of Jessie's personal data. Where continued retention of Jessie's personal data constitutes a breach of the Data Protection Provisions21, Organisation XYZ should also cease such retention.

Notes

Need to obtain consent. PDPA applies.
⇒ Competition for professional free-lancer.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – CCTV

Notes

- Organisations should provide notifications and obtain consent for the collection, use or disclosure of personal data contained in CCTV footage, unless an exception applies.

- Notices or other forms of notifications should be placed in a manner that enables individuals to have sufficient awareness that CCTVs are in operation. For example, it may be appropriate to place a notice at points of entry to a building or prominent locations in a venue or a vehicle, where individuals are able to read the notice prior to collection of their personal data.

Do not forget carparks.

> *Example:*
> *ABC deploys CCTVs for security purposes at the entrance to its office premises. It places a notification at the entrance to its office, which clearly and prominently states the use and purpose of video surveillance.*
>
> *Such notifications would be considered sufficient for the ABC's purpose.*

- The placement or content of notifications to reveal the exact location of the CCTVs is not required. Organisations may provide notice that CCTVs are deployed in the general locale instead of indicating the specific points where the CCTVs are installed.

- In collecting CCTV footage beyond the boundaries of its premises, organisations should consider the extent of coverage that is reasonable for the purpose of installing the CCTVs, although the PDPA does not prohibit an organisation from having CCTVs that collect footage beyond the boundaries of its premises.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – CCTV

Notes

- In the case of processing an access request for CCTV footage, an organisation is generally required to provide the individual access to personal data requested, unless the request falls within one of the prohibitions or any exception under the PDPA.

- When an organisation decides to provide access, organisations should provide a copy of the CCTV footage and have the option of charging the individual a reasonable fee for providing the copy. If the CCTV footage resides in a form that cannot be provided to the individual in physical or electronic copies, (e.g. the data cannot be extracted from a special machine owned by the organisation), or if it is prohibitively costly to provide the footage in the aforementioned formats, then the organisation may provide the individual a reasonable opportunity to examine the requested data in person, with appropriate masking of the personal data of other individuals where required.

For more information on CCTVs, refer to Chapter 4 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – CCTV

Notes

Is an organisation required to accede to requests to delete CCTV footage?

The PDPA does not require an organisation to delete personal data upon request from an individual. Nonetheless, individuals may at any time, upon giving reasonable notice, withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation.

Examples (video masking methods):

- "Video masking" refers to the process of concealing parts of the video from view. Video masking may include masking certain body parts or inanimate objects that could potentially disclose the personal data of an individual.
- The common types of masking include:
    i. Solid colour masking
    ii. Blur masking
    iii. Pixelated masking
- Where solid colour masking is used, no details or movement in the scene covered by the masked area can be viewed. However, when pixelated or blurred masking is used, the resulting image enables a partial outline to be seen but detailed features will be obscured. This may be a less foolproof method as it is possible for pixelated or blurred images of individuals to still be identifiable.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

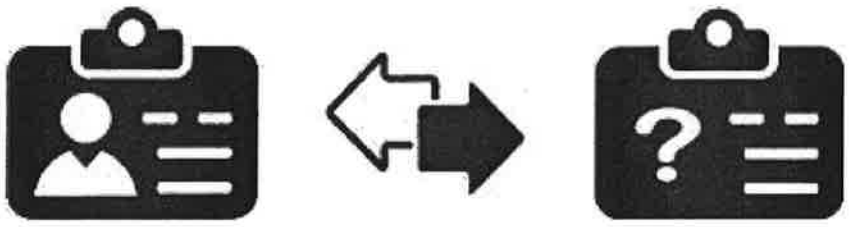
Selected Topics – Anonymisation

Notes

In general, anonymisation refers to the process of removing identifying information, such that the remaining data does not identify any particular individual. In the context of the definition of personal data under the PDPA, anonymisation refers to the conversion of personal data into data that cannot be used to identify an individual whether from that data itself, or from that data and other information to which the organisation has or is likely to have access.

Some examples of anonymisation techniques include:

- Pseudonymisation – replacing personal identifiers with other references;
- Aggregation – displaying values as totals, so that none of the individual values which could identify an individual is shown;
- Replacement – replacing values or a subset of the values with a computed average or a number derived from the values;
- Data reduction – removing values that are not required for the purpose;
- Data suppression – banding or hiding the value within a given range;
- Data shuffling – mixing up or replacing values with those of the same type so that the information looks similar but is unrelated to the actual details;
- Masking – removing certain details while preserving the look and feel of the data.



For more information on the Anonymisation, refer to Chapter 3 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Anonymisation – Re-identification

Notes

Re-identification is the process by which anonymised data is combined with other information such that an individual can be identified and becomes personal data.

- Lowering re-identification risks:
  - Limiting disclosure to restricted persons;
  - Imposing additional enforceable restrictions on the use and subsequent disclosure of the data;
  - Implementing processes to govern proper use of the anonymised data in line with the restrictions, including access restrictions; and
  - Implementing processes and measures for the destruction of data as soon as possible.
- Organisation should assess risk of re-identification, if it intends to publish or disclose the data set to another organisation.
- E.g. motivated-intruder test in UK Information Commissioner's Office (ICO)'s Code of Practice "Anonymisation: Managing Data Protection Risk Code of Practice".

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Unique Identification by Combining Zip Code, Sex, Birth date

Notes

Example 1: Re-identification

Latanya Sweeney, a computer science professor, conducted a study in 1990 and found that data sets containing zip code, birth date, and sex could be combined to uniquely identify 87% of the United States population.

She was able to identify a Massachusetts governor from two data sets:

- A purchaser of health insurance for employees disclosed a data set from which names, addresses, social security numbers had been removed but not the zip codes, sex and birth dates of the employees.
- The information disclosed by the purchaser of health insurance was combined with data from voter rolls, which included name, zip code, address, sex, and birth date of voters in Cambridge, where the governor resided.

Re-identification was possible because:

- From the first data set, only six people in Cambridge were born on the same day as the governor, half of them were men.
- The voter rolls revealed that the governor was the only one who lived in the zip code.

The resultant combined data that re-identified the governor revealed information about his health and medical diagnosis.

Source: http://dataprivacylab.org/dataprivacy/projects/kanonymity/index.html

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Netflix Study

Notes

Example 2: Re-identification

As part of a competition in 2006, Netflix released data on user ratings for its movies over a six-year period.

Netflix applied anonymisation techniques to the data before releasing it:

- removing usernames
- assigning unique identification numbers in place of the usernames in order to continuously track user ratings and trends.

Despite anonymisation attempts, researchers at the University of Texas at Austin were able to cross-relate this information with a publicly available movie database (IMDb) and uniquely identify individual Netflix users.

Results of their study:

- 99% of users in the Netflix database can be identified if a person has information on when and how a user rated at least six movies.

Source: http://epic.org/privacy/reidentification/

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Example :

Organisation CBA published masked NRIC numbers of the winners of its recent lucky draw. The masked numbers only revealed the first 3 digits of their NRIC numbers. Since the first two digits typically reveals one's birth year, it could be ascertained that one of the winners was 28 years of age.

Around the same time, a newspaper article on the lucky draw reported that the two youngest participants were both 28 years of age. However, insofar as it was only a guess as to which of the two youngest participants might be the winner, re-identification did not occur.

However, the ability to narrow down possible identities is a factor that increases the probability of re-identification. In this example, if CBA had also published the full names of the winners, the data published by CBA could be found to have a non-trivial risk of re-identification.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Example :

Company V is an online retailer selling consumer products. As part of its effort to understand customer needs and improve its product delivery times, it analyses customer purchases to identify linkages between what products are sold at various times of the year and at which geographic locations. Company V outsources its marketing research function to Company Z. Before disclosing data on customer purchases, V anonymises the data so that only the times, locations and items purchased were left unmodified.

In this scenario, V would still be expected to protect the entire dataset as personal data if it retains the ability to re-identify a customer's purchasing patterns from that data.

However, it is unlikely that Z would be considered to have collected personal data about V's customers, if Z does not possess or is unlikely to have access to any other information which can identify V's customers when combined with the purchase history provided by V.

If Z possess complementary information, for example, another dataset

correlating the times of purchases made from V and the names of the individuals who made those purchases, and is able to match these information with the data provided by V, then the data provided by V is also considered personal data to Z.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – Research & Analytics

Notes

Example 1: Research & Analytics

John signs up for a mobile service with a telecommunications service provider. John consents to his personal data being collected and used by the service provider for the purposes of providing him the mobile service. The service provider collects and analyses some of John's personal data for the purposes of managing its network and planning enhancements to improve the quality of mobile services provided to him.

Such activities would likely fall within the original purpose John consented to.

Example 2: Research & Analytics

An adventure camp company requires all camp participants to provide emergency contact information of an individual, which includes personal data like name, telephone number and address, with consent from the individual. The purpose stated was to use that personal data to contact the individual in the event of an emergency relating to the camp participant. The company subsequently analyses the personal data for the purpose of determining if the individual(s) listed would be a potential camp participant.

This purpose would not fall within the original purpose for which the consent was obtained.



For more information on Analytics and Research, refer to Chapter 2 of the Advisory Guidelines for Selected Topics In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.13 SELECTED TOPICS – PHOTOGRAPHY, CCTV, ANONYMISATION, RESEARCH & ANALYTICS, ONLINE ACTIVITIES

Selected Topics – Online Activities

Notes

An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address.

Web cookie is a message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server.

The main purpose of many cookies is to identify users and possibly prepare customised web pages for them. When user enters a web site using cookies, user may be asked to fill out a form providing such information as user's name and interests. This information is packaged into a cookie and sent to user's web browser which stores it for later use. The next time user goes to the same web site, user's browser will send the cookie to the web server. The server can use this information to present user with custom web pages. So, for example, instead of seeing just a generic welcome page, user might see a welcome page with user's name on it.

- Are IP addresses personal data? No
  - IP address in itself is not personal unless an individual can be identified from the IP address and other available information such as recorded information (e.g. information recorded on the devices), established fact, and personal knowledge.
- Must consent be obtained for the use of cookies? Depends
  - Not all cookies collect personal data and consent is not needed for cookies that do not collect personal data.
  - If collection, use or disclosure of personal data is involved, then consent is generally needed.
- Are organisations allowed to use cookies for behavioural targeting? Depends

The individual's consent is required where this involves the collection or use of personal data.

For more information on Online Activities, refer to Chapter 7 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

- Do Not Call Provisions apply in relation to an organisation sending specified messages to Singapore telephone numbers.
- Do Not Call Provisions apply when:
  - The sender of the specified message is in Singapore when the message is sent; or
  - The recipient of the specified message is in Singapore when the message is accessed.
- Do Not Call Provisions do not apply if both the sender and the recipient are not in Singapore when the message is sent and accessed respectively.
- Do Not Call Provisions came fully into effect on 2 January 2014.

Window of 30 days.



For more information on the Do Not Call Provisions, refer to Chapters 24 - 34 of the Advisory Guidelines On Key Concepts In The Personal Data Protection Act.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

DNC Registry – Specified Message

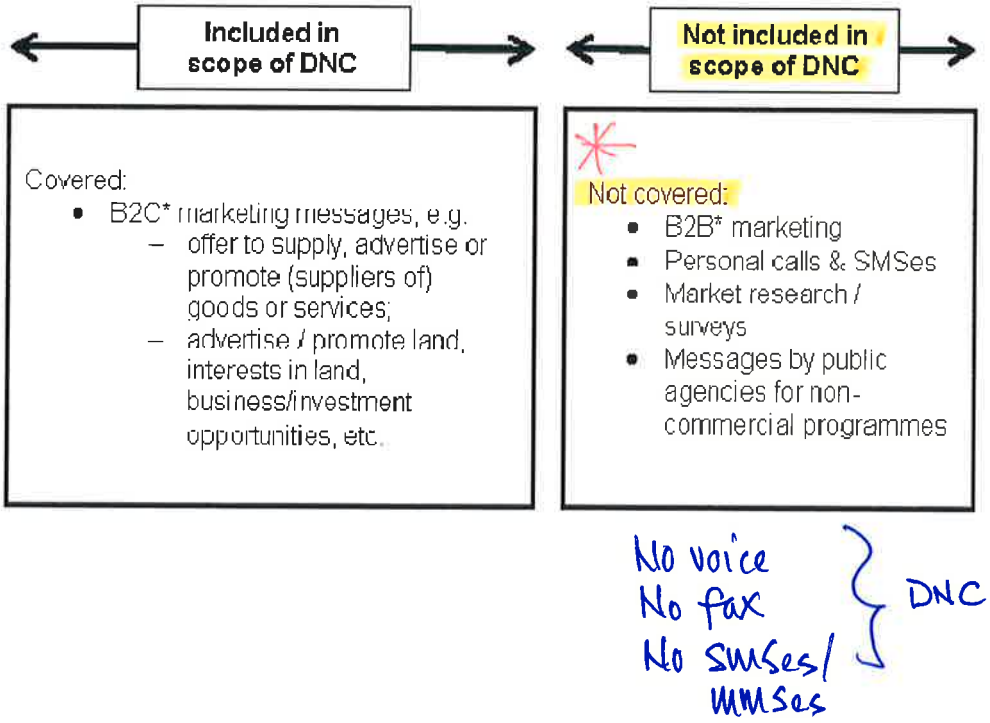
Notes

* B2C – Business to Consumer

* B2B – Business to Business

B2B Marketing Messages

As noted above, one of the excluded messages relates to messages sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation. This exclusion addresses B2B marketing messages and purposes, for example, where company A wishes to market its goods or services to company B, for the purposes of company B. A marketing message sent to an individual acting in a personal or domestic capacity would not be considered a B2B marketing message, even if the message purports to be for a purpose of an organisation.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Specified Message Definition*

A message is a Specified Message if the purpose of the message, or one of its purposes, is:

a) to advertise, promote or offer to supply or provide:

   (i) goods or services;

   (ii) an interest in land; or (land banking)

   (iii) a business opportunity or an investment opportunity;

b) to advertise or promote a supplier/provider (or a prospective supplier/provider) of the items listed in sub-paragraphs (i) to (iii) above; or

c) any other prescribed purpose related to obtaining or providing information.

*See Section 37 for complete definition of "Specified Message". Exclusions from the meaning of Specified Message are set out in the Eight Schedule.

Notes

For more information on 'Definition of a Specified Message', refer to Chapters 2 to 4 of the Advisory Guidelines On The Do Not Call Provision In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Specified Message –Examples

Notes

Example 1: Market research

ABC has been engaged to produce a market research report which illustrates the correlation between investment habits and income, profession and marital status of working Singaporeans aged 25-40. ABC calls Sarah for the sole purpose of gathering information for the report.

Message is excluded under the Eighth Schedule. (Exclusion from meaning of "specified message")

Example 2: Market research followed by offer of goods or services

ABC also calls John to gather information for the report. After John finishes answering all the questions related to the report, ABC asks if John would consider purchasing one of ABC's market reports. In this case, one of the purposes of the call is to offer goods or services to John.

Message is a specified message.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Specified Message – Examples

Notes

Example 3: B2C telemarketing

Agent calls an individual to sell life insurance policies.

It is a specified message.

Example 4: B2B telemarketing

Agent calls an organisation to sell corporate insurance policies.

Message is excluded under the Eighth Schedule. (Exclusion from meaning of "specified message")

Example 5: Notification concerning changes in terms or status of commercial relationship

Agent calls an existing customer to notify expiry of policies / change in terms of policies.

Message is excluded under the Eighth Schedule. (Exclusion from meaning of "specified message")



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Other DNC Examples and Treatment

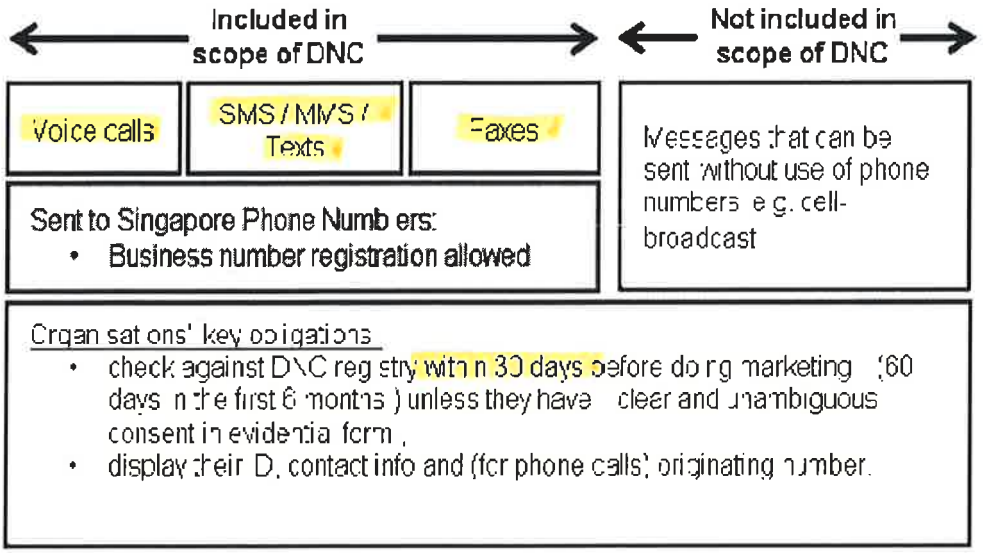
S/N	Example	Treatment
1	ABC organisation sends the following message via voice call, SMS, or fax to John's Singapore telephone number: "ABC would like to send you information about special offers from time to time."	ABC would be considered to have sent a specified message to a Singapore telephone number.
2	ABC organisation sends the following message via voice call, SMS, or fax to John's Singapore telephone number: "ABC would like to send you information about special offers from time to time. Are you registered on any of the DNC Registers? Please reply [Y] or [N]."	ABC would be considered to have sent a specified message to a Singapore telephone number.
3	ABC organisation sends the following message to John's email address: "ABC would like to send you information about special offers from time to time."	ABC would not be considered to have sent a specified message to a Singapore telephone number.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

DNC Registry



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Clear and Unambiguous Consent – Examples

Notes

Example 1:

Sarah fills out a form with a check box next to a clause that clearly states "Please send me special offers about Organisation ABC's products by SMS". This clause is clearly printed directly above where Sarah has to sign the application form. Sarah ticks the check-box and signs the form.

Example 2:

Sarah fills up an online form. This clause is directly above the "Submit" button.

I would like to receive information about promotions and offers by:

( ) Phone

(✓) SMS

(✓) Email

( ) Mail

Sarah puts a tick against the SMS and Email boxes and submits the online form.

For more information on 'Requirement to Obtain Clear and Unambiguous Consent in Evidential Form', refer to Chapters 5 to 7 of the Advisory Guidelines On The Do Not Call Provision In The Personal Data Protection Act.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Other DNC Examples and Treatment

S/N	Example	Treatment
1	ABC organisation sends the following message via voice call, SMS, or fax to John's Singapore telephone number: "ABC would like to send you information about special offers from time to time. Please reply [Y] if you agree."	ABC would be considered to have sent a specified message to a Singapore telephone number.
2	ABC organisation sends the following message to John's email address: "ABC would like to send you information about special offers from time to time by SMS to your Singapore telephone number. Please reply [Y] to this email if you agree."	ABC would not be considered to have sent a specified message to a Singapore telephone number. If John replies Y to the email, ABC would likely be considered to have obtained clear and unambiguous consent from John to send him specified messages by SMS to his Singapore telephone number if they are able reproduce the consent given when required to do so subsequently.
3	An organisation, ABC, is a market research firm that has been engaged to produce a report which illustrates the correlation between investment habits and income, profession and marital status of working Singaporeans aged 25-40. ABC calls Sarah on her Singapore telephone number for the purpose of gathering information for the report. After Sarah finishes answering all the questions related to the report, ABC informs Sarah that she would be entitled to a gift as a token of appreciation for her participation in the form of one of the following: a) A stationery set worth $15; or b) A gift voucher that can be redeemed at 123 Bakery.	As the sole purpose of ABC's call is to conduct market research or a market survey, ABC is not considered to have sent a specified message.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Sender of Specified Message

The "sender" of the specified message is responsible for complying with the Do Not Call Provisions.

"Sender" refers to a person –

a) who sends the message, causes the message to be sent, or authorises the sending of the message; or

b) who makes a voice call containing the message, causes a voice call containing the message to be made, or authorises the making of a voice call containing the message.

If Person A authorises Person B to promote his goods, services, land, interest or opportunity, Person A would be deemed to have authorised the sending of any message for that purpose, unless Person A had taken reasonable steps to prevent Person B from doing so. The determination of whether reasonable steps had been taken depends on the specific facts in question.

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Sender of Specified Message – Examples

Example 1

Developer appoints an agent to market its property. Developer states in its contract with the agent that the agent shall not send any message, whether in sound, text or other form, to a Singapore telephone number to offer, advertise or promote the property.

Developer is likely to have taken reasonable steps to prevent sending of Specified Message.

Example 2:

Developer appoints an agent to market its property, but does not state conditions on marketing.

Developer unlikely to have taken reasonable steps to prevent sending of Specified Message.

Notes

} Better to state this in the contract betw developer & agent.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Exemption Order in Brief

Organisations are only exempt from duty to check the relevant DNC Register where:

- Current **on-going relationship** with recipient
  - Past relationships or one-off transactions not included
- Message **relates to subject of on-going relationship**
  - Unrelated messages not exempted
- Text or Fax message only
  - Does not apply to voice calls



Other conditions:

- Information on how to opt out provided in the message:
  - Same mode as message (i.e. by SMS or fax), no additional charges other than usual fax/text message charges
  - Once opt out, NO further exempt message may be sent to the same number after 30 days
- Individual has not withdrawn consent for or not indicated that he does not consent to the sending of any Specified Message

An exempt message must in any case:

- still have to include clear and accurate information (i) identifying the individual or organisation who sent or authorised the sending of the message; and

  (ii) about how the recipient can readily contact that individual or organisation; and
- where the message is sent via a voice call, not have its calling line identity concealed or withheld.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

On-going Relationship – What It Is or Is Not

- On-going relationship – examples:
  - Membership
  - Subscription
- Not on-going relationship: one-time transactions – examples:
  - Individual calls salesperson to enquire about a property
  - Individual visits a show flat
  - Individual made an appointment/reservation and left his number

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Message Related to Subject of On-going Relationship – Examples

- Credit card company informing card holder that if he uses its credit card at a department store, he can enjoy additional discounts
- The credit card company CANNOT rely on this exemption to notify individual of a launch of property development (this is unrelated to the service they provide individual)

Note: Data Protection Provisions will apply concurrently from 2 July 2014.

Notes

Examples - 'on-going relationship'.

1	Subject of the ongoing relationship between the sender and the subscriber or user of the Singapore telephone number	Message which purpose is related to the subject of the ongoing relationship
2	Recipient is an existing subscriber to ABC Magazine	XYZ Magazine and ABC Magazine are fashion magazines.) "Enjoy 20% off subscription rates to XYZ Magazine." "Get the ABC 2015 calendar, featuring the most popular cover pages of ABC Magazine."
3	Recipient is an existing home fixed-line broadband service subscriber	"Enjoy faster speeds with fibre broadband at only $X a month."
4	Recipient is an existing member of a club or society	"Course for all society members on improving interview and communication skills. Sign up now." "Members enjoy 10% discount at all F&B outlets in the club. Sign up now."

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

DNC Operational Rules

Notes

Creating an Account (For tele-marketing)

- 3 types of accounts for:
  - Organisations registered in Singapore
  - Overseas organisations with no presence in Singapore
  - Individual who needs to check e.g., agents, freelancers etc.
- Each organisation is entitled one main account and as many sub-accounts as required

	1. Registered in Singapore		2. Registered Overseas		3. Individuals
Account	Main	Sub - acct	Main	Sub - acct	Main
One-time Fee	$30	$30 each	$60	$30 each	$30
Annual Free Credits	1,000	None	1,000	None	1,000

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Checking the DNC Registry

Notes

- Account holders to login to the DNC Registry website (www.dnc.gov.sg) to submit their telephone numbers for checking
  - Singpass for local organisation and individuals
  - Issued ID for foreign organisation
- Telephone numbers submitted will be checked against all 3 DNC Registers.
- 2 methods of submitting telephone numbers for checking:

	Small Number Lookup	Bulk Filtering
Submission	Up to 10 at a time	As many as required
Turnaround Time	Immediate	Up to 24 hours – user will be notified of results via email

- Any organisation/individual checking the DNC Registry on behalf of others will have to declare the identity and particulars of the organisation(s) they are checking the registry on behalf of.
- The list can be created during account creation and amended subsequently.



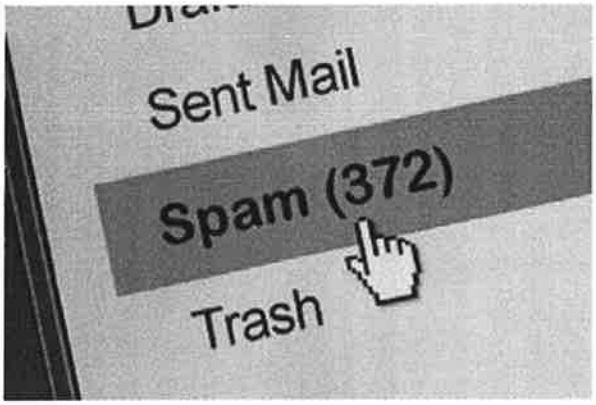
© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Spam Control Act ("SCA") and Do Not Call Provisions ("DNC Provisions")

Notes

While the SCA governs the manner in which the spam message may be sent, the Personal Data Protection Act ("PDPA") applies to the collection, use and disclosure of individuals' personal data for such purposes. These frameworks will operate concurrently.



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

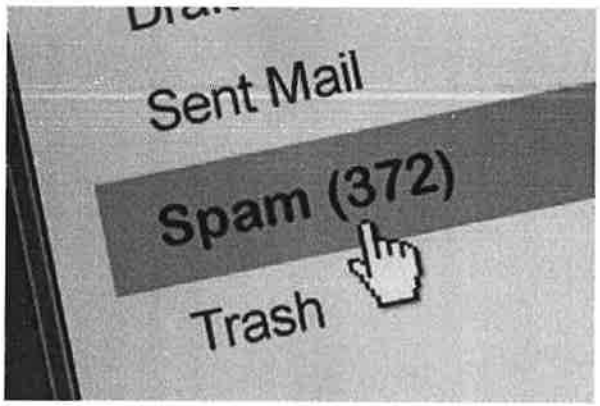
2.14 DO NOT CALL PROVISIONS

Spam Control Act ("SCA") and Do Not Call Provisions ("DNC Provisions")

Notes

Here is a table setting out a brief overview of the regime under the DNC Provisions and the SCA.

Do Not Call Provisions	Spam Control Act
The DNC Provisions apply to the sending of "Specified Messages" to Singapore telephone numbers.	The SCA sets out a framework to manage unsolicited "commercial electronic messages" sent in bulk to electronic mail addresses or mobile telephone numbers, otherwise known as "spam".



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.14 DO NOT CALL PROVISIONS

Do Not Call Provisions	Spam Control Act	Notes
Organisations must either have obtained clear and unambiguous consent to the sending of the Specified Message or check with the DNC register to ensure that they do not send specified messages to a Singapore telephone number (unless the Exemption Order can be relied on and the conditions therein are met). In addition, the messages must contain clear and accurate information identifying the individual or organisation sending or authorising the sending of the messages, as well as its contact details; and if making a phone call, the calling line identity must not be concealed.	Unsolicited commercial electronic messages sent in bulk are required to comply with the requirements set out in the Second Schedule of the SCA. These include, amongst other requirements, the requirement not to send further unsolicited commercial electronic messages 10 business days after an unsubscribe request was made using the unsubscribe facility provided. There are also labelling requirements, such as including the letters "<ADV>" and not to use misleading headers, etc.	
Individuals who continue receiving unsolicited telemarketing calls after registering their telephone numbers with the DNC Registry may file a complaint with the PDPC. Breaches of the duties under the Do Not Call Provisions could constitute a criminal offence.	The SCA, adopts a civil-based regime. Parties who have suffered loss or damage due to non-compliance with the Second Schedule of the SCA can take legal action directly against the sender (amongst others).	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

The PDPA confers various powers on the Commission to enforce the Data Protection Provisions.

These powers may be categorised as:

- Powers relating to alternative dispute resolution. other modes of dispute settlement.
- Powers relating to reviews.
- Powers relating to investigations.
- In exercising its powers to enforce the Data Protection Provisions, the Commission's approach takes into account two main objectives. These are:
    - to facilitate the resolution of an individual's complaint relating to an organisation's contravention, or alleged contravention, of any of the Data Protection Provisions; and
    - to ensure that organisations comply with their obligations under the Data Protection Provisions and, in the event an organisation does not comply with any of the Data Protection Provisions, to ensure that it takes the appropriate corrective measures and any other necessary action in a timely manner.



Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

- Where the Commission receives a complaint from an individual relating to a contravention, or possible contravention, of any of the Data Protection Provisions by an organisation, the Commission will generally prefer to facilitate the resolution of the matters raised in the complaint or application between the individual and the organisation concerned instead of immediately exercising its powers of investigation under the PDPA.

- The Commission is not empowered to award damages to a complainant. As such, facilitation and alternative dispute resolution mechanisms like mediation) to encourage the parties to discuss the issues in a complaint and find a mutually acceptable resolution, which may include compensation.

- For the avoidance of doubt, the two main objectives described in the preceding paragraphs are not intended to be mutually exclusive or to preclude the Commission from taking any action under the PDPA for other reasons. Where the Commission considers it appropriate, the Commission may commence an investigation even if the complainant and the organisation have reached an agreement that resolves the issues in the complainant's complaint. This may include situations where the facts of the case disclose issues of general public interest, or there are other individuals who may be affected by the conduct of the organisation. 1

Notes

leave it to the parties involved, whether SCT or civil court.

[1] Advisory Guidelines On Enforcement Of The Data Protection Provisions (published 21 April 2016)

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Offences Related to the PDPC's Powers of Investigation

Notes

An organisation or a person is also guilty of an offence if any of the following is committed:

- If the organisation or person with an intent to evade a request for access or correction under the Act, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy, a record containing –
  i. Personal data; or
  ii. Information about the collection, use or disclosure of personal data
- If the organisation or person obstructs the PDPC or an authorised officer in the performance of their duties or exercise of their powers under the Act;
- If the organisation or person knowingly or recklessly makes a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC, in the course of the performance of its duties or powers under the Act; and
- If a person makes a request for access or correction under the Act to obtain access to or to change the personal data of another individual without that individual's authority.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Enforcement of the Data Protection Provisions

If the PDPC finds that an organisation is in breach of any of the data protection provisions in the PDPA, it may give the organisation such directions that it thinks appropriate to ensure compliance. These directions may include requiring the organisation to:

- Stop collecting, using or disclosing personal data in contravention of the Act;
- Destroy personal data collected in contravention of the Act;
- Provide access to or correct the personal data; and/or
- Pay a financial penalty of an amount not exceeding $1 million. (Per offence)

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Data Protection Enforcement Cases

Notes

Organisation: 'K Box' Entertainment Group Pte Ltd

In September 2014, a list containing the personal data of 317,000 'K Box' staff members was found to have been leaked and uploaded on http://pastebin.com, a website which allows members of the public to post and share text online publicly. The data included names, contact numbers and residential addresses. Members of the public who noticed the leak lodged complaints with the PDPC.

'K Box' did not ensure that its IT system security was sufficiently robust as security patches were not updated. This allowed external parties to install malware to gain easy access into the system.

There was also no DPO to develop and implement data protection policies, resulting in weak control of access to personal data. For example, unused accounts were not disabled and account-holders used weak passwords consisting of only a single character.

Decision: Breach of section 24 of the PDPA for failing to implement proper and adequate protective measures, resulting in unauthorised disclosure of a large number of personal data.

Additionally, the lack of adequate data protection policies, including the absence of a DPO, was considered and it was found that sections 11(3) and 12(a) were also breached.

Actions Taken: Financial penalty of $50,000 was imposed and other directions issued.

Source : https://www.pdpc.gov.sg/news/press-room/page/0/year/All/pdpc-takes-action-against-11-organisations-for-breaching-data-protection-obligations

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Data Protection Enforcement Cases

Notes

Organisation: Universal Travel Corporation (UTC)

In March 2015, PDPC received a complaint on wrongful disclosure of personal data by Universal Travel Corporation.

Four of UTC's customers had requested for information to facilitate their insurance claims relating to changes in flight timings during a particular tour organised by Universal Travel Corporation.

As there was no clear data protection policy in place, a UTC staff proceeded to share a document that contained the personal data of all 37 customers who had signed up for the same tour without redacting the personal data, such as the name, 'nationality, date of birth, passport number and passport expiry date, of the other customers.

Decision: Breach of section 13 for disclosure of personal data without consent. Additionally, the lack of data protection policies was considered and it was found that section 12(a) was also breached.

Actions Taken: Directions issued for UTC to inform individuals who had received the passenger list not to disclose the list to other third parties; put in place a data protection policy to comply with the PDPA; and to send UTC employees for training on the obligations of the PDPA.

Source : https://www.pdpc.gov.sg/news/press-room/page/0/year/All/pdpc-takes-action-against-11-organisations-for-breaching-data-protection-obligations

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Data Protection Enforcement Cases

Notes

Organisation: Xirlynx Innovations

IT vendor Xirlynx Innovations was engaged by Challenger Technologies Limited to manage its email communications, among others. Its employee had used an erroneous excel database to send out email updates without conducting checks to ensure that the emails were sent to the correct recipients.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised disclosure of Challenger Technologies Limited members' personal data while sending out email communications.

Actions Taken: Warning issued

Source : https://www.pdpc.gov.sg/news/press-room/page/0/year/All/pdpc-takes-action-against-11-organisations-for-breaching-data-protection-obligations

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Enforcement of the Do Not Call Registry Provisions

Notes

The aim of the DNC Registry is to reduce the number of unwanted telemarketing calls, marketing text messages and faxes. Registering your number on the registry does not stop non-telemarketing calls, text messages and faxes and some types of telemarketing calls, text messages and faxes, which may include:

- Calls, text messages and faxes from businesses to which you have given your consent to receive telemarketing calls, text messages and/or faxes;
- Calls, text messages and faxes solely to provide you with periodic updates on your account statement, to notify you of a change in the terms or features of your ongoing commercial relationship with them or otherwise, text or fax messages from organisations with whom you have an ongoing relationship, and the purpose of the text or fax message is related to the subject of the ongoing relationship;
- An individual acting in a personal or domestic capacity;
- An organisation which is delivering goods or services, including product updates or upgrades, that the recipient of the message is entitled to receive under the terms of a transaction that the recipient had previously entered into with the sender;
- An organisation which is facilitating, completing or confirming a transaction that the recipient of the message has previously agreed to enter into with the sender; and
- Public agencies promoting any programme carried out by any public agency which is not for commercial purpose.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Do Not Call Registry Enforcement Cases

Notes

Organisation: Huttons Asia Pte Ltd

In September 2014, a salesperson registered with Huttons Asia Pte Ltd was charged with making unsolicited telemarketing messages to Singapore telephone numbers that were registered with the DNC Registry. The unsolicited telemarketing messages advertised various residential property developments in Singapore.

Decision: The property salesperson faced 27 counts of contravening section 43(1) of the PDPA, relating to the obligation to check the DNC Registry before sending any telemarketing messages to Singapore telephone numbers.

Actions Taken: Financial penalty of $27,000 was imposed.

Source : https://www.pdpc.gov.sg/docs/default-source/media/media-release-for-dp-enforcement-action-(25-apr-2016)(clean).pdf?sfvrsn=0

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Do Not Call Registry Enforcement Cases

Notes

Organisation: Star Zest Home Tuition Pte Ltd

On 27 August 2014, Star Zest Home Tuition Pte. Ltd., and its director, were charged for offences relating to the DNC Registry under the PDPA. Many complaints were made on the tuition agency relating to unsolicited telemarketing messages allegedly sent by the tuition agency to Singapore telephone numbers which had been registered with the DNC Registry. The unsolicited messages offered the teaching services of various tutors signed up with the tuition agency.

Decision: Both Star Zest and its director had faced a total of 26 counts of contravening section 43(1) of the PDPA with 48 other similar offences taken into consideration.

Actions Taken: Financial penalty of $39,000 was imposed on each director, for a total of $78,000.

Source : https://www.pdpc.gov.sg/docs/default-source/media/media-release-for-dp-enforcement-action-(25-apr-2016)(clean).pdf?sfvrsn=0

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

General Offences and Penalties

Notes

It is an offence under section 51(3)(b) and (c) of the PDPA to:

- obstruct or impede the PDPC, its inspectors or other authorised officers in the exercise of their powers or performance of their duties under the PDPA; or
- knowingly or recklessly make a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC, in the course of the performance of the duties or powers of the PDPC under the PDPA.

An organisation or person that commits an offence under section 51(3)(b) or (c) of the PDPA is liable to:

- in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and
- in any other case, to a fine not exceeding $100,000.

DNC Registry Penalties

Any organisation that breaches the DNC provisions in the PDPA is liable to a fine of up to $10,000 per offence. In appropriate cases, the PDPC may compound the offence for a sum of up to $1,000. Whether composition is offered and the amount of composition will be decided by the PDPC based on the facts of each case.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Alternative Dispute Resolution

Notes

Commission's powers relating to alternative dispute resolution

1. If the Commission is of the opinion that any complaint by an individual against an organisation may be more appropriately resolved by mediation, the Commission may, with the consent of the complainant and the organisation, refer the matter for mediation.

2. The Commission may direct a complainant or an organisation or both to attempt to resolve the complaint of the individual in the way directed by the Commission.

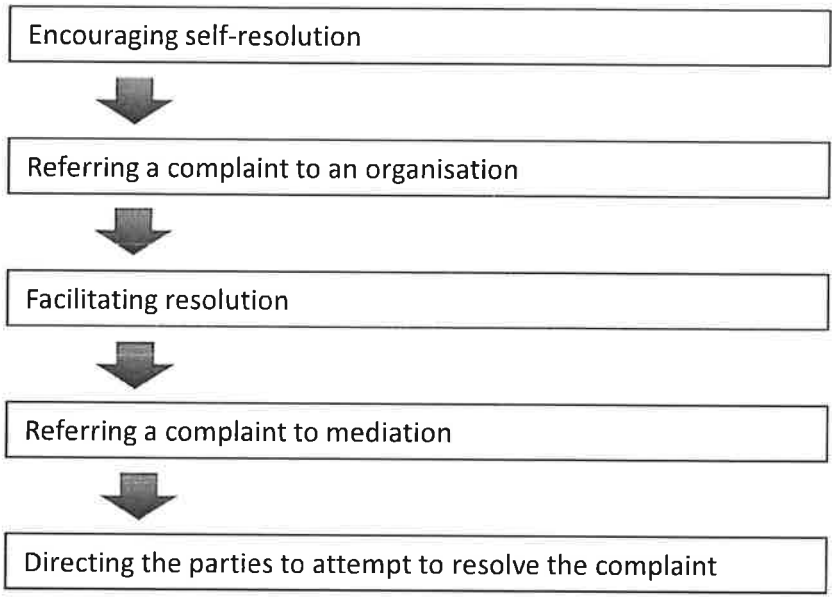
3. It should be noted that the Commission's powers in relation to alternative dispute resolution do not include deciding on disputes between a complainant and an organisation or ordering an organisation to compensate a complainant who suffers a loss as a result of a contravention of any of the Data Protection Provisions by the organisation.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Measures to facilitate resolution of a complaint

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

2.15 ENFORCEMENT

Mediation as an Alternative

- Mediation can be a faster and less costly way of resolving disputes, and takes place outside of the PDPC's investigation process and the court process.
- When individuals and organisations have disputes, they may choose to solve their issues through mediation. When the individual and organisation meet at the mediation table, it could lead to a better understanding of each side's interests and areas of disagreement.
- Both individuals and organisations may also independently approach mediation bodies, such as Consumers Association of Singapore (CASE) or the Singapore Mediation Centre (SMC), regarding their mediation services without first coming to the PDPC.

CASE

Singapore Mediation Centre

smc

Notes

Passive instead of active. Only react on complaints.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 3: ROLE OF DATA PROTECTION OFFICER (DPO)

At the end of this chapter, participants will be able to acquire knowledge for "the Role of a Data Protection Officer".

- *Appointment of DPO*
- *Functions of a DPO*
- *Governance Structures*

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

3.1 APPOINTMENT OF DPO

Under the Openness Obligation, an organisation is required to:

- Develop and implement its data protection policies and practices;
- Develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;
- Communicate to its staff information about its data protection policies and practices; and
- Make information available on request about its data protection policies and practices and its process to receive and respond to complaints.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.2 Functions of a DPO

Generally, a DPO is responsible for ensuring an organisation's compliance with the PDPA in respect of the personal data in the organisation's possession or under organisation's control. The role of the DPO may accordingly include:

- Understanding organisation's personal data inventory and reviewing the data management framework and processes to align them with the PDPA. For example, determining how, when and where organisation collects the data, the purpose of data collection and ensuring that consent is obtained for the use and disclosure of the personal data collected;
- Assessing organisations' policies, procedures and contracts (e.g. research processes, data management policies, service contracts, etc)
- Developing policies for handling personal data in electronic or non electronic forms, communicating internal personal data policies to customers and handling any queries or complaints about personal data;
- Inform all employees of the organisation's data protection policies and their role in safeguarding personal data;
- Ensure the employees know what the internal processes are with regard to protecting personal data;
- Conduct regular internal audits to ensure that the organisation's processes adhere to the PDPA; and
- Assess and alert the organisation of any risk of a data breach or other breaches of the PDPA and to liaise with the PDPC for investigations on breaches, if necessary.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.3 GOVERNANCE STRUCTURES

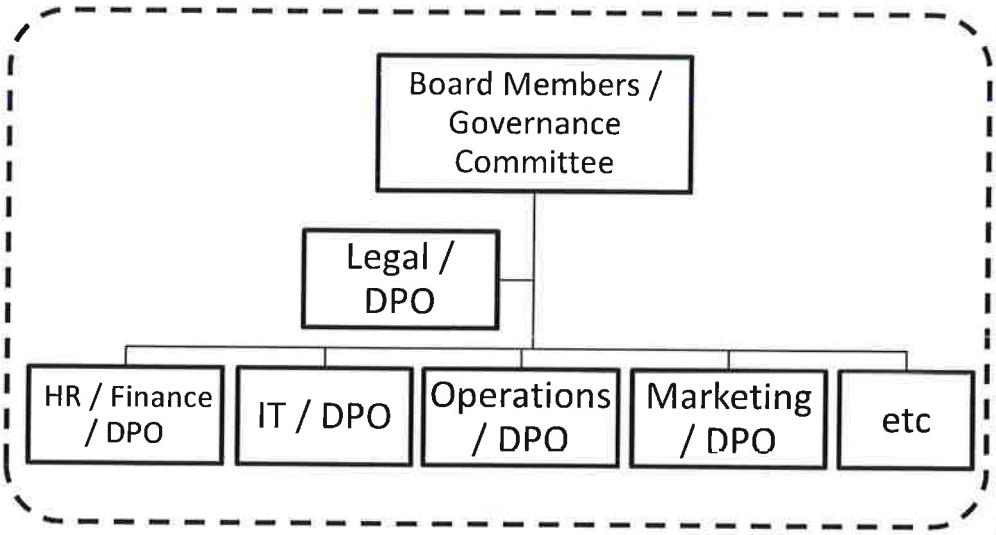
- It is important to establish a proper governance structure for data protection matters so that there is clarity as to various roles and responsibility of each officer identified within the organisation, as well as, to set out the rules for flow of information and for making decisions on data protection matters.
- While the Openness Obligation requires each organisation to designate at least one individual to be responsible for ensuring its compliance with the PDPA, it does not prescribe who this individual may be or how an organisation should be set up as part of its internal governance.
- Each organisation may wish to adopt the best structure or approach to meet its internal business needs. The examples that we will be showing are illustrative and do not provide a comprehensive list of approaches that may be adopted by an organisation.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.3 GOVERNANCE STRUCTURES

Example 1: In-sourcing Model - Appointment of DPO/s Within the Organisation Structure

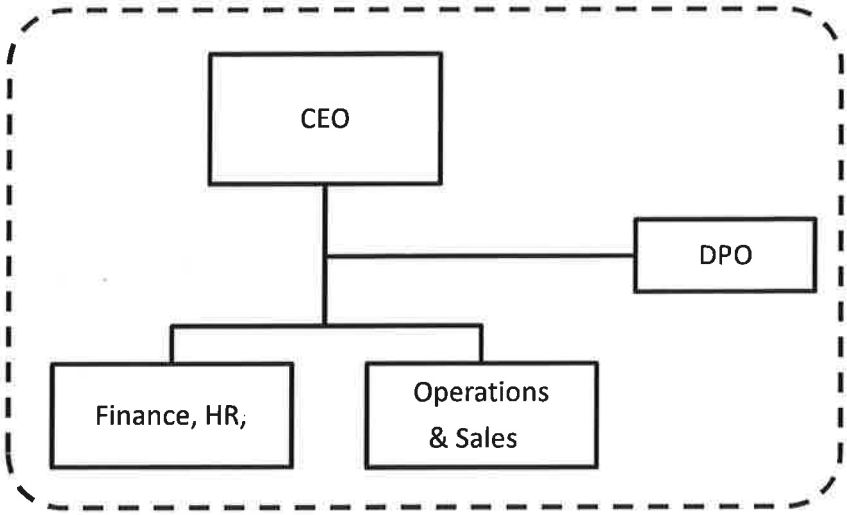


Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.3 GOVERNANCE STRUCTURES

Example 2: Out-sourcing Model - Appointment of Individual/s Outside of the Organisation as DPO/s

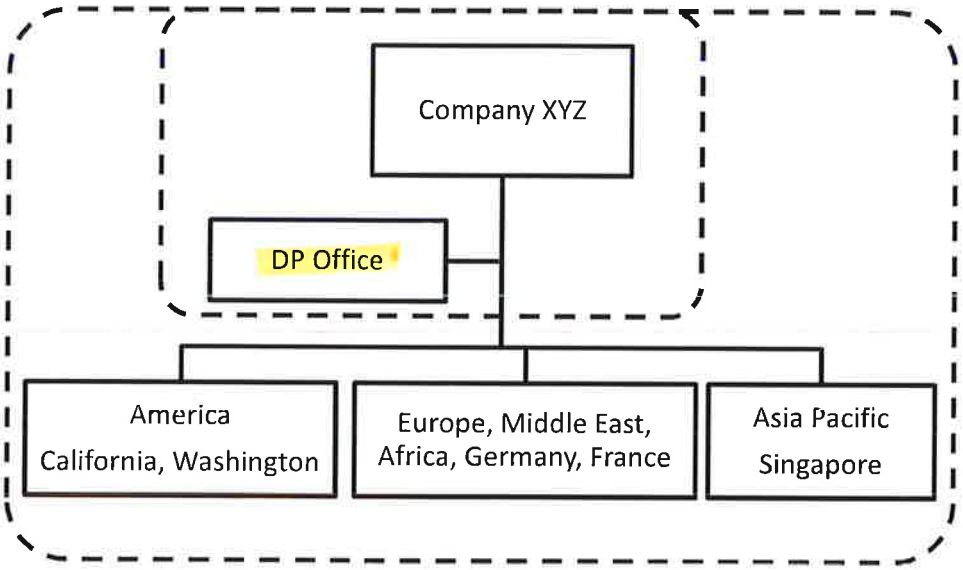


Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.3 GOVERNANCE STRUCTURES

Example 3: Centralised Model - Centralising DPO functions at the HQ within a Group of Companies – Establishing a Common DP Policy to be Adopted by All



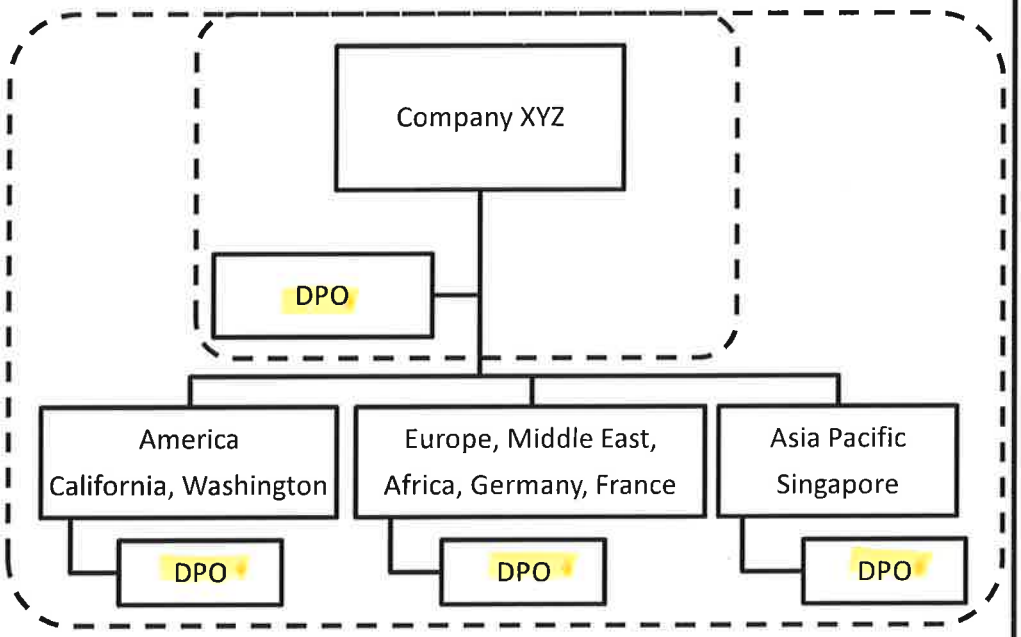
Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

3.3 GOVERNANCE STRUCTURES

Example 4: Decentralised Model - Decentralising DPO Functions to be Managed Individually by Each Company within a Corporate Group – Policy within Each Company may be Customised

Notes



Different regulatory framework.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Learning Activity 1 – Role of Data Protection Officer

Instructions

Using the template provided in the next page, discuss as a group on how a DPO can perform the following within their organisation:

- Setting up policies and processes for compliance with the PDPA
- Assess organisations' policies, procedures and contracts
- Identify and document possible areas of non-compliance
- Auditing for compliance

- Group discussion – 20 minutes
- Key sharing by nominated member of each group – 10 minutes
- Debrief by facilitator – 10 minutes

Note: The group can decide the industry or the company they wish to discuss on

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Learning Activity 1 – Role of Data Protection Officer

Setting up policies and processes for compliance with the PDPA

To consider the following:

PDPA Obligations in relation to the business activity/ies

① Based on collection, use & disclosure
- Set out how consent may be obtained & recorded
- Set up a process to allow an individual to withdraw consent.

② Based on access & correction
- Establish a clear practice for assessing & processing both access & correction requests.

③ Based on care for personal data (Protection & Retention)
- set out how PD in custody may be well-protected
- Classify the PD to better manage housekeeping.
- Make avail info on how customers may request to access/correct their PD with org.

Assess organisations' policies, procedures and contracts

(list the various policies, procedures and contracts that needs to be reviewed)

① Codes of conduct
② Data collection Policies and/or Procedures
③ Data / Document Retention Policies
④ Privacy Policies
⑤ Procedures for updating records
⑥ Sales Contracts
⑦ Refunds Policies and/or Procedures

Identify and document possible areas of non-compliance in their organisations' current activities.

Sources of info =
① Quality Assurance Dept
② SOP process owners
③ Company website
④ Document control dept

Auditing for compliance

(i.e. how, when and what do you check to ensure compliance)

① Internal communications & training to staff on company's policies & procedures in relation to the PDPA.
② Conduct periodic audits using PDPC's organisational / biz checklist.
③ Facilitate cross-disciplinary involvement from IT, legal, audit & core business functions to ensure compliance.
④ Recommend relevant employees to undergo the 2-day PDPA WSQ course.
⑤ Understand + adhere to org. policy on non-compliance/non-adherence.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 4:
CREATE AN ORGANISATION'S DATA INVENTORY MAP (DIM) AND IDENTIFY AREAS OF NON-COMPLIANCE

At the end of this chapter, participants will be able to acquire knowledge and skills to "create an organisation data inventory map and identify possible areas of non-compliance".

- *What is a DIM and How to Create One for the Organisation*
- *Example of a DIM*

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

4.1 WHAT IS A DATA INVENTORY MAP AND HOW TO CREATE ONE FOR THE ORGANISATION

What is a Data Inventory Map (DIM)?

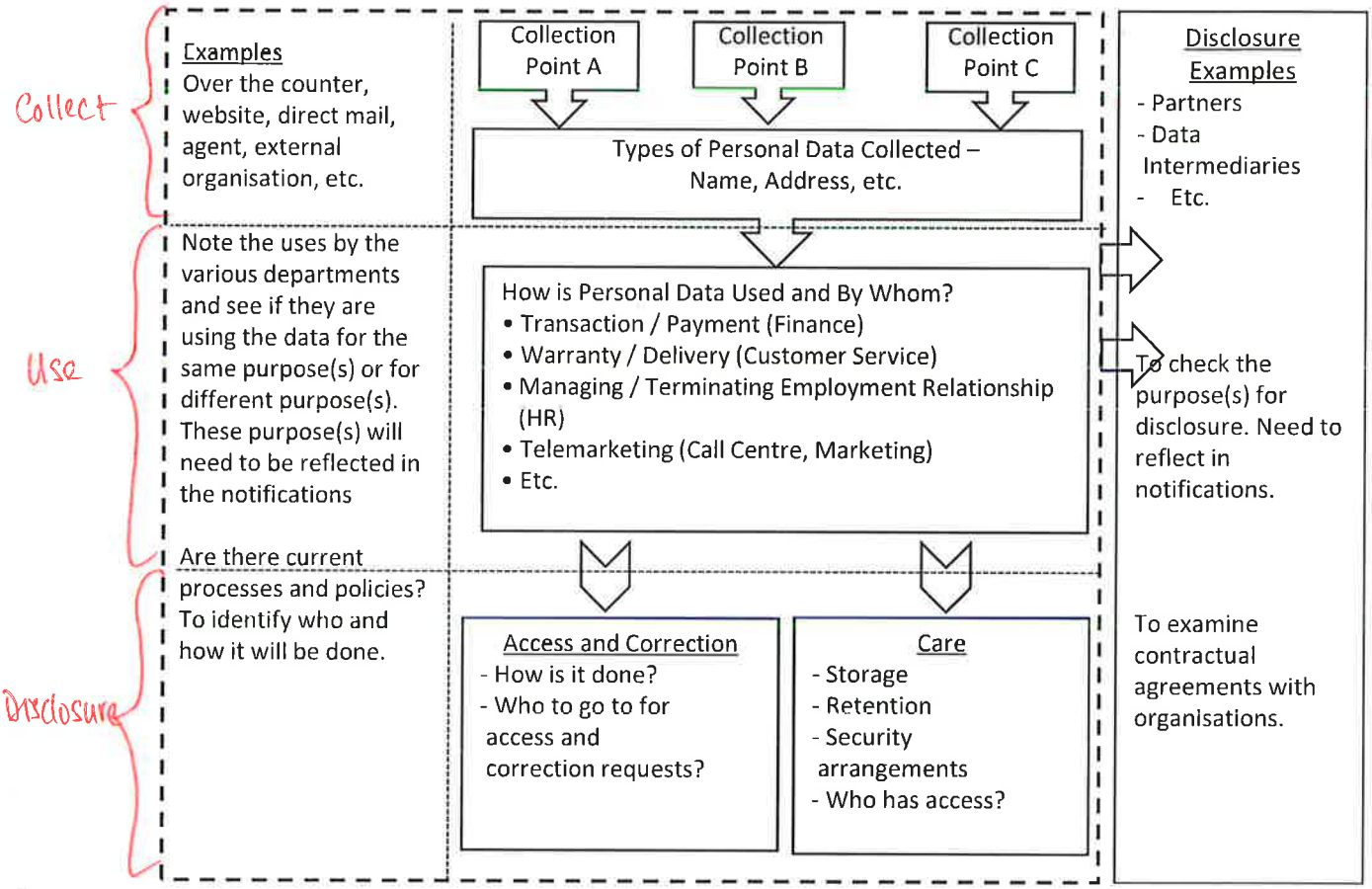
The DIM is an inventory of the personal data in the possession or under the control of an organisation.

Information that it contains could include the types of personal data collected and how the personal data is being collected, used, accessed, corrected, cared, transferred and shared with other organisations etc.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

4.2 EXAMPLE OF A DATA INVENTORY MAP



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

4.2 EXAMPLE OF A DATA INVENTORY MAP

DIM of a Retail Shop – Example

Data Activities	Current Processes
Collection - What? - Where? - Who?	Purchase information, financial information Point-of-Purchase (POP) Cashiers
Use - How? - Who?	For payment of goods/services. For accounting purposes by store managers and accounts department.
Care of Data - Where is it stored? - Is it secured	Credit card chits are kept in cashier's drawer that is locked and accessible only be selected staff. Information in POP system is encrypted and requires password for access.
Disclosure - To whom?	Information is disclosed to credit card companies for verification purposes. Information will be disclosed to outsourced audit company for annual audit.
Retention - Where? - How long?	Daily records are sent back to main office and filed for audit purposes. Records will be kept for X years before they are destroyed.
Telemarketing - Who to call? - How often?	Outsourced Call Centre. Monthly SMS sent out to list of telephone numbers of customers.

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 5:
DEVELOP A PROCESS FOR DISPUTE RESOLUTION
(Compliant Handling)

At the end of this chapter, participants will be able to acquire knowledge and skills for "developing a process for dispute resolution " in an organisation.

- *Typical Complaint Handling Process*
- *What to Consider When Developing Process for Handling Complaints Relating to Data Protection*
- *Example of Complaint Handling Process Relating to Data Protection*

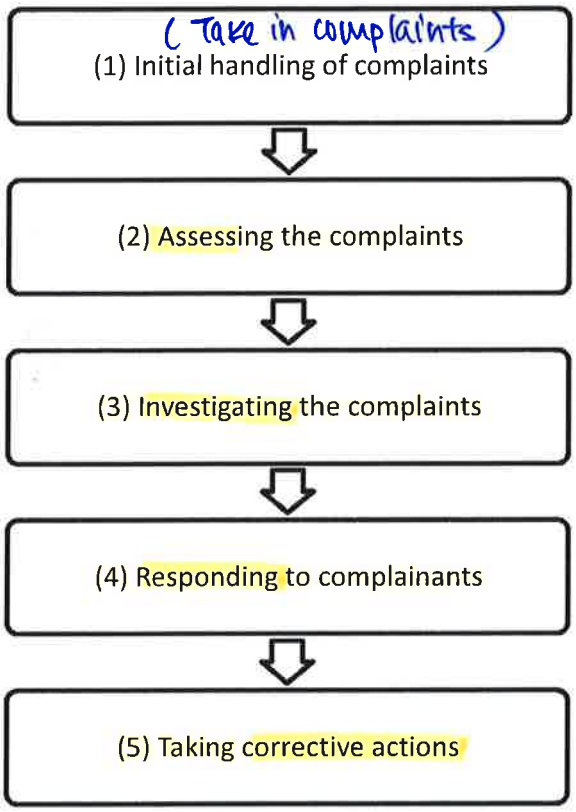
FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

5.1 TYPICAL COMPLAINT HANDLING PROCESS

Objective: To ensure fast and appropriate handling of complaints by customers, so that the result is satisfactory or acceptable to all parties.

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.2 WHAT TO CONSIDER WHEN DEVELOPING PROCESS FOR HANDLING COMPLAINTS RELATING TO DATA PROTECTION

Notes

(1) Initial handling of complaints

- Mode and tracking of complaints: What modes of complaints does your organisation intend to handle and how your organisation intend to keep track of data protection related complaints?
- Information required: What kind of information does your organisation need to collect with regard to the complaint?
- Turnaround time: What is the expected turnaround time to acknowledge receipt of compliant?
- Management attention: Who shoud be kept informed of all data protection related complaints and how often?

Assessing the complaints

Investigating the complaints

Responding to complainants

Taking corrective actions

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.2 WHAT TO CONSIDER WHEN DEVELOPING PROCESS FOR HANDLING COMPLAINTS RELATING TO DATA PROTECTION

Notes

Initial handling of complaints

(2) Assessing the complaints

- Resourcing: Does your organisation need to form a pool of staff to carry out investigation work and if so, how large should this pool be?
- Assessment: Assess the validity and severity of complaint and the priority to be accorded to the investigation.
- Turnaround time: Assess the timeframe needed to achieve closure for the complaint and inform complainant accordingly.
- Management attention: What is the appropriate management level to be escalated to?

Investigating the complaints

Responding to complainants

Taking corrective actions

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.2 WHAT TO CONSIDER WHEN DEVELOPING PROCESS FOR HANDLING COMPLAINTS RELATING TO DATA PROTECTION

Initial handling of complaints

Assessing the complaints

(3) Investigating the complaints

- Investigation process: What is your organisation's process to carry out the investigation?
- Engaging complainant: How does your organisation intend to keep the complainant informed on the status of the complaint?
- Remedial actions: What are the different types of remedial actions your organisation could take?
  - Corrective actions
  - Improvement actions
  - Preventive actions
- Management attention: What level of management should the investigation report be sent to? DPO should be informed.
- Informing authorities: Under what circumstances should this compliant be reported to the authorities?

Whenever there's a breach, esp. industry wide, DPO needs to escalate to the PDPC.

(4) Responding to complainants

- Engaging complainant: How does your organisation intend to share the result of the investigation and the proposed remedial action(s) with the complainant? Consider mediation (refer to page 163)
- Closure of case: How to close the case once complainant agree with the remedial action and how to gather feedback from complainant?
- Escalation process: What level of escalation is required should complainant disagree with the proposed remedial action(s)?

(Appeal)

Taking corrective actions

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.2 WHAT TO CONSIDER WHEN DEVELOPING PROCESS FOR HANDLING COMPLAINTS RELATING TO DATA PROTECTION

Responding to complainants

Notes

Mediation

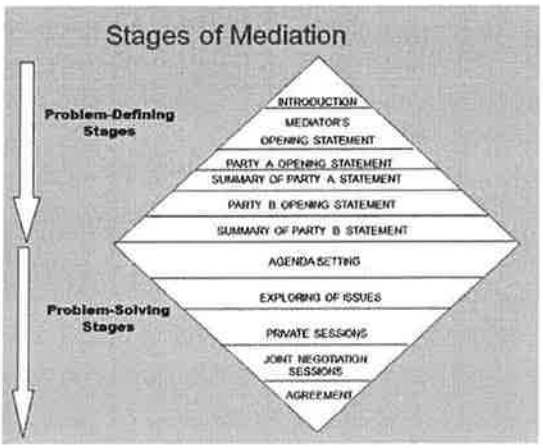
When resolving a dispute, organisations could adopt mediation process between them and complainant as a first step.

Mediation Process:

The mediation process will involve the parties, their representatives and/or advisors (if any) and the Mediator(s). The mediation will be conducted in confidence, and all communications will be on a 'without prejudice' basis.

The mediation will be conducted in confidence, and no transcript or formal record will be made of the proceedings. Only the mediator, the parties and/or their authorised representatives and advisers will be permitted to be present during the mediation. There the process is flexible, a mediation will generally include the following stages:

- The mediator will begin with an opening statement to introduce the parties to the process.
- The parties will then be invited to share their concerns.
- The next step in the process will be to draw up a list of all relevant issues to be discussed.
- The mediator will then lead and encourage the parties to consider each issue in turn. At some point in time, the mediator may request to see the parties privately. They may subsequently be brought together again for further joint discussions.
- Where a settlement is reached in the mediation, the terms of the settlement will usually be recorded in writing and signed by or on behalf of the parties.



Source: Singapore Mediation Centre (SMC)
http://www.mediation.com.sg/about-us/#approach-to-mediation

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.2 WHAT TO CONSIDER WHEN DEVELOPING PROCESS FOR HANDLING COMPLAINTS RELATING TO DATA PROTECTION

Initial handling of complaints

Assessing the complaints

Investigating the complaints

Responding to complainants

(5) Taking corrective actions

Observe trends (repeated complaints)

- Identify systemic issues: What kind of mechanisms does your organisation intend to put in place to analyse current and past complaints to identify systemic issues?
- Finetune data protection policies and processes: What kind of mechanisms does your organisation intend to put in place process to finetune current data protection policies and processes, so as to prevent recurrences of such complaints in future?

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.3 EXAMPLE OF COMPLAINT HANDLING PROCESS RELATING TO DATA PROTECTION

Stages of complaint process	Steps that my organisation could take	Turnaround time	Person-in-charge
(1) Initial handling of complaints	<u>Preparatory work</u> • Make the complaint handling process readily available to the public • Develop and maintain a data protection complaint register to keep track of the status of the complaints		DPO
	<u>Upon receipt of complaint</u> • Send acknowledgement reply to complainant • Record complaint into register • Inform Chief DPO of all DP-related complaints	Within the day that the complaint is filed	DPO
(2) Assessing the complaints	• Assign an investigation officer to follow up on the complaint • Assess the validity of the complaint. • If valid, determine which of the Data Protection or Do Not Call provisions has the organisation not complied with and assess the impact and severity of the complaint • Escalate to the appropriate level of management based on the escalation level defined	1 day after the complaint is filed X days after investigation officer is assigned	DPO Investigation officer Investigation officer

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.3 EXAMPLE OF COMPLAINT HANDLING PROCESS RELATING TO DATA PROTECTION

Stages of complaint process	Steps that my organisation could take	Turnaround time	Person-in-charge
	• Assess the timeframe needed to achieve closure for the complaint and inform complainant accordingly	X days after investigation officer is assigned	
(3) Investigating the complaints Progression control	• Determine what caused the non-compliance to take place, who were involved and how and why it happened • Provide interim updates to the complainant and find out from the complainant how he/she might want his/her complaint to be resolved • Submit investigation report to appropriate level of management, including (1) findings made; (2) recommendations on the remedial actions to be taken to achieve resolution of the complaint • If need be, report to/inform the relevant authorities such as police and PDPC	Average turnaround time is based on estimates by investigation officer Average turnaround time is based on estimates by investigation officer	Investigation officer Investigation officer
(4) Responding to complaints	• Inform complainant about the results of the investigation and the remedial actions to be taken • If complainant disagrees with the remedial actions, this could be escalated to the CEO or independent third party for resolution	X days after the report has been approved	DPO and investigation officer

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

5.3 EXAMPLE OF COMPLAINT HANDLING PROCESS RELATING TO DATA PROTECTION

Stages of complaint process	Steps that my organisation could take	Turnaround time	Person-in-charge
(5) Taking corrective actions	• Analyse current and past complaints to determine if there are systemic issues that might cause such complaints to be lodged in the first place. • Once these systemic issues are identified, recommend specific actions such as fine-tuning of specific data protection policies and processes, staff training, etc. to prevent future recurrences.	X weeks after closure of complaint	DPO

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Learning Activity 2 – Process for Dispute Resolution

Instructions

Group discussion: Based on the complaints handling process that you have developed for your organisation, share with the group on one of the processes that developed within the group. Nominate a member from your group to share with the class.

- Group discussion – 20 minutes
- Key sharing by nominated member of each group – 10 minutes
- Debrief by facilitator – 10 minutes

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Learning Activity 2 – Process for Dispute Resolution

Notes Page



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 6:
TRAINING AND COMMUNICATIONS TO STAFF FOR COMPLIANCE TO DATA PROTECTION PROVISIONS

At the end of this chapter, participants will be able to acquire knowledge and skills for "training and communications to staff for the compliance to PDPA provisions".

- *Objectives and Outcomes of Staff Training and Communications*
- *What to Consider When Developing a Training and Communications Plan*
- *Example of a Training and Communications Plan*
- *Breach Management and Notification*

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

6.1 OBJECTIVES AND OUTCOMES OF STAFF TRAINING AND COMMUNICATIONS

Awareness

Understanding

Acceptance

Commitment

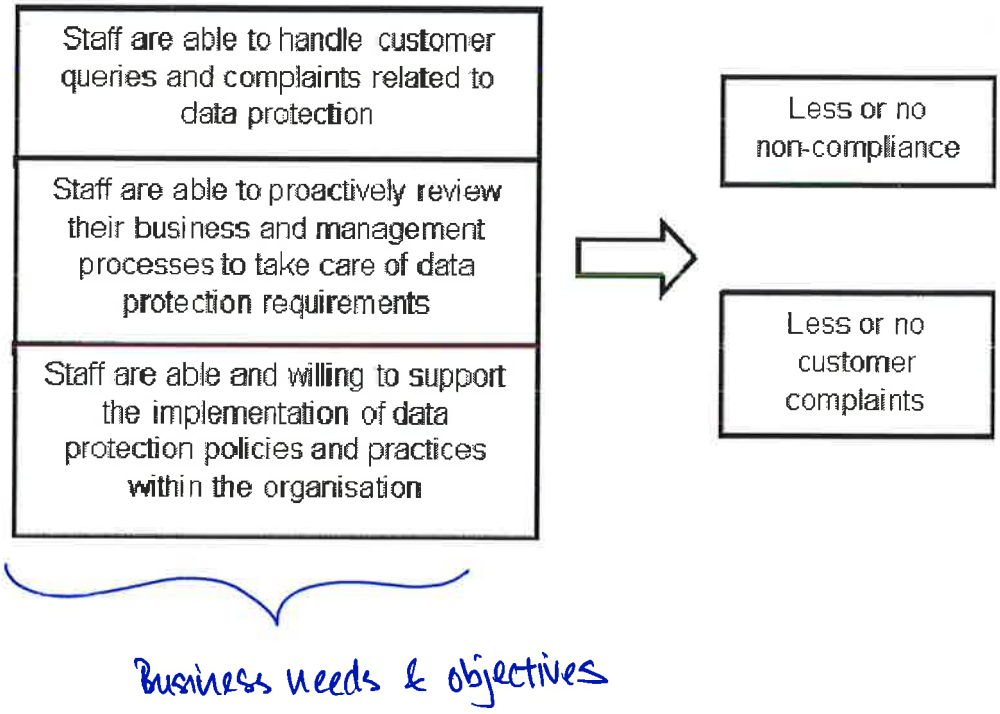
Action

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.1 OBJECTIVES AND OUTCOMES OF STAFF TRAINING AND COMMUNICATIONS

Outcomes of Staff Training and Communications

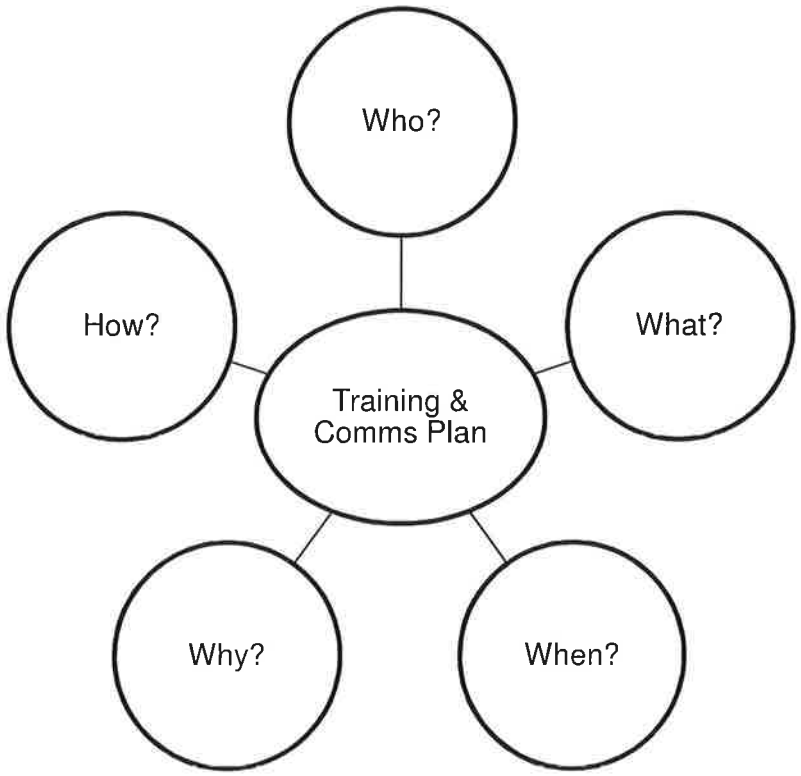
Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN

Notes



© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN



WHO

Company's staff includes:

- Sales and marketing
- Customer service
- HR and administration
- IT
- Finance and accounts
- Operation
- Management
- Etc.

Functional Groups

Notes

* Different plans for different groups

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN



WHAT

Contents could include:

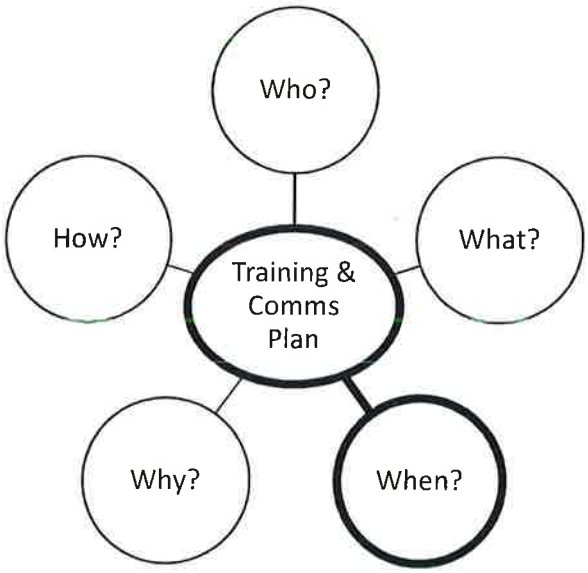
- Overview of the PDPA
- Company's data protection policies and processes, e.g.:

– Notify purpose and seek consent for the collection, use and disclosure of personal data
– Request to access and correct one's personal data
– Protection, retention and overseas transfer of data

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN



WHEN

As soon as content is ready

Eg. Flow Charts

Will be guided by when the policies and processes are ready

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN



WHY

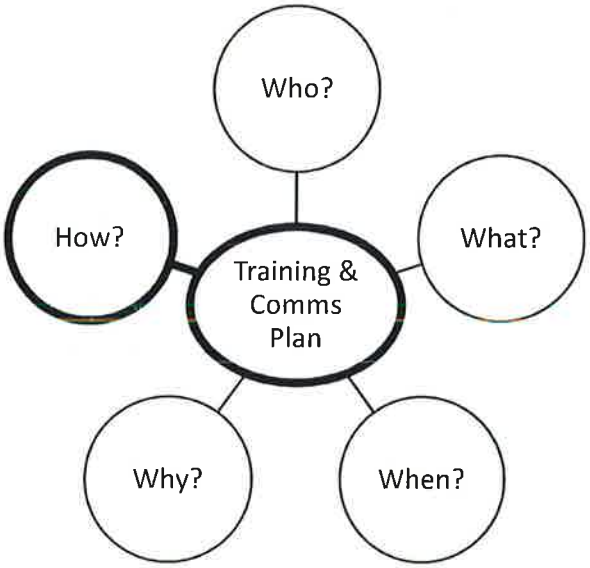
- To comply with the new regulation and legislation
- To inform the staff about the company's data protection policies and processes
- To implement the new procedures

Notes

Intranet + Company website (w DPO contact)

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.2 WHAT TO CONSIDER WHEN DEVELOPING A TRAINING AND COMMUNICATIONS PLAN



How

- Training could be done through workshops and could be done either by in-house or external trainers

- Communication channels could include:
  - Letter / Email
  - Brochure
  - Newsletter
  - Intranet
  - Briefing
  - Townhall
  - Teleconference
  - Orientation

Notes

- Videos
- Re-fresher trainings

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.3 EXAMPLE OF A TRAINING AND COMMUNICATIONS PLAN

Organised by stages of PDPA implementation, e.g.

- At the start of the organisation's PDPA journey;
- Implementation kick-off;
- Completion of the DP and DNC policies and processes;
- On-going basis;
- Develop;
- "Who", "What", "When", "Why", "How" of the organisation's training and communications plan; and
- Ascertain the desired outcomes of the training and communications intervention. (Are people more aware of PDPA ?)

Notes

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.3 EXAMPLE OF A TRAINING AND COMMUNICATIONS PLAN

STAGES of PDPA Implementation	WHO to train and communicate?	WHAT to train and communicate on?	WHEN must the training and communication take place?	WHY must they be trained or communicated on this?	HOW to train and communicate?	OUTCOMES of the training and communication effort
(1) At the start of the organisation's PDPA journey	Members of the management team.	PDPA & its implications for the organisation. Role of individual members of the management team.	At the start of the organisation PDPA compliance journey.	To inform management team of their role and seek their commitment.	Presentation.	Management commitment. Alignment to biz
(2) Implementation kick off	All staff.	Overview of PDPA, impact to the organisation, and details of the implementation plan.	Before the start of implementation.	To inform staff of the impact of PDPA to their organisation and to get their commitment to contribute to the implementation.	Mass briefing or email.	Staff are able and willing to support the implementation of DP policies and practices within the organisation.
(3) Completion of the policies and processes for each of the stages below: a)Data collection b)Data access and correction c)Data accuracy d)Data protection and retention e)Data transfer f) DNC g) Complaint handling	Depends on organisation business and structure but it should include staff handle personal data, e.g.: - Sales & Marketing; - HR; - Admin; - Customer Service; and -Operations Cover in stages or by location (eg. NTUC outlets)	Organisation's data protection policies and processes with regards to data collection, use and disclosure, access & correction, accuracy, protection & retention and data transfer. The roles your staffs play in complying with the policies and processes. Use of IT systems that are implemented in support of the data protection policies and processes.	Before the data protection policies and processes are to be implemented. During orientation for new staff.	To fulfil the various obligations of the PDPA, namely: a) Consent, Purpose & Notification; b) Access & Correction; c) Accuracy; d) Protection & Retention; e) Transfer Limitation; f) DNC; and g) Openness.	Conduct briefings & trainings on: a) Policies and processes; b) Usage of IT systems, where applicable; and c) Access to knowledge repository containing the data protection policies and processes.	Staff are able to handle customer queries and complaints related to data protection. Staff are able to proactively review their business and management processes to take care of data protection requirements. Staff are able and willing to support the implementation of DP policies and practices within the organisation.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.3 EXAMPLE OF A TRAINING AND COMMUNICATIONS PLAN

STAGES of PDPA Implementation	WHO to train and communicate?	WHAT to train and communicate on?	WHEN must the training and communication take place?	WHY must they be trained or communicated on this?	HOW to train and communicate?	OUTCOMES of the training and communication effort
(4) On-going basis	All staff.	Updates in data protection policies and processes. Organisation's non-compliance case studies. Best practices.	As and when there are updates or on a regular, e.g.: quarterly or half-yearly bases. Depends on how frequent they are in contact with personal data. At least once a year.	To ensure on-going compliance to PDPA.	Briefings.	Staff are able to handle customer queries and complaints related to data protection. Staff are able and willing to support the implementation of DP policies and practices within the organisation.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

6.3 EXAMPLE OF A TRAINING AND COMMUNICATIONS PLAN

PDPC's E-LEARNING PROGRAMME ON ESSENTIALS OF THE PDPA

Notes

The e-Learning programme comprises 5 modules that cover basics one will need to know about the key terms and organisations' obligations under the PDPA, and offer ways in which data protection officers can develop good data protection policies and practices.

There is also an assessment module to allow users to apply their knowledge of the PDPA gained from the 5 modules.

Organisations keen to evaluate their employees' understanding of the PDPA may request for a free PDPC E-learning Corporate Account to access the scores of their employees.

Corporate Account holders will be assigned an organisation code, to be entered by employees taking the Assessment Module.

Interested organisations may download and fill up the form from PDPC's website and email it to outreach@pdpc.gov.sg.



Visit the website : https://www.pdpc.gov.sg/resources/e-learning-programme

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Learning Activity 3 – Communications Plan and Management Report Writing

Instructions

Based on the case provided below, using the templates provided, discuss in your groups and complete the following:

1. Communications Plan for the company
2. Management Report for your management to inform them on the need for compliance with PDPA.

Tat Best Helpers Pte Ltd is a maid agency that provides employment services. This company is made up of 5 units (i.e. Sales and marketing, operations, finance, human resources and customer service) and has about 35 staff which is situated at 4 different locations of the island. The company has recently commissioned your team to develop a plan to communicate its PDPA journey.

Template 1: Communications Plan

STAGES of PDPA Implementation	WHO to train and communicate?	WHAT to train and communicate on?	WHEN must the training and communication take place?	WHY must they be trained or communicated on this?	HOW to train and communicate?	OUTCOMES of the training and communication effort
1. At the start of the organisation's PDPA journey; 1. Implementation kick-off; 2. Completion of the DP and DNC policies and processes; 3. On-going basis;						

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Learning Activity 3 – Communications Plan and Management Report Writing

Template 2: Management Report

Short brief (Introduction) on what the organisation's obligations are in terms of the collection, use and disclosure of personal data.
Highlight current gaps and/or potential contraventions of the PDPA under its current policies and processes.
Propose course of action to close the gaps and/or to mitigate the potential contraventions (e.g. timeline, people involved, activities, ensuring that a DPO is appointed, communications and training to employees, etc)
Highlight the available resources which the organisation can draw on.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CHAPTER 7:
MANAGING DATA BREACHES

At the end of this chapter, participants will be able to acquire knowledge and skills for "Managing Data Breaches".

- *What is a Data Breach and How Data Breach Could Occur*
- *Responding to a Data Breach*

For more information on the Managing Data Breaches, please refer to Guide to Managing Data Breaches (published on 8 May 2015)

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT

© Copyright 2016
PERSONAL DATA PROTECTION COMMISSION

7.1 WHAT IS A DATA BREACH AND HOW DATA BREACHES COULD OCCUR?

What is a Data Breach?

A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and personal data.

Data breaches are generally recognised as one of the more costly security failures of organisations. They could lead to financial losses, and cause consumers to lose trust in an organisation.

How Data Breaches Could Occur?

Data breaches can occur for different reasons. They may be caused by employees, parties external to the organisation or computer system errors. Possible ways in which a data breach may occur are:

Malicious Activities Eg. KBox	• Hacking incidents / Illegal access to databases containing personal data • Theft of computer notebooks, data storage devices or paper records containing personal data • Scams that trick organisations into releasing personal data of individuals (Eg. Update particulars of paypal a/c)
Human Error	• Loss of computer notebooks, data storage devices or paper records containing personal data • Sending personal data to a wrong e-mail or physical address, or disclosing data to a wrong recipient • Unauthorised access or disclosure of personal data by employees • Improper disposal of personal data (e.g. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted)
Computer System Error	• Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

Notes

Loss of reputation, credibility & confidence of customers.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

CARE

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

7.2 RESPONDING TO A DATA BREACH

A) Data Breach Management Plan

Notes

Organisations should develop and implement a data breach management and response plan to manage data breaches. The plan may include the following sets of activities:

Containing the Breach
Assessing Risks and Impact
Reporting the Incident
Evaluating the Response & Recovery to Prevent Future Breaches

An organisation's data breach management and response plan may also include:

- **Details of the data breach management team**, with a clear command and reporting structure of key employees who would take charge and make time-critical decisions on steps to be taken to contain the breach and manage the incident.
- **Circumstances under which the data breach management team would be alerted of any data breach**. Information should also include the contact details of the management team and when the team would be activated to manage a data breach situation.
- **Possible data breach scenarios and how to respond to them.**

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

7.2 RESPONDING TO A DATA BREACH

B) Containing the Breach

Notes

An organisation should act as soon as it is aware of a data breach. It should consider the following measures, where applicable:

Shut down the compromised system that led to the data breach.

Put a stop to practices that led to the data breach.
(e.g. shredding paper documents containing personal data instead of throwing into the garbage bin.)

Establish whether steps can be taken to recover lost data and limit any damage caused by the breach.
(e.g. remotely disabling a lost notebook containing personal data of individuals.)

Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

Prevent further unauthorised access to the system. Reset passwords if accounts and passwords have been compromised.

Address lapses in processes that led to the data breach.

Notify the police if criminal activity is suspected and preserve evidence for investigation.
(e.g. hacking, theft or unauthorised system access by an employee.)

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

7.2 RESPONDING TO A DATA BREACH

C) Assessing Risks and Impact

Knowing the risks and impact of data breaches will help organisations determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected. Here are some considerations:

i) Risk and Impact on Individuals

- How many people were affected? - A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
- Whose personal data had been breached? - Does the personal data belong to employees, customers or minors? Different people will face varying levels of risk as a result of a loss of personal data.
- What types of personal data were involved? - This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimise the impact of a data breach? - E.g. a lost device protected by a strong password or encryption could reduce the impact of a data breach.

ii) Risk and Impact on Organisations

- What caused the data breach? - Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help organisations identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- When and how often did the breach occur? - Examining this will help organisations better understand the nature of the breach (e.g. malicious or accidental).
- Who might gain access to the compromised personal data? - This will ascertain how the compromised data could be used. In particular notification to affected individuals would be required if personal data is acquired by an unauthorised person.
- Will compromised data affect transactions with any other third parties? - Determining this will help identify if other organisations need to be notified.

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

Notes

likelihood & Impact

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

7.2 RESPONDING TO A DATA BREACH

R

D) Reporting the Incident

Who to Notify	• Notify individuals whose personal data have been compromised. This includes guardians or parents of young children whose personal data have been compromised. • Notify other third parties such as banks, credit card companies or the police, where relevant. • Notify PDPC especially if a data breach involves sensitive personal data.
When to Notify	• Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data. • Notify affected individuals when the data breach is resolved.
How to Notify	• Adopt the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, e-mails, telephone calls, faxes and letters). • Notifications should be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves.
What to Notify	• How and when the data breach occurred, types of personal data involved in the data breach. • What the organisation has done or will be doing in response to the risks brought about by the data breach. • Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused. • Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites).

Notes

Do a broadcast if do not know the affected individuals.

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

7.2 RESPONDING TO A DATA BREACH

Reporting the Incident to PDPC

- Organisations are advised to notify PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.
- Details of data breaches can be sent to the PDPC at info@pdpc.gov.sg with the e-mail subject "[Data Breach Notification]". For urgent notification of major cases, organisations may also contact the Commission at +65 6377 3131.
- The notification should include the following information, where available:
    - Extent of the data breach
    - Type and volume of personal data involved
    - Cause or suspected cause of the breach
    - Whether the breach has been rectified
    - Measures and processes that the organisation had put in place at the time of the breach
    - Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so
    - Contact details of persons whom the PDPC could liaise with for further information or clarification
- Where specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the incident.
- Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect PDPC's decision on whether an organisation has reasonably protected the personal data under its control or possession.

Notes

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

7.2 RESPONDING TO A DATA BREACH

E

E) Evaluating the Response and Recovery to Prevent Future Breaches

Notes

After steps have been taken to resolve the data breach, organisations should review the cause of the breach and evaluate if existing protection and prevention measures are sufficient to prevent similar breaches from occurring. Organisations may wish to consider the following areas:

Operational and Policy Related Issues	• Were audits regularly conducted on both physical and IT-related security measures? • Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse? • Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet? • Were the methods for accessing and transmitting personal data sufficiently secure, e.g., access limited to authorised personnel only? • Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data? • Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data? • Is there a need to develop new data-breach scenarios?
Resource Related Issues	• Were there enough resources to manage the data breach? Should external resources be engaged to better manage such incidents? • Were key personnel given sufficient resources to manage the incident?
Employee Related Issues	• Were employees aware of security related issues? • Was training provided on personal data protection matters and incident management skills? • Were employees informed of the data breach and the learning points from the incident?
Management Related Issues	• How was management involved in the management of the data breach? • Was there a clear line of responsibility and communication during the management of the data breach?

Source : https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-managing-data-breaches-v1-0-(080515).pdf?sfvrsn=2

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

ANNEX A: SAMPLE ACCESS REQUEST FORM

I. APPLICATION TO ACCESS PERSONAL DATA	
1. Under the Personal Data Protection Act 2012 ("PDPA"), you are entitled to request for your personal data that we have, and request to know how your personal data has been used or disclosed over the past year. 2. Please complete this form and submit it to: <Please specify any other modes to submit an access request below>	
In person or by post: Data Protection Officer Organisation ABC ABC Complex 123, ABC Road Singapore 123456	Alternatively, you can email the completed form to us: DPO@abc.com.sg
II. PARTICULARS OF REQUESTOR	
<For this section, please determine the types of information your organisation requires in order to process the access request, including any documentation required to establish that the requestor is legally authorised to act on behalf the other individual(s)>	
Name of requestor:	
Contact number:	Email address:
Please check the applicable box(es): □ I am making an access request for my own personal data □ I am making an access request on behalf of other individual(s)	
Please complete this section if you are making an access request on behalf of other individual(s)	
Name of other individual(s) whom you are making an access request on behalf of:	
Contact number:	Email address:
III. DESCRIPTION OF THE PERSONAL DATA REQUESTED	
To enable us to process your access request quickly and efficiently, please provide us with as much information as possible about the personal data you are requesting access to (e.g. type of personal data, date, time).	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

ANNEX A: SAMPLE ACCESS REQUEST FORM

IV. DECLARATION	
By submitting this form, I confirm that the information stated above is true, complete and accurate to the best of my knowledge and belief.	
_____ Name & Signature	_____ Date (DD/MM/YYYY)

Additional Notes:

- If there are terms and conditions for services that your organisation may provide to the individual in conjunction with the access requests (e.g. reproduction costs depending on the number of copies requested), please provide these to the individual together with this form. However, please note that organisations cannot limit their obligations to provide access through contractual terms and any fee should be reasonable. Individuals may apply to the Commission for review if an organisation does not comply with its obligation to provide access or if the fee charged by the organisation to respond to the access request is not reasonable.
- If the information is lengthy, please consider directing the requestor to other channels of information. For example, you may wish to consider if it would be appropriate to provide the terms and conditions on a separate page or your organisation's website.

<Proof of identity>

- If an individual is making an access request for his/her own personal data, what form(s) of proof of identity or documentation does your organisation require or accept?
- If the applicant is making an access request on behalf of another individual, what form(s) of proof of identity or documentation does your organisation require or accept?

<Fees>

- Please make clear if your organisation charges a fee for an access request, and how your organisation will inform the individual of any applicable fees.
- What mode and/or term(s) of payment does your organisation accept?

<Processing>

- Please make clear the processing time for an access request, and how does your organisation inform the individual if it requires more time to process the access request?

<Denial of access request>

- Please make clear if there are any circumstances where your organisation does not grant an access request. For example, prohibitions or exceptions that are provided under the PDPA or other written law.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

How well does your organisation protect personal data? This self-assessment checklist is based on the nine personal data protection obligations underlying the Personal Data Protection Act 2012 (PDPA) and is designed to assist your organisation in reviewing its policies and to consider ways in which it can protect the personal data in its custody.

Please note that the data protection provisions in the PDPA (parts III to VI) do not apply to:

- An individual acting in a personal or domestic capacity;
- An employee acting in the course of his or her employment with an organisation;
- A public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data; and
- Business contact information. This refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes

Consider the following questions along with your organisation's current practices.

S/N	Item	Yes/No Action Plan
1–3. Consent, Purpose Limitation and Notification Obligations		
A. Collection of Personal Data		
1.	Do you collect personal data about your customers or employees, such as: • Full name • NRIC or FIN number • Passport number • Photograph or video image of an individual • Mobile telephone number • Personal email address • Thumbprint • DNA profile • Name and residential address • Name and residential telephone number *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.*	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
2.	Do you have a personal data inventory map on: • What personal data is collected and why? • Who collects it? • Where it is stored? • Who it is disclosed to? *Knowing the personal data you collect may help you to identify and put in place appropriate data protection policies.*	
3.	When collecting personal data, do you clearly inform the individual the purpose(s) for which it will be collected, used or disclosed and obtain his/her consent?	
4.	If you collect personal data from third parties, do you ensure that the third party has obtained consent from the individuals to disclose the personal data to you for your intended purposes? *You should generally ensure that the third party has obtained the consent from the individuals to collect, use and disclose their personal data for your intended purposes, before collecting, using or disclosing the personal data.*	
5.	If you are engaging a data intermediary to collect, use or disclose personal data on your organisation's behalf, have you ensured that the data intermediary will take the necessary action to ensure that your organisation will be in compliance with the PDPA? *Whilst a data intermediary may only be required to comply with the Protection and Retention Limitation Obligations, the organisation for whom it is processing personal data will be subject to the entire PDPA in respect of such personal data.*	
6.	Is there a formal process for the withdrawal of consent by individuals in respect of the collection, use or disclosure of their personal data? *Ensure that the individual's personal data is no longer collected, used or disclosed after a reasonable period for the withdrawal process to take place.*	
7.	If you intend to collect personal data without consent, have you checked the Second Schedule and other provisions of the PDPA to understand when you may collect personal data without consent?	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
A.	**Use of Personal Data**	
8.	Do you limit the use of personal data collected to only purposes that you have obtained consent for?	
9.	For personal data collected before the data protection requirements of the PDPA come into operation, are you using the personal data only for the purposes that it was collected for? *You may continue to use personal data that has been collected before the data protection requirements of the PDPA come into operation for the purposes for which the personal data was collected, unless the individual has withdrawn consent. If there is a fresh purpose for the use of such personal data, consent should be obtained. For personal data collected after the data protection requirements of the PDPA come into operation, you should notify and obtain the individual's consent to the collection, use and disclosure of his/her personal data.*	
10.	If you intend to use personal data without consent, have you checked the Third Schedule and other provisions of the PDPA to understand when you may use personal data without consent?	
A.	**Disclosure of Personal Data**	
11.	Do you limit the disclosure of personal data collected to only purposes that you have obtained consent for?	
12.	If you intend to disclose personal data without consent, have you checked the Fourth Schedule and other provisions of the PDPA to understand when you may disclose personal data without consent?	
4. Access & Correction Obligations		
13.	Have you established a formal procedure to handle requests for access to personal data? *Under the PDPA, individuals may request to access their personal data. There are, however, prohibitions and exceptions under the PDPA that may apply.*	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
14.	Do you have a list of third party organisations to whom personal data was disclosed and for what purposes? *You should provide information about the ways in which the individual's personal data has been or may have been used or disclosed by the organisation within a year before the request.*	
15.	If you are imposing an administrative fee for access requests, have you developed the fee structure? *Please refer to the Regulations on the charging of an administrative fee for access requests.*	
16.	Have you established a formal procedure to handle correction requests of personal data? *An individual may request to correct an error or omission in the personal data that you have about him/her. Unless you are satisfied on reasonable grounds that the correction should not be made, you should correct the personal data as soon as practicable, unless an exception under the PDPA applies.*	
17.	Have you established a formal procedure to send corrected personal data to third party organisations that personal data was disclosed to within one year of the correction? *If a correction is made, generally, you should send the corrected data to other organisations to which the data has been disclosed within a year the correction is made, unless the organisation does not need the corrected data for business or legal purposes. Further, with the individual's consent, you may send the corrected data only to selected organisations (unless you are a credit bureau).*	
18.	Have you checked S21(3), and the Fifth and Sixth Schedules of the PDPA to understand when you are not required to provide access or correct personal data?	
5. Accuracy Obligation		
19.	Do you make reasonable effort to verify that the personal data kept are accurate and complete (i) prior to any use to make a decision that affects the individual or (ii) prior to disclosure? *You are obligated to keep the personal data you collect* reasonably *accurate and complete, if the personal data is likely to be used to make a decision about the individual, or is likely to be disclosed to another organisation.*	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
6. Protection Obligation		
20.	Have you assessed the personal data protection risks within your organisation and put in place personal data security policies?	
21.	Is the personal data that you hold adequately classified? *Different sets of data may be accessed by various parties. It is important that your employees, vendors and partners access the personal data on a need-to-know basis, hence the data should be classified and stored adequately to ensure only authorised access.*	
22.	Is the personal data kept in a secure manner? *Keep personal data in your possession or under your control safe and secure from unauthorised access, modification, disclosure, use, copying, disposal or similar risks, whether in manual or electronic form. Analyse the likelihood of security failures occurring, considering possible threats and vulnerabilities.*	
23.	Do external parties have easy access to the personal data that you hold? *For example, hardcopy records that require customers or vendors to fill in should be filed immediately upon submission to prevent others from obtaining access. Visitors to your premises should be escorted, and employees be informed prior to keep personal data out of sight.*	
24.	Are there any remedial measures in place in the event of a breach? *Draft up a remedial plan that identifies the appropriate action, resources, responsibilities and priorities for managing personal data security breaches.*	
25.	Do you conduct or schedule regular audits on the data protection processes within your organisation?	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
26.	Are there contractual provisions in place to ensure proper safeguards in respect of personal data disclosed to outsourced parties who will be processing personal data on your behalf? *Ensure that such outsourced parties who are data intermediaries under the PDPA will take the necessary action to ensure that your organisation will be in compliance with the PDPA. Please refer to the note in Qn 5.*	
7. Retention Limitation Obligation		
27.	Is there regular data housekeeping? *Do not keep personal data for longer than necessary for business or legal purposes. Define specific retention periods for your various classifications of personal data in accordance with legal and business requirements.*	
28.	Do you remove personal data no longer needed for business or legal purposes? *For example, hard copy records containing personal data should be shredded or otherwise securely destroyed. Electronic data should be erased completely. Otherwise, anonymise the data such that no individual can be identified from the data kept.*	
8. Transfer Limitation Obligation		
29.	Do you put in place the appropriate contractual arrangements or binding corporate rules to govern the transfer of personal data overseas? *Do not transfer any personal data to a country or territory outside Singapore unless you ensure that the standard of protection accorded to the data transferred is comparable to the protection under the PDPA. Please refer to the Regulations for the requirements relating to a transfer of personal data overseas.*	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
9. Openness Obligation		
30.	Have you designated one or more individuals (who may be referred to as data protection officers) to be responsible for ensuring that the data protection policies and practices of your organisation are in compliance with the PDPA? *In a small business, the designated individual may be the owner or manager. In a larger organisation, the designated individual may be someone on the management team or a specific data protection officer with the requisite seniority, authority and competencies for the role. The person(s) designated may delegate his/her responsibilities in relation to the organisation's obligations under the PDPA to another individual.*	
31.	Does your data protection officer(s) know his/her roles and responsibilities in ensuring personal data in your organisation's possession or control is well-protected?	
32.	Is the business contact information of your designated data protection officer(s) made available to the public? *Organisations should make their data protection policies and the business contact information of their data protection officers (or the individuals to whom the responsibility have been delegated to) publicly available.*	
33	Have you developed and implemented data protection policies for your organisation to meet its obligations under the PDPA? Are your organisation's data protection policies made available to the public? *Please refer to the note in Qn 32.*	
34.	Have you developed a process to receive, investigate and respond to complaints that may arise with respect to the application of the PDPA?	
35.	Is information on your organisation's complaint process made available on request?	
36.	Have you communicated information about your organisation's data protection policies and practices to your employees, in particular, but not limited to, employees who are handling personal data? *Employees in the marketing, computer security or database management departments may require specialised training to ensure their management of personal data complies with the PDPA.*	
37.	Do your employees know who to pass the requests to if it is not their responsibility to respond to such requests?	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
1.	Personal Data	**Exclusions** Excluded personal data 5.16 The PDPA does not apply to, or applies to a limited extent to, certain categories of personal data. 5.17 The PDPA does not apply to the following categories of personal data: a) Personal data that is contained in a record that has been in existence for at least 100 years; and b) Personal data about a deceased individual who has been dead for more than 10 years. 5.18 For personal data about a deceased individual who has been dead for 10 years or less, the PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply.
2.	Business contact information (BCI)	**Exclusions** The Data Protection Provisions do not apply to business contact information. Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".
3.	Organisations	**Exclusions** **Excluded organisations** 6.5 The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of organisations are therefore excluded from the application of the Data Protection Provisions: a) Any individual acting in a personal or domestic capacity; b) Any employee acting in the course of his or her employment with an organisation; c) Any public agency; and d) Any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data. In addition, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below. 6.7 Organisations which are not within an excluded category should note that they are required to comply with the PDPA when dealing with an organisation that is within an excluded category. **Individuals acting as employees** 6.11 The second significant exclusion for individuals in the PDPA relates to employees who are acting in the course of their employment with an organisation. Employees are excluded from the application of the Data Protection Provisions. The PDPA defines an employee to include a volunteer. Hence, individuals who undertake work without an expectation of payment would fall within the exclusion for employees.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex B – PERSONAL DATA PROTECTION CHECKLIST FOR ORGANISATIONS

S/N	Item	Yes/No Action Plan
40.	In relation to individuals who have not given their clear and unambiguous consent for telemarketing, have you established an internal process for checking with the DNC registry prior to your telemarketing campaigns? *Please refer to the note in Qn 39.*	
41.	If you purchase databases of contact information from third parties for your telemarketing activities, do you ensure that the third party has obtained the necessary consents for the collection, use and disclosure of the personal data by you?	
42.	When you make a voice call containing a marketing message, is your calling line identity concealed or withheld from the recipient? *If your organisation is making (or causing or authorising the making of) a voice call containing a marketing message, ensure that the calling line identity (phone number or information identifying the sender) is not concealed.*	
43.	Do your telemarketing messages include clear and accurate information identifying your organisation as well as contact details? *The message should include information about the organisation and how the recipient can readily contact you. In addition, the message should reasonably be valid for at least 30 days after the message is sent. This allows the recipient to contact you for clarifications, if necessary.*	
44.	If you outsource the telemarketing function, do you ensure that your vendor complies with the DNC provisions in the PDPA? *Whether you are directly sending the marketing messages or authorising another organisation to do so, you have to ensure that such messages are not sent to Singapore telephone numbers registered with the DNC registry (unless the clear and unambiguous consent of the individuals to the sending of the telemarketing messages to the Singapore telephone numbers have been obtained).*	

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
1.	Personal Data	**Exclusions** Excluded personal data 5.16 The PDPA does not apply to, or applies to a limited extent to, certain categories of personal data. 5.17 The PDPA does not apply to the following categories of personal data: a) Personal data that is contained in a record that has been in existence for at least 100 years; and b) Personal data about a deceased individual who has been dead for more than 10 years. 5.18 For personal data about a deceased individual who has been dead for 10 years or less, the PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply.
2.	Business contact information (BCI)	**Exclusions** The Data Protection Provisions do not apply to business contact information. Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".
3.	Organisations	**Exclusions** **Excluded organisations** 6.5 The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of organisations are therefore excluded from the application of the Data Protection Provisions: a) Any individual acting in a personal or domestic capacity; b) Any employee acting in the course of his or her employment with an organisation; c) Any public agency; and d) Any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data. In addition, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below. 6.7 Organisations which are not within an excluded category should note that they are required to comply with the PDPA when dealing with an organisation that is within an excluded category. **Individuals acting as employees** 6.11 The second significant exclusion for individuals in the PDPA relates to employees who are acting in the course of their employment with an organisation. Employees are excluded from the application of the Data Protection Provisions. The PDPA defines an employee to include a volunteer. Hence, individuals who undertake work without an expectation of payment would fall within the exclusion for employees.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
4.	Consent Obligation	**Exceptions** 12.50 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) only in the circumstances provided in the Second Schedule (Collection of personal data without consent), Third Schedule (Use of personal data without consent) and Fourth Schedule (Disclosure of personal data without consent) to the PDPA respectively. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations. 12.51 One significant exception in the Second, Third and Fourth Schedules to the PDPA relates to personal data that is publicly available. The term "publicly available" is defined in section 2(1) of the PDPA and refers to personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public. 12.61 For the avoidance of doubt, the PDPA provides exceptions for news organisations to collect, use and disclose personal data without consent solely for its news activity, regardless whether the personal data is publicly available.
5.	Access and Correction Obligations	**Exceptions** 15.22 The obligation in section 21(1) is subject to a number of exceptions in sections 21(2) to 21(4) including some mandatory exceptions relating to situations where an organisation must not provide access. These exceptions are listed below. 15.23 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to. The exceptions specified in the Fifth Schedule include the following matters: a) opinion data kept solely for an evaluative purpose;9 b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
5.	Access and Correction Obligations	**Exceptions** d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; e) a document related to a prosecution if all proceedings related to the prosecution have not yet been completed; f) personal data which is subject to legal privilege; g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation; h) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed i) the personal data was collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he was appointed to act – i. under a collective agreement under the Industrial Relations Act (Cap. 136); 75 ii. by agreement between the parties to the arbitration or mediation; iii. under any written law; or iv. by a court, arbitral institution or mediation centre; or j) Any request – i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; iii. for information that does not exist or cannot be found; iv. for information that is trivial; or v. that is otherwise frivolous or vexatious. **Exceptions to the obligation to correct personal data** 15.44 Section 22(6) provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. In addition, section 22(7) provides that an organisation is not required to make a correction in respect of the matters specified in the Sixth Schedule to the PDPA. These are: a) opinion data kept solely for an evaluative purpose;17 b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; and e) a document related to a prosecution if all proceedings related to the prosecution have not been completed.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
6.	Transfer Limitation Obligation	**Exemptions** •Section 26(2) of the PDPA provides that the PDPC may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to section 26(1) in respect of any transfer of personal data by that organisation. •An exemption granted under section 26(2) may be granted subject to such conditions as the PDPC may specify in writing and may be revoked at any time by the PDPC.
7.	DO NOT CALL provisions "specified message"	**Exclusions** 27.1 Section 37(5) provides that a specified message will not include any of the messages referred to in the Eighth Schedule to the PDPA. The messages referred to in the Eighth Schedule are therefore not specified messages for the purpose of the Do Not Call Provisions and are not subject to the application of those provisions. A specified message shall not include any of the following: a) any message sent by a public agency under, or to promote, any programme carried out by any public agency which is not for a commercial purpose; b) any message sent by an individual acting in a personal or domestic capacity; c) any message which is necessary to respond to an emergency that threatens the life, health or safety of any individual; d) any message the sole purpose of which is – i. to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender; or ii. to provide warranty information, product recall information or safety or security information with respect to a product or service purchased or used by the recipient of the message; or iii. to deliver goods or services, including product updates or upgrades, that the recipient of the message is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender; e) any message the sole purpose of which is to provide – i. notification concerning a change in the terms or features of; ii. notification of a change in the standing or status of the recipient of the message with respect to; or iii. at regular periodic intervals, account balance information or other type of account statement with respect to, f) any message the sole purpose of which is to conduct market research or market survey; or g) any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
7.	DO NOT CALL provisions "specified message"	**Exemption for certain specified messages** 4.1 The Commission notes that individuals with an ongoing relationship with other persons may wish to receive information from those persons about goods and services which are related to the subject of the ongoing relationship. In the same vein, persons may wish to keep their customers or members (with whom they have an ongoing relationship) updated about related goods and services that are available to them. This is especially the case if the information is beneficial in some way to the individuals who are in an ongoing relationship, for example if it facilitates the individuals' utilisation of the goods and services purchased through the ongoing relationship or their utilisation of a membership.
8.	DO NOT CALL provisions exclusions	**Exclusion** 30.1 The PDPA excludes certain persons from the scope of the Do Not Call Provisions to the extent that the sending of the message does not involve active intervention on their part. Specifically, under section 36 (2) and (3) of the PDPA, the following persons are presumed not to have sent or authorised the sending of a message unless the contrary is proved: a) a telecommunications service provider who merely provides a service that enables the sending of a specified message; and b) the owners or authorised users of a telecommunication device, service or network that was used to send a specified message if, at the relevant time, that device, service or network was controlled by a person without the knowledge of the owner or authorised users.
9.	Closed-circuit television cameras ("CCTVs")	**Exceptions** The exception relating to "managing or terminating an employment relationship" only apply when there is an employment relationship. Where an organisation is collecting the personal data of individuals that are not its employees for a specific purpose, this specific exception would not apply. However, other exceptions may apply, for example where the organisation is required under written law to collect personal data of such individuals in order to assess whether the qualifications of such individuals comply with regulatory requirements.

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex C – EXCEPTIONS, EXEMPTIONS AND EXCLUSIONS

S/N	Item	Exceptions / Exemptions / Exclusions
10.	Photographs	**Exceptions** Exceptions to this Consent Obligation may apply depending on the circumstances, for example where the photographer is acting in his personal or domestic capacity (such as when an individual takes photographs for his own personal purposes at a gathering for family and friends).
11.	Enforcement - Investigation	**Exclusions** 15.6 Where the Commission has conducted a review under section 28 of the PDPA and made a decision or issued a direction under section 28(2) of the PDPA, the Commission will generally not commence an investigation in relation to the organisation's compliance with section 21 or 22 of the PDPA unless there appears to the Commission to be a significant non-compliance with section 21 or 22 of the PDPA or there are exceptional circumstances which, in the Commission's view, indicate that an investigation should be commenced. For this purpose, a significant non-compliance with section 21 or 22 of the PDPA may include the following: (a) systemic failure on the part of the organisation including (without limitation) where an organisation does not have any processes in place to comply with section 21 or 22 of the PDPA; or (b) intentional non-compliance with section 21 or 22 of the PDPA or a decision or direction under section 28(2) of the PDPA, for example, where an organisation has sought, through its processes, to deny individuals' requests for reasons that are not permitted under the PDPA

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 1

Managing Personal Data Breaches with C.A.R.E



In this highly-connected day and age, personal data breaches can happen to any organisation. This is why organisations should always have a data breach management plan in place.

With more and more personal data being collected and stored in the digital format in an increasingly connected world, savvy organisations know that they should not only take steps to prevent data breaches, but to also be ready for them if and when they occur.

Personal data breaches can happen in various ways. This includes malicious activities such as hacking or theft of electronic storage devices, human errors such as accidental disclosure to an unintended recipient via email or improper disposal of devices containing personal data, and computer system errors where errors or bugs in programming code render the software vulnerable to unauthorised disclosure. "Personal and sensitive data have always been the target of criminals due to the value they bring," says Mr Alagu Karuppiah, Head of Information Technology Department at Diners Club Singapore. "As the world becomes more intertwined with Internet of things (IoT), we foresee that cyber security incidents and data breaches will increase in the future." This concern is shared by Mr Tan Boon Chew, Data Privacy Officer and Head of Regulatory Compliance and Assurance at AIA Singapore (AIAS). As a life insurer, AIAS is the custodian of policy records belonging to over one million customers. These records contain a multitude of personal data such as customers' NRIC number and date of birth, and are stored in digital format for ease of administration and processing.

"With increasingly sophisticated methods in data theft, it is important to protect and secure these personal data against intrusion," he says.

Consequences Of A Data Breach

A personal data breach can exact a high toll on an organisation, not just from a financial standpoint but also in terms of reputational damage. Mr P K Raman, Chief Information Officer at Standard Chartered Bank Singapore, shares findings from the 2015 Cost and Data Breach Study conducted by Ponemon Institute, which pegged the average cost paid for each lost or stolen record containing sensitive and confidential information at US$154.

More serious than that, however, is the potential fallout in terms of customer trust and confidence.

"For the bank, our most valuable assets are trust and reputation and we need to uphold these vigorously," says Mr Raman. "Losing customers' trust will damage corporate reputation and can in turn lead to loss of customers and business. Moreover, banking is a heavily regulated sector and we have to comply with all regulations or risk facing enforcement actions."

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/May-16/pdf/Managing_Personal_Data_Breaches_with_C_A_R_E.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES



CASE 1 (cont'd)
Managing Personal Data Breaches with C.A.R.E

Consequences Of A Data Breach

Building and protecting trust is also an important business imperative for the insurance sector. "The insurance business is built on trust as we deal with customers' personal and sensitive information, such as their medical history, claim details and financial data," says Mr Tan. "Hence, a major breach on personal data would significantly impact an insurer's reputation, brand and market value."

Besides these business considerations, organisations that fail to safeguard personal data may also be subject to enforcement actions by the Personal Data Protection Commission (PDPC).

Under the Protection Obligation of the Personal Data Protection Act (PDPA), organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Penalties for breaching the PDPA depend on numerous factors, such as the seriousness and impact of the breach, the immediacy and effectiveness of corrective actions taken to address the breach, and whether the breach was caused by the organisation deliberately, wilfully or out of negligence.

Minimising The Impact

Prevention is always better than cure. However, an organisation should also have in place a data breach management plan so that it can respond swiftly and effectively to personal data breaches.

While Diners Club Singapore had worked with an audit firm to develop its policies and operating processes for data breach management, Mr Karuppiah shares that there are many reliable sources of information that can help organisations build a data breach management plan, such as the resources found on the PDPC website.

PDPC's Guide on Managing Data Breaches points out that organisations may consider adopting the CARE model when developing a data breach management plan. The acronym CARE stands for containing the breach, assessing risks and impact, reporting the incident and evaluating the response and recovery to prevent future breaches.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/May-16/pdf/Managing_Personal_Data_Breaches_with_C_A_R_E.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 1 (cont'd)
Managing Personal Data Breaches with C.A.R.E



Putting The Plan To The Test

Having a data breach management plan itself does not suffice; it has to be tested regularly to ensure that it is effective, says Mr Karuppiah. This can be done alongside an organisation's business continuity planning.

Testing may involve putting a case study through the various stages of breach management to see if the plan works. However, this cannot be a onetime effort, he adds. "Incident management is a continuous learning process. The organisation has to adapt and change with the environment and situation."

At Standard Chartered Bank, its data breach management plan is also constantly tested and revised in line with industry best practices, says Mr Raman. "This helps ensure that if a data breach happens, we can act promptly and appropriately to identify the issue, minimise the impact, recover, and restore the confidence of our stakeholders quickly".

Getting Senior Management Involved

Another point that was highlighted by the organisations is the importance of involving senior management in data breach management.

Having support from the top and a culture of ownership are essential in developing a good data breach management plan, says Mr Tan. This will help ensure that critical components of the plan such as an effective reporting system, lapse treatment and remediation processes are well embedded within the organisation.

One suggestion would be to have the incident response committee spearheaded by the senior management. Key stakeholders that oversee the plan should also recognise that the plan is not intended to be static and must be refined along the way for continuous improvement, he adds.

Conclusion

Due diligence, trained staff, regular audits and reviews of systems and processes are essential in ensuring the security of personal data. However, prevention alone is not enough. Organisations also have to be prepared to deal with data breaches when they occur by putting in place an effective data breach management plan.

As Mr Karuppiah says, it should not be a question of "if" but "when" a data breach will occur. "With a tested breach management response plan, an organisation will be better able to minimise the impact of a breach by engaging its legal, insurance, public relations, technology and management among other stakeholders, in a timely manner to save its reputation and business."

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/May-16/pdf/Managing_Personal_Data_Breaches_with_C_A_R_E.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 2
Transparency and Accuracy of Personal Data
A Win-Win Situation



A guest at a private event asks to view a photograph of him taken by the official event photographer. Does the event organiser accede to his request?

A member of a spa wants to know how her personal data is being used by the company. Does the spa provide her with the information?

Under the Access and Correction Obligation of the Personal Data Protection Act (PDPA), an organisation has to allow an individual access to, and correction of, his personal data that is in the possession or control of the organisation, unless there is an applicable exception. Meeting these obligations will help the organisation demonstrate transparency and ensure that personal data is updated so that any decision it makes in relation to any individual is based on accurate data about the individual.

As Mr Poh Chee Yong, Data Protection Officer (DPO) of real estate agency ERA Realty Network pointed out, "The data is used for contacting customers, providing updates and for billing purposes, so it is in the commercial interest of both parties to want the particulars to be correct."

In the case of ERA, its clients would have bought or sold a property, or leased or tenanted one, through its salespersons. "Most of the time, if not all, our salespersons would make sure that the personal data is accurate. In the unlikely event that there is an error, it is critical that such information is amended in the first instance," he said. For ERA, individuals typically call or write in to the DPO – whose email is made available online together with the company's personal data protection policies – to find out what personal data is in the company's possession or control, and to update or correct it if necessary. To ensure that such requests are promptly addressed, the email address dpo@era.com.sg is checked by both the DPO and the head of the company's IT department, Mr David Seah. Customers can expect a reply within one or two working days, said Mr Poh, who is also ERA's Chief Financial Officer.

Providing Access To Personal Data

Under the PDPA, an access request does not need to be accompanied by a reason. However, asking the requester to be more specific as to what personal data he requires could be helpful to both the individual and the organisation.

For the organisation, it will help them to prepare the information in a way that will be useful to the requester and to do it more efficiently.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/april-16/pdf/TransparencyAndAccuracyOfPersonalDataAWin-WinSituation.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES



CASE 2 (cont'd)
Transparency and Accuracy of Personal Data
A Win-Win Situation

Providing Access To Personal Data

For example, if an individual is requesting for CCTV footage to ascertain whether he had left a particular piece of belonging in a restaurant at a specific time, providing this information will enable the relevant footage to be prepared more quickly. Alternatively, a written description may suffice in some instances.

> "The data is used for contacting customers, providing updates and for billing purposes, so it is in the commercial interest of both parties to want the particulars to be correct."
>
> **- Mr Poh Chee Yong**
> Data Protection Officer (DPO) of
> Real Estate Agency ERA Singapore

For the individual, being more specific with the request will be beneficial as it reduces both the time and costs of access, if applicable. The PDPA allows organisations to levy a reasonable fee based on the incremental costs of providing access, and this fee should fairly reflect the time and effort involved in responding to an access request.

While granting access, organisations should also exercise due diligence and adopt appropriate measures to verify the requester's identity.

Under ERA's personal data protection policy, the company may ask for proof of identity before revealing any information to the requester. Depending on what the company has on record, this proof of identity could take the form of the requester's full name and NRIC, FIN or passport number, or date of birth, residential address, or transaction history if the requester is not comfortable in revealing certain particulars such as his NRIC.

If an organisation receives an access request from an individual, it will have to provide the requester with access to the relevant personal data, as soon as reasonably possible and also information about the ways in which the personal data has been used or disclosed within the preceding 12 months.

This is assuming that the request is not a frivolous one (for example, from a serial requester), and that the burden or expense of providing access would not be unreasonable to the organisation or disproportionate to the individual's interests.

Other exceptions to the Access obligation include cases where personal data, if disclosed, would reveal confidential commercial information that could harm the competitive position of an organisation, or where personal data has been collected, used or disclosed without consent for investigations, proceedings and appeals that have not yet been completed. These are among the exceptions stated in paragraph 1(e) of the Second Schedule and the Third Schedule, and paragraph 1(f) of the Fourth Schedule of the PDPA.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/april-16/pdf/TransparencyAndAccuracyOfPersonalDataAWin-WinSituation.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 2 (cont'd)
Transparency and Accuracy of Personal Data
A Win-Win Situation



Providing Access To Personal Data

If a request does not fall under any of the exceptions, one question would be how much information does the organisation need to provide? In general, the question of "how" can be answered by indicating the purpose for which the data was used rather than detailing the specific activities involved.

For example, the organisation could indicate that the personal data was used for audit purposes, without going into specific instances on when the audits were carried out. However, when it comes to the ways in which the personal data has been disclosed, it may be more helpful to provide specific names of organisations to whom the data has been disclosed to. This will allow the individual to approach the third-party organisation for more information should he wish to do so.

One good practice is to maintain a list of all possible third parties that the organisation discloses personal data to, and share this with any individual who puts in an access request. The information that is given to the individual should be in documentary form, or if it is impractical, the requester should be given the opportunity to examine the personal data and how it had been used or disclosed.

Addressing Errors And Omissions

In addition to acceding to access requests, organisations are also generally required to correct errors or omissions in an individual's personal data upon his request. Under the PDPA, they are not entitled to impose a charge for this. The correction should be made as soon as it is practical to do so and the amended version sent to every other organisation that the personal data was disclosed to within a year before the date the correction was made; unless that other organisation does not need the corrected personal data for any legal or business purposes. Third-party organisations which are notified of the correction will then generally have to correct the personal data that is in their possession. There may, however, be instances where a correction is not made.

For example, a customer may request an online retailer to update his residential address, which forms part of his personal data, and the retailer duly notifies an affiliate that is servicing the customer's warranty. The affiliate may determine that there are reasonable grounds not to correct its records relating to the customer because the customer's warranty has expired. In cases like this, it is good practice to make a note as to why a correction has not been made.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/april-16/pdf/TransparencyAndAccuracyOfPersonalDataAWin-WinSituation.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

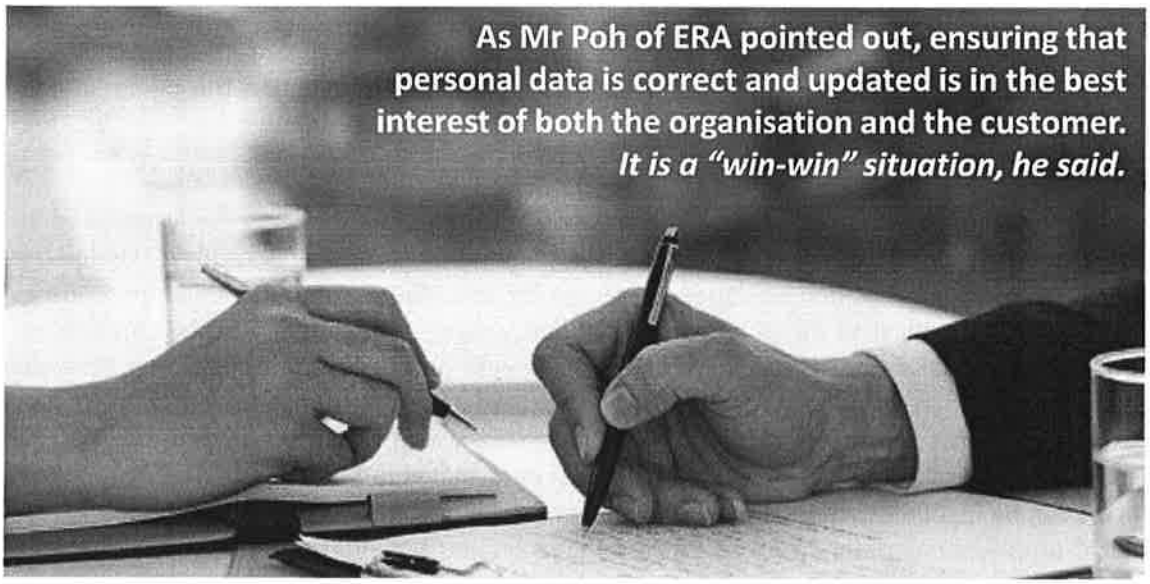
CASE 2 (cont'd)
Transparency and Accuracy of Personal Data
A Win-Win Situation



There are also specific circumstances where corrections need not be made, such as those cited in section 22(6) and the 6th Schedule of the PDPA.

Conclusion

It makes business sense to respond promptly and transparently to request for access and correction. A good practice for organisations to adopt would be to institute standard procedures and forms that will help them respond to such requests efficiently and effectively. As Mr Poh of ERA pointed out, ensuring that personal data is correct and updated is in the best interest of both the organisation and the customer. It is a "win-win" situation, he said..



Source: https://www.pdpc.gov.sg/resource/DPO-Connect/april-16/pdf/TransparencyAndAccuracyOfPersonalDataAWin-WinSituation.pdf

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 3
Protecting the Personal Data of Job Applicants and Employees



Most employers are aware of the PDPA and have implemented some measures to comply with the PDPA. This is according to a 2015 survey conducted by the Personal Data Protection Commission.

The survey found 92 percent of employers to be aware of the PDPA, and 86 percent had implemented some compliance measures.

Pretty encouraging figures to ponder over since the PDPA came into force in 2014[1]. Nonetheless, Executive Director of the Singapore National Employers Federation (SNEF), Mr. Koh Juan Kiat, believes that more can be done to close certain gaps, by "developing comprehensive policies and procedures to ensure that all the legal obligations of the PDPA are observed." Mr. Koh highlighted that "employers, especially their human resource representatives, must know the organisations' legal obligations under the Personal Data Protection Act (PDPA) and have in place policies and procedures to comply with them".

SNEF has observed that some employers might not have fully grasped the concept of personal data, and that personal data in written form is only one of many forms of personal data that they are collecting. Personal data may also be captured in photographs or CCTVs (in the form of an individual's image). Irrespective of the type of personal data, organisations should treat the personal data of their employees and job applicants with equal care as they would treat the personal data of any other individuals. Organisations have to comply with the PDPA when they collect, use or disclose personal data, such as notifying the individual of the purposes and obtaining their consent. They must also protect the personal data in their possession or under their control, unless an exception applies for certain obligations.

Obtaining Consent

The PDPA does not prescribe the manner in which organisations should obtain consent from an individual for the collection, use and disclosure of his personal data, although written consent is encouraged to prevent potential disputes.

The PDPA also provides for "deemed consent" to apply in certain situations. For example, a job applicant who voluntarily provides his personal data when applying for a job with the organisation may be deemed to have consented to the organisation's collection and use of his personal data for the purpose of processing his job application.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/March-16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf?123

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 3 (cont'd)
Protecting the Personal Data of Job Applicants and Employees



Obtaining Consent

There may also be certain situations where consent is not required to collect, use or disclose personal data, such as when it is necessary for certain evaluative purposes, for instance, obtaining references from a potential job applicant's former employer to determine his suitability for employment, or obtaining performance records to determine an employee's suitability for promotion.

Organisations also do not have to obtain the consent of the employee when their collection of the employee's personal data is reasonable for the purposes of managing or terminating the employment relationship with him, for example, collecting his bank account details for payment of salaries etc. However, organisations do need to notify employees of the collection, use or disclosure of their personal data for such purposes. Organisations may wish to consider if it would be appropriate to notify their employees through avenues like employment contracts, employee handbooks, or notices in the company intranet.

Securing Personal Data

Making reasonable security arrangements to protect personal data in its possession or under its control is another obligation under the PDPA. There is no "one size fits all" solution in protecting personal data and organisations should consider the nature of personal data, the form in which personal data has been collected and potential impact on the individual concerned if there was unauthorised access to the personal data when determining the security arrangements to adopt.

Recruitment company, PrimeStaff acknowledges the protection of personal data it collects in the course of its business as a business imperative. Its managing consultant and head of HR functions, Mr. George Gaspar, shared that the company has been protecting personal data even before the PDPA was enacted and explains the business philosophy as "an important part of protecting our reputation."

Amongst the slew of measures adopted by PrimeStaff include authorised personnel such as its recruiters and consultants having controlled access to PrimeStaff's Applicant Tracking System which stores job applicants' data. In addition, when an applicant is assessed to be suitable for a particular role, his profile is sent to the client, but not before personal data such as NRIC number or contact information are removed.

Source: https://www.pdpc.gov.sg/resource/DPO Connect/March-16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf?123

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES

CASE 3 (cont'd)
Protecting the Personal Data of Job Applicants and Employees



Securing Personal Data

A second measure involves the banning of external email services such as Gmail and Hotmail in the workplace to prevent data leakage. "When it comes to work-related matters, employees have to use the corporate email system," said systems administrator Mr. Wong Chew Foong, who is also PrimeStaff's Data Protection Officer. "We block all third-party email service providers and also media-sharing web sites such as Dropbox, iCloud and Google Drive to prevent soft copies of personal data from being transferred. Corporate email is the only way for our consultants to communicate with our applicants and clients."

Efforts have also been made to partially disable third-party storage devices such as thumb drives in a way that information can only be copied from the device to the computer, but not the other way round. And a strict hand phone policy ensures that employees conduct business communications using only company issued mobile devices.

The People Challenge

"One of the bigger challenges in ensuring compliance with the PDPA has to do with people", Mr. Wong noted. "A lot of information is transmitted daily. Employees can present a challenge because they may, unknowingly, accidentally or even deliberately do something that contravenes the PDPA."

To address this, whenever new employees join PrimeStaff, the dos and don'ts of personal data protection are clearly explained to them. The PDPA obligations are also reiterated during their monthly town hall meetings.

Internal training and sanctions are an important part of the equation. "If an employee breaches our policies, he has to face the consequences," said Mr. Gaspar. Training and constant reminders on personal data protection have proven to be effective too, as Mr. Gaspar was happy to note that "in all these years, there has not been a single case where we needed to penalise anyone".

Dealing with Data Intermediaries

Besides ensuring that their own policies, practices and systems are aligned with the requirements of the PDPA, organisations are also accountable for personal data that is being processed on their behalf by data intermediaries; another common PDPA compliance gap identified by SNEF. "Some organisations do not have a strict process to ensure that their data intermediary (third party) takes proper security measures to protect personal data. This is crucial when businesses outsource functions such as payroll and employee benefits," said Mr. Koh.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/March-16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf?123

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Annex D – CASE STUDIES



CASE 3 (cont'd)
Protecting the Personal Data of Job Applicants and Employees

Dealing with Data Intermediaries

Before organisations hand over their employees' personal data to a third party for processing, it is important that organisations talk to their vendor about the standards of personal data protection and include provisions in their written contract to clearly set out the data intermediary's responsibilities and obligations in handling the personal data.

Meeting the Retention Limitation Obligation

As part of the overall framework for personal data protection, the PDPA also requires employers and recruitment agencies to comply with the Retention Limitation Obligation. For example, after an employer has decided which job applicant to hire, the personal data that it has collected from other job applicants should only be retained for as long as it is necessary for business or legal purposes.

At PrimeStaff, when consent for the retention of personal data of a job applicant is given, the personal data of the job applicant is typically retained for three years unless the applicant opts out before that. "We keep the data in view that there would be another opportunity for the job applicant", said Mr. Gaspar. "Our observation shows that after three years, the data often has no more value. The applicant may have found another job or the information on the resume goes out of date."

Job applicants may also withdraw their consent for the retention, use and disclosure of their personal data by giving reasonable notice to effect the changes. To facilitate such withdrawal, organisations are to make available their consent withdrawal policy and advise job applicants on the manner to submit the withdrawal and the consequences of such withdrawal.

Conclusion

Organisations need to be equally mindful of their obligations under the PDPA when it comes to the personal data of their employees. It is essential for employers and recruitment agencies to have in place policies and processes to comply with the PDPA, obtain consent from their employees for the collection, use and disclosure of their personal data when required to do so, and ensure that their personal data is properly protected, accurate and stored only for the period that it is needed.

Source: https://www.pdpc.gov.sg/resource/DPO-Connect/March-16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf?123

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION

Other Resources

- **Guide To Securing Personal Data In Electronic Medium -** https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-securing-personal-data-in-electronic-medium-v1-0-(080515).pdf?sfvrsn=4

© Copyright 2016 PERSONAL DATA PROTECTION COMMISSION