Data Protection

Background

- Today, vast amounts of personal data are collected, used and even transferred to third party organisations for a variety of reasons.

- This trend is expected to grow exponentially as the processing and analysis of large amounts of personal data becomes possible with increasingly sophisticated technology.

- There is growing concerns from individuals about how their personal data is being used.

- By regulating the flow of personal data among organisations, the PDPA also aims to strengthen and entrench Singapore's competitiveness and position as a trusted, world-class hub for businesses.

CLICK./(+).click
CLICK./"..///=per-son-al (D+a+t+a)
"PERSONAL-data
data click+)))/"PERSONAL-data
PERSONAL DATA/*cLICK..))))))
CLICK./(+).click++click++click++~
CLICK./"..///=per-son-al (D+a+t+a)"
CLICK./"..///=per-son-al (D+a+t+a)"(/)
personal data click+)))/"PERSONAL-data
PERSONAL DATA/*cLICK..))))))
CLICK./(+).click++click++click+}=
CLICK./"..///=per-son-al (D+a+t+a)"
personal data click+)))/"PERSONAL

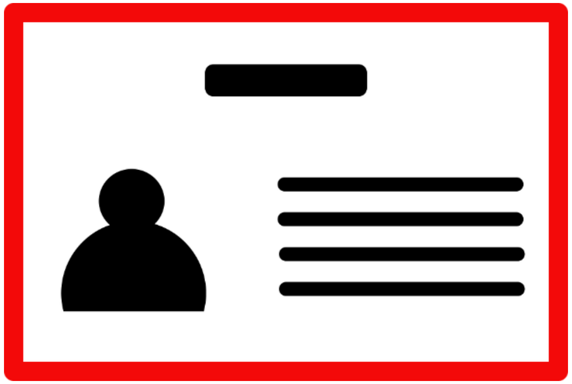
Data Privacy and Personal Data

- Data privacy is the right to prevent the release of personal information to the public.

- In Singapore, personal data is protected under the Personal Data Protection Act 2012 (PDPA) which :
  - came into operation on 2 Jan 2013
  - Is administered by Personal Data Protection Commission (PDPC).

What is Personal Data?

“**Personal data**” refers to **data 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.



Does it matter whether it is ***true or not*** ?

NO – covers both true or false PD

Personal data of ***deceased individuals***?

- Only certain rules (disclosure & safeguarding) apply
- Protection up to 10 years after death

Coverage – ***electronic or non-electronic data*** or both?

Both

Examples of Personal Data?

- **Unique identifiers**

  NRIC number

- **Set of data which put together would identify an individual**

  Name, age, occupation, address

- **Includes 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
- Name and residential telephone number

Stricter NRIC data collection rules

Unless required by law, from Sept 1, it will be illegal for organisations to physically hold on to an individual’s NRIC and collect its full number. Penalty up to $1 million.

- When is it required by law to collect IC number?
- Retention of IC for entering public sector buildings?
- What about HP numbers – key identifier for fund transfers such as PayNow?

https://www.straitstimes.com/tech/less-than-a-week-before-stricter-nric-rules-kick-in-non-compliance-could-result-in-hefty-fines (NRIC)
https://www.advomi.com.sg/amendments-pdpa/
https://www.connectedasia.com/update-on-proposed-amendments-to-singapores-pdpa/ (proposed amendments to Singapore’s PDPA)

Personal Data Protection

- **PDPA comprises rules governing**
  - **Collection,**
  - **Use,**
  - **Disclosure and**
  - **Care**

  of personal data.

- **PDPA recognises both the**:
  - Rights of individuals to protect their personal data, including rights of access and correction,
  - and the needs of organisation to collect, use or disclose personal data for legitimate and reasonable purposes.

PDPC’s Decisions

Breach of the Protection Obligation by Tan Tock Seng Hospital - *04 Nov 2019*

- A warning was issued to Tan Tock Seng Hospital for failing to put in place reasonable security arrangements to prevent the unauthorised disclosure of personal data of its patients.

- 85 Notification letters to patients to reschedule appointments were sent to wrong addresses.

Who has to comply with PDPA?

ORGANISATION

- Individual, company, association or body of persons, corporate or incorporate, whether or not
  - Formed or recognised under Singapore Law, or
  - Resident or having an office or a place of business in Singapore

NB: ‘Organisations’ will have to comply with the PDPA as well as other relevant laws that are applied to the specific industry that they belong to (e.g. Banking Act, Insurance Act). Data Intermediaries are also subject to PDPA.

What PDPA does not cover?

The PDPA does not cover:

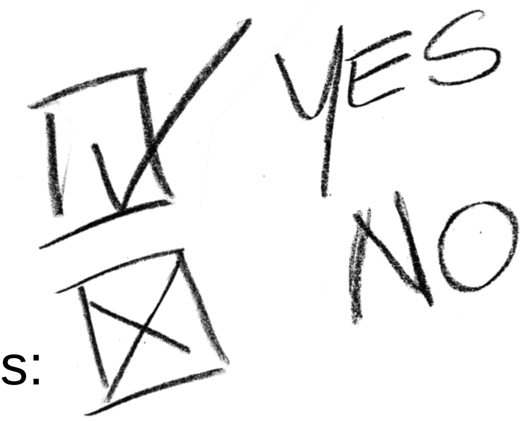
(a) Any individual acting in a personal or domestic capacity = personal friends

(b) Any employee acting in the course of his employment with an organization = as an employee

(c) Any public agency or an organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data = government agencies – eg; civil service

NB: Business contact information also not covered. 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 or her personal purposes (*business contacts*).

Key concepts in PDPA



The PDPA takes into account the following concepts:

- **Consent** – Organisations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);

- **Purpose** – Organisations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure; and

- **Reasonableness** – Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Overview of Data Protection Regime

Technology-neutral **Principles based**

Individuals to be aware/notified and have consented to data activities

Data activities limited by consent and purpose – limiting collection, use and disclosure

Organizations' obligations to care for personal data

- Accuracy
- Protection
- Retention limitation
- Transfer limitation

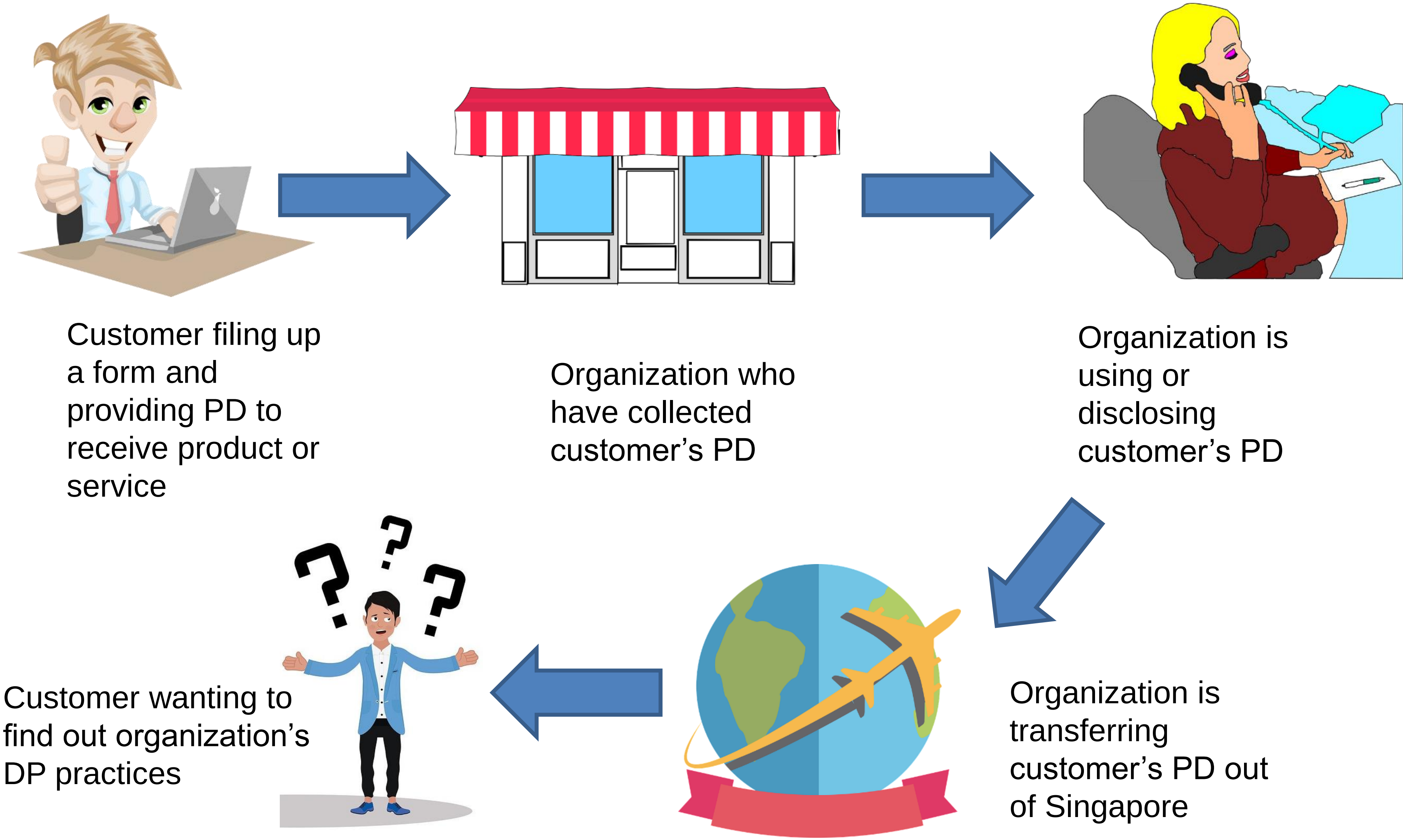
Organizations' accountability to individuals

- Openness (accountability and challenging compliance)
- Access and correction

Complaints-based regime

https://singaporelegaladvice.com/law-articles/personal-data-protection-act-obligations

Illustration – For Class Discussion



Customer filing up a form and providing PD to receive product or service

Organization who have collected customer’s PD

Organization is using or disclosing customer’s PD

Organization is transferring customer’s PD out of Singapore

Customer wanting to find out organization’s DP practices

Class Discussion

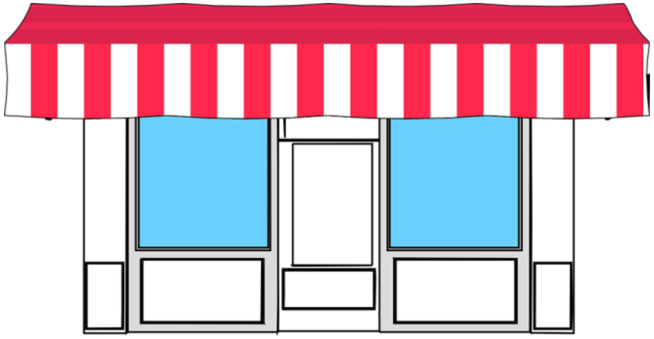
Customer filing up a form and providing PD to receive product or service

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.

Organisation must obtain Consent of the individual before collecting, using or disclosing his or her personal data for a purpose.

Organisation must state the Purpose for the collection, use or disclosure of personal data about an individual

Class Discussion



Organization who have collected customer's PD

Organisation must upon request, provide an individual Access to his/her 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.

Organisation 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.

Class Discussion

Organization is using or disclosing customer's PD

Organisation must make a reasonable effort to ensure that PD collected by or on behalf of the organisation is Accurate and complete if the PD 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 Protect PD in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar.

Organisation must Cease to Retain documents containing PD or remove the means by which the PD can be associated with particular individuals when there is no legal or business purposes.

Class Discussion

Organization is transferring customer's PD out of Singapore

Transferring organisation 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.

Class Discussion

Customer wanting to find out organization’s DP practices

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.

Case Studies

Case study 1:

Travel Agency A emailed a spreadsheet containing personal data of all individuals in the same tour group to certain of these individuals. The purpose of doing so was so that these individuals could use the spreadsheet as a supporting document for their travel insurance claims. While this was done at the request of those few individuals, the rest of the individuals had not consented to such disclosure of their personal data.

Unauthorised disclosure? What could the Agency have done instead?

Case Studies

- This disclosure is therefore unauthorised. Instead, Travel Agency A could ensure that:
  - Where customers request for the personal data, employees extract only the relevant information from the company database; and
  - Customers' personal data is sent separately to each requesting customer.

- Travel Agency A could also conduct regular training for its employees to keep them updated of such standard operating procedures.

Case Studies

Case Study 2:

Retail Company A sent a mass marketing email to all its subscribers. The recipients could see everyone else’s email addresses as the email addresses were put in the email’s “To” field. However, the subscribers had not authorised Retail Company A to disclose their email addresses to other subscribers.

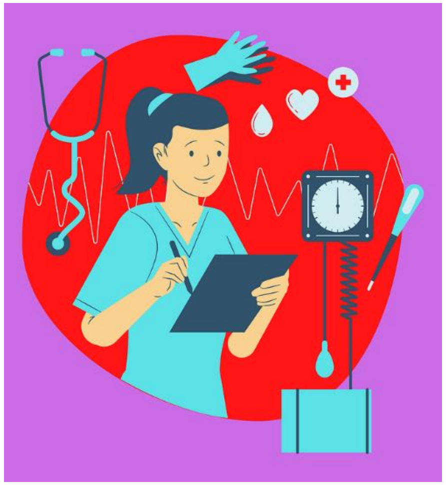
How could the retail company have prevented such unauthorized disclosure?

Case Studies

- To prevent subscribers' email addresses from being disclosed in such a manner, Retail Company A could:
  - Establish email procedures for recipients' email addresses to be put in the "BCC" field of emails; or
  - Use a group mailing list of undisclosed recipients when sending such mass emails.

- Retail Company A could also conduct regular training for its employees to keep them updated of such standard operating procedures.

Case Studies

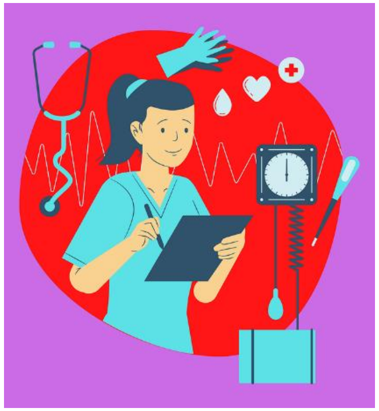


Case study 3:

Medical Clinic A wanted to send Laboratory B its patients' health records. However, as the email addresses of Laboratory B and client C began with the same few letters, the "To" field of the email was wrongly auto-completed with the email address of client C and not Laboratory B. The health records were therefore wrongly sent to client C.

What could the medical clinic have done to prevent such incidents from happening?

Case Studies



To prevent such a situation from arising in the future, Medical Clinic A could:

- Require employees to password-protect documents containing sensitive personal data (such as patients' health records);
- Disable its email software's email address auto-complete function;
- Require employees to double-check the recipient's email address before sending the email; and
- Configure its email software to delay the sending of emails by a few minutes after the employee has pressed the Send button, to allow emails to be recalled if necessary.

- Medical Clinic A could also conduct regular training for its employees to keep them updated of its standard operating procedures relating to the emailing of documents containing sensitive personal data.

Case Studies

Case study 4:
(The facts of this case study are based on Aviva Ltd,
a decision handed down by the PDPC in October 2017.)

- An employee of insurance company Aviva mailed letters containing a policyholder's personal data to the wrong address. Sensitive personal data, including the policyholder's NRIC and CPF account numbers, were disclosed to the wrong person as a result.

- During investigations, it was found that the only person checking the letters before they were mailed was the assigned processing employee. This constituted a "systemic weakness" in Aviva's letter-sending procedure.

- Due to the **absence of second-level checks**, Aviva was found to have failed to implement reasonable security measures to protect personal data, as required by the PDPA. It was fined $6,000.

Case Studies

Case Study 5: Simply throwing physical documents into the rubbish bin is not sufficient.

The PDPC has fined a financial consultant $1,000 for failing to properly dispose of his clients' policy-related documents. This was in view of how:

- The financial consultant had merely put the documents in a plastic bag, tied it up and placed it in a rubbish bin in a residential estate;
- The plastic bag did not have the effect of securing the documents, but merely concealed them; and
- The documents were unshredded and intact, and it was easy for others to open the plastic bag to retrieve the documents inside (and the personal data on them).

How to dispose of PD stored in electronic media?

Personal data in electronic media can be disposed of in 2 ways:

- **Physical destruction of the media itself to render stored data inaccessible:** e.g. cutting up CDs and DVDs, or smashing hard disks with a hammer until they no longer work (and cannot be repaired); or
- **Disposal of the personal data in the media only:** Specialised software tools can be used to securely erase all personal data contained in the media. Deleting files by simply moving them to the computer's "Recycle Bin" is insufficient as the files may still be recoverable (even after the "Recycle Bin" has been emptied).

Companies are free to choose their preferred method(s) of disposal, so long as the personal data contained in the medium cannot be recovered in part or full.

Other Points to Note re PDPA

- Companies are liable for their employee’s acts/breaches of PDPA
- Engaging external service providers to dispose of documents containing personal data does not relieve companies of their PDPA obligations to protect PD.

PDPC fines SingHealth for data breach

https://www.todayonline.com/singapore/pdpc-slams-singhealth-being-overly-dependent-ihis-metes-out-total-s1-million-fines-over?cid=h3_referral_inarticlelinks_03092019_todayonline (SingHealth)

Recent Personal Data leak by Singapore Accountancy Commission

singapore
accountancy
commission

https://www.straitstimes.com/singapore/singapore-accountancy-commission-accidentally-leaks-personal-data-of-6541-people?utm_source=STSmartphone&utm_medium=share&utm_term=2019-11-22+18%3A16%3A16

Do Not Call Registry

- The PDPA also provides for the establishment of a national **Do Not Call (DNC) registry**.
- The DNC registry will allow individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations.
- Note: *Email advertisements* (unsolicited commercial electronic messages) are regulated by the Spam Control Act Cap. 311A

Do Not Call Registry

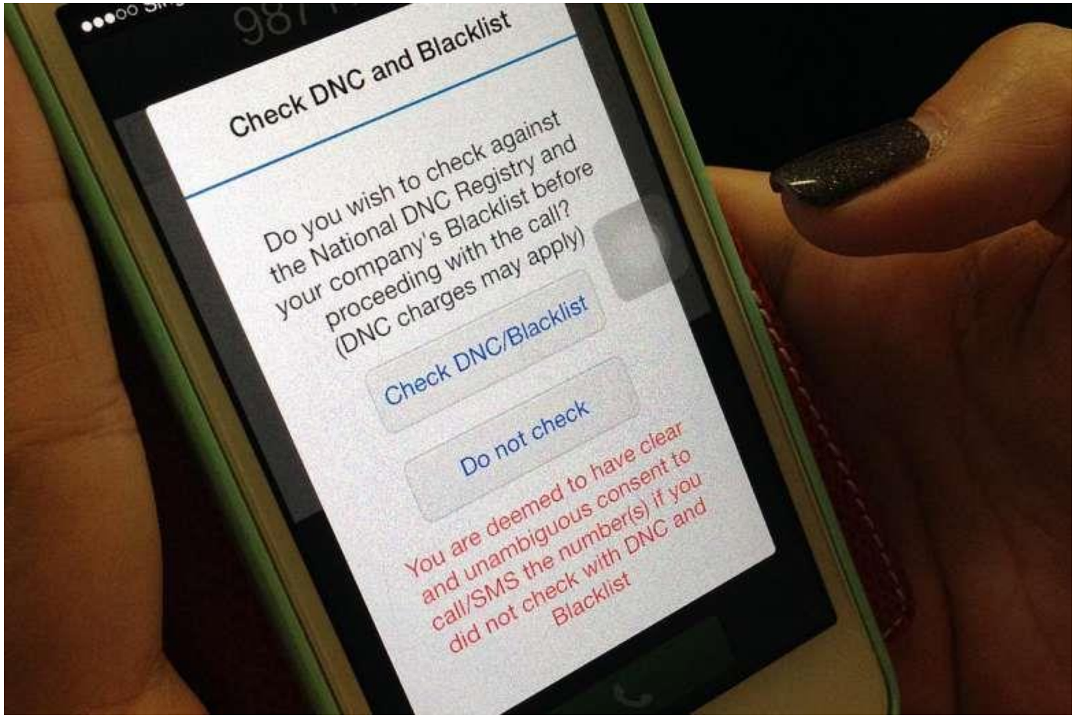
- Covered
  - B2C marketing messages
  - E.g. offer to supply, advertise or promote goods/services
  - Includes voice calls, SMS/MMS/Texts, Faxes

- Not covered
  - B2B marketing
  - Personal calls & SMSes
  - Market research/surveys
  - Messages by public agencies for non-commercial programmes
  - Does not include messages sent without use of phone numbers e.g. cell-broadcast

= Organizations obliged to check against DNC registry within 30 days before doing marketing unless they have clear and unambiguous consent in evidential form; display their ID, contact info and (for phone calls) originating number

= individual registers phone number with DNC registry (FOC), number added to DNC register(s) (voice calls, text messages and fax messages registers) & number remains in DNC register(s) unless individual deregisters or terminates service (i.e. registration does not expire; DNC registry will purge terminated phone numbers).

DNC effective?



Check DNC and Blacklist

Do you wish to check against the National DNC Registry and your company's Blacklist before proceeding with the call? (DNC charges may apply)

You are deemed to have clear and unambiguous consent to call/SMS the number(s) if you did not check with DNC and Blacklist

Photo by: Straits Times

https://www.straitstimes.com/singapore/do-not-call-registry-an-easy-guide-for-consumers (tuition agency charged by PDPC)

https://www.straitstimes.com/forum/letters-in-print/do-not-call-registry-does-not-appear-to-stop-unsolicited-messages-calls (ST forum letter)

https://www.youtube.com/watch?v=tcxDikKvIb8 (overview of PDPA)

End Of Lecture