C11 Data Protection

PDPA - Personal Data Protection Act (2012)

Purpose of PDPA

To govern the collection, use and disclosure of individuals' 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 purpose that a reasonable person would consider appropriate in the circumstances.

Source : http://www.pdpc.gov.sg

What is Personal Data?

Personal data is defined as data, *whether true or not*, about an **individual*** who can be identified –

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access.

If the collected data is false, or if the collected data has changed such that it is no longer true, such data will still be personal data.

* Individual is defined as a natural person (ie human being) whether living or **deceased**.

- PDPA only applies for a limited time of 10 years for the personal data of a deceased individual.

(Advisory Guidelines on Key Concepts in the PDPA, revised 9 Oct 2019 – section 5.1)

Examples of Personal Data

- Full Name
- NRIC or Passport number
- Personal mobile telephone number
- Facial image
- Voice recording (sufficiently clear and sufficient duration)
- Fingerprint
- Iris image
- DNA profile

The above is not an exhaustive list of unique identifiers. (Section 5.11)

Other possible unique identifiers:

- home or email address
- location data
- Internet Protocol (IP) address

Whether any data or dataset constitutes personal data would depend on the specific facts of each case. Data or datasets that may identify an individual in a certain situation may not identify an individual in another situation. (Section 5.13)

Example: Dataset comprising data points which, individually, cannot identify a particular person

Organisation DEF conducts a street intercept survey and collects the following information from passers-by:

- Age range
- Gender
- Occupation
- Place of work

Although each of these data points, on its own, would not be able to identify an individual, Organisation DEF should be mindful that the dataset, comprising a respondent's age range, gender, occupation and place of work may be able to identify the respondent.

Respondent A is a female individual who is between 20 and 30 years of age, and works as a retail salesperson at Orchard Road. This dataset may not be able to identify Respondent A since there could be many female salespersons in their 20s working in retail outlets at Orchard Road.

Respondent B is a male individual who is between 20 and 30 years of age, and works as a security officer at Bencoolen Street. This dataset may be able to identify respondent B if there are no other male security officers in their 20s working at Bencoolen Street.

Given that some of the respondents' datasets are likely to identify the respondents, Organisation DEF should treat the datasets as personal data and ensure they comply with the Data Protection Provisions.

PDPA Milestones:

- **6 Nov 2009 –** Madrid Resolution: International Standard on Protection of Personal Data and Privacy by ICDPPC adopted by more than 50 countries.
- **15 Oct 2012 –** Singapore parliament passed the Personal Data Protection Act (PDPA).
- **2013 –** Personal Data Privacy Commission (PDPC) was established to promote awareness, administering and enforcing the PDPA.
- **2 Jan 2014 –** DNC Registry enforced
- **1 Sept 2019 –** New NRIC guidelines enforced
- **25 May 2018 –** The European Union (EU) General Data Protection Regulation (GDPR) was enforced.

YouTube : What is GDPR? A summary of the EU GDPR

How does PDPA helps me as an individual?

- Protect my privacy
- Prevent Fraud and Cyber Attacks
- Avoid unsolicited advertisements and nuisance calls/messages

Myths about PDPA

- PDPA only concerns big organisations, companies and online businesses. It does not concerns me because I am just an individual.

1. Obtain consent from individual.
2. Tell the individual the purpose.
3. Collect the minimum data.
4. Use it for the purpose it was collected.
5. Protect your files with strong password.
6. Destroy the data when it is no longer needed for its original purpose.

PERSONAL DATA PROTECTION ACT https://youtu.be/P-CVvjd8nKk

Key Obligations of PDPA

- Prevent unauthorised access, collection, use, disclosure or similar risks
- Electronic data must be password protected or encrypted, especially before sending out any email containing personal data
- Physical data should be kept under lock and key
- Reveal Personal Data on a need to know basis only

1. **Consent Obligation**
2. **Protection Obligation**
3. **Retention Obligation**
4. **Transfer Limitation**

Consent + Purpose
→ Valid Consent

Before disclosing the Personal Data:
- ensure you have obtained the consent;
- ensure the recipient signs a Letter of Undertaking.

Once the Personal Data is no longer required for the original purpose, delete or cease the retention of the data.

[9 Main Data Protection Obligations (DP Starter Kit p3-4)]


HOWEVER, PDPA IS NOT APPLICABLE TO GOVERNMENT MINISTRIES AND PUBLIC AGENCIES DURING COURSE OF DUTY
CREATED USING POWTOON

INCLUDING

HOUSING & DEVELOPMENT BOARD

URBAN REDEVELOPMENT AUTHORITY

To make Singapore a great city to live, work and play

Land Transport Authority

"Is it justifiable for public agencies to be exempted from the PDPA?"

- query by NMP Irene Quay during Parliament on 1 Apr 2019.

- There are fundamental differences in how the public sector operates compared to the private sector.
- The public sector agencies have to comply with Government Instruction Manuals and the Public Sector (Governance) Act (PSGA).
- Collectively, these provide comparable, if not higher, standards of data protection compared to the PDPA, he said, adding that similar investigations and enforcement actions are taken against data security breaches.

- reply by Minister for Communications and Information, S Iswaran.

Public agencies must not abuse their authority for personal reasons

What so 'serious' about Personal Data?

Drones of the Future are HERE!

AI, Autonomous Weapons

https://youtu.be/TlO2gcs1YvM

Effort to ban lethal autonomous weapons (https://autonomousweapons.org/)

Enforcement by PDPC https://www.pdpc.gov.sg/Commissions-Decisions?page=1

- Breach of the Consent, Notification, Protection, Accuracy, Accountability, Retention, Openness, Access, Purpose and Transfer Limitation Obligations
- Decision: Warning, Directions, Financial Penalty
- Since 21 April 2016

Organisation	Penalty	Date
IHiS	$750,000	15 Jan 2019
SingHealth	$250,000	15 Jan 2019
Ninja Logistics	$90,000	04 Nov 2019
Learnaholic	$60,000	05 Dec 2019
Horizon Fast Ferry	$54,000	02 Aug 2019
K Box Entertainment	$50,000	21 Apr 2016
Amicus Solutions	$48,000	10 Oct 2019
Marshall Cavendish Education	$40,000	04 Nov 2019

- AXA, Income, AIA, Aviva Insurance
- Singtel, NHG, SAFRA, SPH, TTSH, PCF, MyRepublic, NUS
- Genki Sushi, GrabCar, COURTS, 4 Hair Salon, Taekwondo Federation, Hazel Florist & Gifts, Comfort and CityCab, Metro, Challenger, Royal Caribbean Cruises, EU Holidays ...

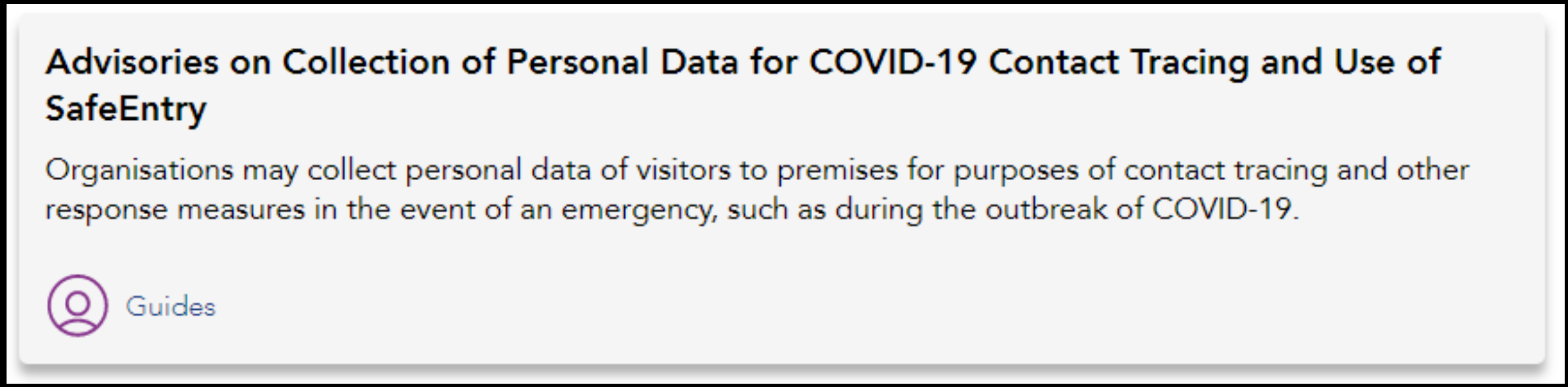
Interesting Cases:

- K Box Entertainment Group : Unauthorised disclosure of 317,000 members' personal data.
- Marshall Cavendish Education : Teaching materials and user data on the 11 servers and network storage devices for the Learning Management System (LMS) were encrypted by ransomware.
- Advance Home Tutors : A freelance web developer stored all the tutors' educational certificates in a public 'image' directory and coding script did not include necessary validation condition check before disclosure.
- SMU Alumni Association : Any person with the FIN or NRIC number of an applicant would have been able to access the personal data of that applicant through its publicly accessible webpage.
- A Former Financial Consultant : Failing to take reasonable security measures to protect the personal data of his clients when disposing the physical insurance documents.
- An Individual Selling Personal Data : Buying 'leads' from unknown online sellers for telemarketing and re-selling the 'leads' multiple times subsequently.

How do I know if I or my company comply with PDPA?

- Is there a Data Protection Officer (DPO) to advice you on the main obligations of PDPA?
- Is there a work process for collection NRIC/FIN or other personal data?
- Is there a Standard Operating Procedure (SOP) for staff handling personal data?
- Is there a Data Protection Management Programme (DPMP) in the organisation?
- and more ...

Latest updates on Data Protection during COVID-19 ...



https://www.pdpc.gov.sg/help-and-resources/2020/03/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing

Welcome to the Do Not Call (DNC) Registry

Since 2 Jan 2014

Consumer - Register Your Phone Number

Consumers who do not wish to receive telemarketing messages via phone call, SMS or fax, can register their Singapore telephone numbers with the DNC Registry. This applies to home, office and mobile numbers. Registration is free and does not expire. *Read More*

Click *here* to view the DNC Registry User Guide for Consumers.
Click *here* for FAQ.
Click *here* to lodge a complaint for unsolicited telemarketing message.

Organisation - Check the Registry Before You Do Telemarketing

With effect from 2 January 2014, Organisations must check with the DNC Registry to ensure that the Singapore telephone numbers that they are sending telemarketing messages to, are not listed in the Registry. *Read More*

Click *here* to view the DNC Registry User Guide for Organisations.
Click *here* for FAQ.
Click *here* to find out more about CorpPass.

Register Online

Click here to add or remove your phone number

Register by SMS

Send an SMS with the message '**DNC**' to 78771

Click here to find out more

Register by Phone

Call our toll-free number 1800 248 0771

Click here to find out more

Apply for a DNC Checking Account

Click here to apply for an account to check phone numbers before sending telemarketing messages

Login with CorpPass

For organisation registered in Singapore

Login with SingPass

For individual person

Login with DNC User ID

For organisation registered overseas

Duty to check the DNC Registry

1. A person* who intends to send a specific message to a Singapore telephone number must check with the DNC Registry or obtain a clear and unambiguous consent to the sending the message.

   * a sender who is *in an ongoing relationship with the individual* may be exempted.

2. A Direct Marketing firm using a list of Singapore numbers from a third party source could obtain the evidence of consent from this third party or obtain the consent directly from the individuals for sending the marketing materials/messages.

3. An individual may withdraw any consent given by giving a notice of withdrawal and the sender, and its agents, must cease sending messages to the individual.

Advisory Guidelines on the DO NOT CALL Provisions (revised 27 July 2017) – Part III

Do Not Call (DNC) Registry (dnc.gov.sg)

DNC Registry Figures

Summary

As at end March 2020

- Consumer Numbers Registered: 1,114,049
- Organisation Accounts Created:10,200
- Numbers Checked by Organisations: 2.83 billion

- https://www.pdpc.gov.sg/help-and-resources/2020/04/dnc-registry-figures

After 5 years of DNC Registry, can more be done to stop persistent nuisance calls, messages?

Advisory Guidelines for NRIC*

NRIC numbers are a permanent and irreplaceable identifier issued by the Singapore Government primarily for public administration purposes and to facilitate transactions with the Government.

With effect on 1 Sept 2019, private sector organisations are only allowed to collect, use or disclose NRIC numbers or copies of the NRIC if:

- The collection, use or disclosure is required by the law; or
- It is necessary to establish or verify an individual's identity to a high degree of accuracy.

In addition, an individual's physical NRIC, or other identification documents containing NRIC numbers or other national identification numbers, can only be retained by an organisation if required by law. The checking of the physical NRIC, Foreign Identity card or passport is allowed if the organisation needs to verify an individual's particulars.

* The same treatment extends to Birth Certificate numbers, Foreign Identification Number (FIN), Work Permit numbers, Passport and other National Identification Numbers

Technical Guide to Advisory Guidelines on NRIC Numbers (dated 26 Aug 2019)

Advisory Guidelines on the PDPA for NRIC and Other National Identification Numbers (31 Aug 2018)

Key considerations for choosing a replacement identifier for NRIC numbers

- Be easily remembered by the user
- Must be unique to be used in the system database
- Does not contain sensitive personal information
- Cannot be easily guessed by others

Alternatives to using NRIC as an Identifier:

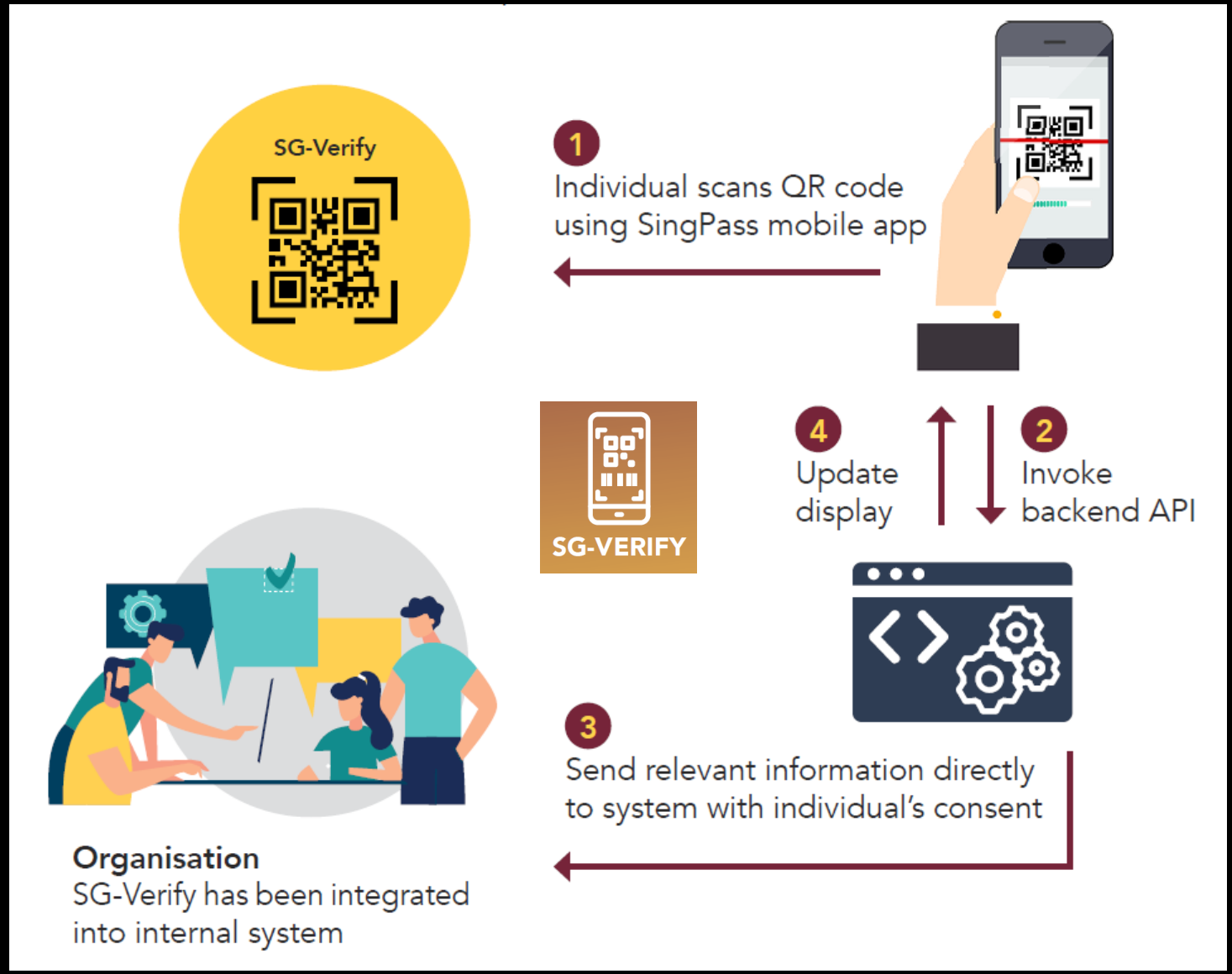
- User selected username
- Organisation auto-generated identifiers
- Email address or mobile number* (must validate, allow user to change)
- Combination of identifiers (should not contain sensitive personal info)
- Partial NRIC number (eg yijc567A)

* must include a process to manage the situation when a user uses a recycled old mobile no.

1. Check at registration that the new identifier has not been used.
2. Check that it meets the organisation's system requirements, eg the length or the use of special characters.
3. Include option for user to request for username to be sent to the user's email or mobile no.

SG-Verify by GovTech

- Organisation can verify the user's identify with SingPass
- Organisation need not handle the identification documents, both physically or electronically.
- Relevant personal data, or partial NRIC numbers, will be securely transferred to the organisation.



The End