

## Media Release

### For Immediate Release

# PDPC REMINDS ORGANISATIONS ON NRIC ADVISORY GUIDELINES COMPLIANCE DEADLINE

*Organisations should not indiscriminately collect, use or disclose NRIC numbers  
from 1 September 2019*

**SINGAPORE – 26 August 2019:** The Personal Data Protection Commission (“**PDPC**”) today reminded organisations not to indiscriminately collect, use, retain or disclose National Registration Identity Card (“**NRIC**”) and other national identification numbers from 1 September 2019, when the updated NRIC Advisory Guidelines (“**NRIC AG**”) take effect.

Organisations have been given a year to prepare themselves to comply with the updated NRIC AG, announced in August 2018.

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. As NRIC numbers can be used to retrieve data relating to individuals, there is a need to reduce indiscriminate or unjustified collection and negligent handling of NRIC numbers.

Accordingly, the PDPC has been encouraging organisations to use alternative identifiers according to their business and operational needs and avoid excessively collecting other personal data as substitutes to NRIC numbers. Organisations are also advised to put in place security measures such as password protection and two-factor authentication.

Organisations can also consider using the SG-Verify service, which is an in-built feature of SingPass Mobile that enables faster identity verification checks and secure data transfer through QR Code scanning.

Under the updated NRIC AG, private sector organisations are not allowed to collect, use or disclose NRIC numbers or copies of the NRIC unless:

- 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.

The same treatment extends to Birth Certificate numbers, Foreign Identification Numbers and Work Permit numbers. While passport numbers are periodically

replaced, organisations should avoid collecting the full passport numbers of individuals unless justified as well.

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.

Where the collection, use and/or disclosure of NRIC numbers or retention of physical NRICs is permitted, organisations must ensure that adequate security protection measures are in place to safeguard the personal data in their possession or under their control, in compliance with their obligations under the Personal Data Protection Act ("PDPA").

To help organisations comply with the updated NRIC AG, the PDPC and the Infocomm Media Development Authority ("IMDA"), have developed and made available the following resources:

- A technical guide on how organisations can replace NRIC collection with alternative identifiers such as customer IDs. The guide has been updated with information on SG-Verify;
- Pre-approved solutions available on the SME Portal's Tech Depot for functions such as visitor management, point of sales and customer relationship management; and
- New template notices which commercial and residential buildings can put up for visitor management.

Organisations may also refer to a list of Frequently Asked Questions on this topic, such as when organisations should consider using partial NRICs as an alternative identifier, and what they should do with existing documents and databases containing NRIC data. These can be found at [www.pdpc.gov.sg/NRIC-faqs](http://www.pdpc.gov.sg/NRIC-faqs). Citizens and organisations can also refer to a listing of relevant legislations requiring the collection of NRIC numbers at [www.pdpc.gov.sg/NRIC-Extracts](http://www.pdpc.gov.sg/NRIC-Extracts).

Organisations found in breach of the PDPA may face financial penalties of up to S\$1 million. For more information on the NRIC AG, please visit [www.pdpc.gov.sg/AG](http://www.pdpc.gov.sg/AG)

## **Annex A: Factsheet on Summary of Updated Advisory Guidelines on NRIC and Other National Identification Numbers**

---

ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

---

***About Personal Data Protection Commission (PDPC)***

*The PDPC administers the Personal Data Protection Act 2012 (PDPA) in Singapore, which aims to safeguard individuals' personal data against misuse and promote proper management of personal data in organisations. The PDPA enhances Singapore's competitiveness and strengthens our position as a trusted business hub, among the leading jurisdictions in data protection. For more information, please visit [www.pdpc.gov.sg](http://www.pdpc.gov.sg).*

For media queries, please contact:

Mr Eugene Neubronner  
Manager, Communications and Marketing  
Personal Data Protection Commission  
c/o Info-communications Media Development Authority  
Tel: 6211 1182  
E-mail: [eugene\\_neubronner@imda.gov.sg](mailto:eugene_neubronner@imda.gov.sg)

Mr Chua Hian Hou  
Deputy Director, Communications and Marketing  
Personal Data Protection Commission  
c/o Info-communications Media Development Authority  
Tel: 6202 4956  
E-mail: [chua\\_hian\\_hou@imda.gov.sg](mailto:chua_hian_hou@imda.gov.sg)

## ANNEX A FACTSHEET

### SUMMARY OF UPDATED ADVISORY GUIDELINES ON NRIC NUMBERS AND OTHER NATIONAL IDENTIFICATION NUMBERS

Organisations are not allowed to collect, use or disclose an individual's NRIC number (or copy of an NRIC), unless under the following circumstances:

- 1) Where it is required under the law (or an exception under the PDPA applies);  
or
- 2) Where it is necessary to establish or verify the identity of the individual to a high degree of accuracy.

#### **1a. Where it is required under the law**

The following are some examples of situations where the collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law. As good practice, organisations should still notify individuals of the purpose for doing so.

##### **Example: Subscribing to a mobile telephone line**

Mr X would like to sign up for mobile phone service with telecommunication company ABC. ABC asks Mr X to provide his NRIC details when signing up for the subscription, and proceeds to keep a record or scanned copy of his NRIC.

ABC may do so, as it is required by law to comply with its licence conditions to maintain a register of subscribers as evidence of identity for the provision of mobile services.

#### **1b. Where an exception under the PDPA applies**

There could also be situations where there is an applicable exception under the PDPA, such that consent is not required. Organisations must still ensure that their conduct is reasonable in the circumstances.

##### **Example: Disclosure of NRIC numbers without consent in an emergency situation**

Mr Y at medical centre ABC is unconscious after sustaining a fall and has to be admitted to the hospital. The staff at the centre can provide the hospital with Mr Y's

personal data including his name, NRIC number and medical allergies, without his consent, as there is an applicable exception in the PDPA about responding to an emergency that threatens a persons' health.

## **2. Necessary to establish or verify the identity of the individual to a high degree of accuracy**

Organisations may collect, use or disclose individuals' NRIC numbers (or copies) where it is necessary to establish or verify the identity of an individual to a high degree of accuracy, for instance:

- i) Where failing to do so may pose a significant safety or security risk; or
- ii) Where failing to do so may pose a risk of significant impact or harm to an individual and/or the organisation. Examples could include transactions relating to healthcare, financial or real estate matters, such as property transactions, insurance claims, or entrance to high-security zones.

When collecting the NRIC number (or a copy), organisations should be able to explain – on the request of either the individual or the PDPC - as to why the collection, use or disclosure is necessary to establish or verify the identity of an individual to a high degree of accuracy. The PDPC does not consider it a collection of personal data where there is no intention to obtain control or possession of the physical NRIC beyond checking the NRIC, and where no personal data will be retained once the NRIC is returned.

### **Example: Verifying age of a customer who wishes to purchase tobacco**

Mr Z would like to purchase a packet of cigarettes at a convenience store. The cashier requests for a proof of identity (such as his NRIC or driving license) to check Mr Z's date of birth and determine if he meets the minimum legal age for the purchase of tobacco.

As there are no other viable alternatives for verifying the customer's age, the convenience store is allowed to request Mr Z to produce one such identification document for this purpose.

## Alternatives to NRIC numbers or storing a copy of the NRIC

Organisations should consider alternative unique identifiers to meet their needs in place of collecting NRIC numbers or keeping copies of the NRIC. Some substitutes include organisation/user-generated IDs, tracking numbers, or email addresses.

Organisations should also consider whether the substitute options are reasonable, and avoid over-collecting other forms of personal data as an alternative to NRIC numbers.

The following examples illustrate scenarios where the collection, use or disclosure of NRIC numbers (or copies) as well as the retention of physical NRICs, is not required under the law, and some alternatives that organisations may consider adopting:

### **Example: Registering interest in a product and submitting feedback**

Retail store ABC is releasing a new product for sale next month. To ensure that priority is given to interested buyers, the store allows customers to register their interest in advance. The store also allows individuals to submit feedback regarding its store catalogue.

The store is not allowed to collect NRIC numbers to track interest in its new product or for receiving feedback from customers. Instead, it can use alternatives such as names, mobile numbers or email addresses.

### **Example: Online purchase of movie tickets**

Cinema ABC wishes to verify the identity of customers who purchased movie tickets online, to ensure tickets are issued to the right customers during collection.

The cinema is not allowed to collect NRIC numbers for this purpose. The cinema could consider other appropriate means of verification, such as through a booking reference number or an SMS confirmation.

### **Example: Establishing identity of visitors to a private condominium**

Condominium ABC wants to record the identity of visitors as part of providing security to the residents. ABC could record the visitor's full name, mobile number and partial NRIC number, checking against the visitor's NRIC or other photo identification.

ABC could also adopt visitor management systems that store such information electronically and is protected by passwords instead of an open visitor log book.