

Media Release

Embargoed until Friday, 31 August, 10am

PDPC ISSUES NRIC ADVISORY GUIDELINES TO ENHANCE CONSUMER PROTECTION

Organisations must implement changes by 1 September 2019

SINGAPORE – 31 August 2018: The Personal Data Protection Commission (PDPC) today issued its updated Advisory Guidelines to enhance consumer protection against the indiscriminate or unjustified collection, use and disclosure of individuals' National Registration Identity Card (NRIC) numbers and retention of physical NRICs.

The NRIC number is a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to an individual. In today's Digital Economy, indiscriminate collection or negligent handling of NRIC numbers can increase the risk of unintended disclosure and may result in NRIC numbers being used for illegal activities such as identity theft or fraud.

Under the updated Advisory Guidelines, organisations are not allowed to collect, use or disclose NRIC numbers or copies of the NRIC except under certain specific circumstances. These circumstances are: if the collection, use or disclosure is required by the law; or it is necessary to accurately establish or verify an individual's identity to a high degree of fidelity.

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.

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.

Where the collection, use and disclosure of NRIC numbers or retention of physical NRICs is permitted, organisations must ensure that adequate 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).

All organisations are required to comply with the above with effect from **1 September 2019**.

The PDPC developed the updated guidelines in consultation with consumers and businesses over a six-week period from 7 November 2017 to 18 December 2017¹. The PDPC received strong support for its proposals.

Organisations are encouraged to assess the suitability of identifiers used in place of NRIC numbers according to their business and operational needs. In addition, they should consider whether the alternatives provided are reasonable, and avoid collecting excessive personal data as alternatives to NRIC numbers. The PDPC recognises that some organisations may require time to review and assistance to implement changes to their practices to comply with the updated guidelines. The PDPC and the Infocomm Media Development Authority (IMDA) will help organisations make the transition by:

- Publishing a technical guide² which provides organisations with guidance on replacing the NRIC number with alternative identifiers for websites and public facing computer systems;
- Identifying pre-approved technology solutions such as visitor management systems; point of sales; and customer relationship management systems, through the SME Portal's Tech Depot, to help organisations automate and align their operations with the updated Advisory Guidelines³; and
- Developing template notices⁴ that organisations can use to manage customer expectations during the transition period.

More details of the updated Advisory Guidelines can be found on www.pdpc.gov.sg/AG.

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

ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

About Personal Data Protection Commission

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, putting Singapore on par with the growing list of countries with data protection laws. For more information, please visit www.pdpc.gov.sg.

¹ The public consultation closed on 18 December 2017 with 82 responses from individuals and organisations from various sectors, including retail, media and finance. Please refer to the PDPC's Closing Note for more information on the consultation.

² The technical guide can be found at www.pdpc.gov.sg/og

³ For more information on the pre-approved solutions, please visit: <https://www.smeportal.sg/content/tech-depot/en/psg.html>

⁴ The template notices can be found at www.pdpc.gov.sg/org-resources



PERSONAL DATA
PROTECTION COMMISSION
S I N G A P O R E

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

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

ANNEX A

FACTSHEET

SUMMARY OF ADVISORY GUIDELINES ON NRIC NUMBERS

In general, 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 accurately establish or verify the identity of the individual to a high degree of fidelity.

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 license 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 accurately establish or verify the identity of the individual to a high degree of fidelity

Organisations may collect, use or disclose individuals' NRIC numbers (or copies of NRIC) with due notification and consent where it is necessary to accurately establish or verify the identity of an individual to a high degree of fidelity, 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 include transactions relating to healthcare, financial or real estate matters, such as property transactions, insurance applications and claims.

When collecting the NRIC number (or copy of the NRIC), organisations should be able to provide justification – on the request of either the individual or the PDPC - as to why the collection, use or disclosure is necessary to accurately establish or verify the identity of an individual to a high degree of fidelity. 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 alternatives 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 of NRIC) 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 as 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.