ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS

Issued 31 August 2018

TABLE OF CONTENTS

PART I: INTRODUCTION 2
1 Background 2
2 Overview of the Data Protection Provisions 3
PART II: APPLICATION OF DATA PROTECTION PROVISIONS 5
3 Collection, use or disclosure of NRIC numbers (or copies of NRIC) 5
4 Retention of Physical NRIC 9
5 Alternatives to NRIC 10
PART III: IMPLEMENTATION 14
6 Implementation timeframe 14

PART I: INTRODUCTION

1 Background

1.1 These Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines"[1].

1.2 The Singapore National Registration Identification Card ("NRIC") number is a unique identifier assigned by the Singapore Government to Singapore citizens and permanent residents of registrable age under the National Registration Act. It is often used for transactions with the Government as well as in commercial transactions. The NRIC number of an individual is considered personal data as the individual can be identified from the unique sequence of numbers and letters.

1.3 As the NRIC number is a permanent and irreplaceable identifier which can potentially be used to unlock large amounts of information relating to the individual, the collection, use and disclosure of an individual's NRIC number is of special concern. Indiscriminate or negligent handling of NRIC numbers increases the risk of unintended disclosure with the result that NRIC numbers may be obtained and used for illegal activities such as identity theft and fraud. The retention of an individual's physical NRIC is also of concern. The physical NRIC not only contains the individual's NRIC number, but also other personal data, such as the individual's full name, photograph, thumbprint and residential address.

1.4 These Guidelines clarify how the Personal Data Protection Act 2012 ("PDPA") applies to organisations' collection, use and disclosure of NRIC numbers (or copies of NRIC), and retention of physical NRICs[2] by organisations. Under the updated Guidelines, organisations are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC). The treatment for NRIC numbers also applies to Birth Certificate numbers, Foreign Identification Numbers ("FIN") and Work Permit numbers, collectively referred to in these Guidelines as 'other national identification numbers'.

1.5 While passport numbers are periodically replaced, they too are important identification numbers that can serve the same purposes as the NRIC, FIN, Work Permit and Birth Certification numbers. Therefore, organisations should accord passports similar treatment as that for NRICs, i.e. refrain from collecting passport numbers. If there is a need to collect passport numbers, organisations should limit their collection to partial passport numbers and ensure an appropriate level of security to protect the passport numbers collected.

[1] Available at https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Main-Advisory-Guidelines
[2] To be clear, 'NRIC' refers to both pink and blue NRIC.

1.6 The treatment for retention of physical NRIC applies to other identification documents containing the NRIC numbers or other national identification numbers (e.g. driver's licence, passport and work pass).

1.7 These Guidelines do not apply to the collection, use and disclosure of NRIC numbers (or copies of NRIC), and the retention of physical NRICs by a public agency or an organisation that is acting on behalf of a public agency. Public agencies in Singapore (including Government Ministries, Statutory Boards and Organs of State) are excluded from the Data Protection Provisions of the PDPA[3].

2 Overview of the Data Protection Provisions

2.1 Organisations are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC). Where organisations are permitted to collect NRIC numbers of individuals, they will nevertheless have to comply with the Data Protection Provisions under the PDPA. The Data Protection Provisions of the PDPA contain a number of obligations which are elaborated in the PDPC's Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines").

2.2 Among other obligations, the PDPA requires organisations to develop, implement and regularly review their policies and practices that are necessary to meet their obligations under the PDPA.

2.3 The Consent[4], Notification[5] and Purpose Limitation[6] obligations require organisations to notify an individual of the purposes for the collection, use and disclosure of his or her personal data, including NRIC number, and obtain his or her consent, unless it is required under any law or an exception[7] under the PDPA applies. In situations where an individual voluntarily provides his or her personal data to an organisation for a purpose and it is reasonable[8] that he or she would voluntarily provide the data, the individual is deemed to consent to the collection, use or disclosure of the personal data.

---

[3] The Data Protection Provisions are found in Parts III to VI of the PDPA. Section 4(1)(c) of the PDPA provides that Parts III to VI shall not impose any obligation on any public agency or organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data.
[4] Sections 13 to 17 of the PDPA.
[5] Section 20 of the PDPA.
[6] Section 18 of the PDPA.
[7] Please refer to the Second, Third and Fourth Schedules under the PDPA for exceptions which may apply.
[8] Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes – (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable.

2.4 The Protection[9] obligation requires organisations to make reasonable security arrangements to protect personal data in its possession or under its control. The sensitivity and potential adverse impact to the individual of any unauthorised use or disclosure of his or her NRIC number must be taken into consideration in determining whether an organisation's collection, use or disclosure of NRIC numbers meet the requisite standard of reasonableness. Given the risks and potential impact of any unauthorised use or disclosure of personal data associated with the individual's NRIC number, organisations are expected to provide a greater level of security to protect NRIC numbers (or copies of NRIC) in the possession or under the control of the organisations. Organisations may wish to consider employing technological solutions, such as scanning of physical NRICs into software systems to capture NRIC numbers and store the data in a secure manner.

2.5 Under the Retention Limitation[10] obligation, organisations must cease to retain documents containing personal data, or to remove the means by which the personal data can be associated with particular individuals, as soon as the purpose for which the personal data was collected is no longer served by the retention of the personal data, and retention is no longer necessary for business or legal purposes. The PDPA does not prescribe a specific retention period for personal data. Organisations should regularly review the NRIC numbers (or copies of NRIC) in their possession or under their control to determine if the data is still needed, and should not keep the data "just in case" when it is no longer necessary for the purposes for which the personal data was collected or for any legal or business purpose.

2.6 Please refer to the Key Concept Guidelines for more details on the Data Protection Provisions of the PDPA.

2.7 The following sections outline the application of some of the Data Protection Provisions to NRIC numbers (or copies of NRIC). They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. Organisations that collect, use or disclose NRIC numbers (or copies of NRIC) should ensure that their policies specifically address the need to do so and that their processes are designed to ensure that these NRIC numbers (or copies of NRIC) are sufficiently protected.

[9] Section 24 of the PDPA.
[10] Section 25 of the PDPA.

PART II: APPLICATION OF DATA PROTECTION PROVISIONS

3 Collection, use or disclosure of NRIC numbers (or copies of NRIC)

3.1 Organisations are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC). They may do so only in the following specified circumstances:

a) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA applies); or

b) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA applies)

3.2 Organisations may collect, use or disclose an individual's NRIC number (or copy of NRIC) without his or her consent if it is required under the law[11]. As good practice, organisations should still notify the individual of the purpose for the collection, use or disclosure, as the case may be.

3.3 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.

3.4	**Example: Seeking medical treatment at a General Practitioner clinic** Siti would like to seek medical treatment at a General Practitioner Clinic XYZ. Clinic XYZ requires Siti to provide her physical NRIC when she registers with the clinic as a patient, for the purpose of identifying her and collecting her NRIC number and other personal details required to maintain accurate, complete and up-to-date medical records. For subsequent visits, Siti may also be required to provide her NRIC for verification purposes.

[11] Section 13(b) of the PDPA provides that an organisation shall not collect, use or disclose personal data unless with the individual's consent or if the collection, use or disclosure without consent is required or authorised under the PDPA or any other written law. Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law.

	All healthcare institutions need to carry out proper documentation and accurate verification of a patient's identity to ensure that medical care and treatment is provided to the right patient. The requirement to maintain accurate, complete and up-to-date medical records for the purposes above is supported by regulations 12(1) and (1A)(a) of the Private Hospitals and Medical Clinics Regulations. Clinic XYZ may obtain the information contained in Siti's NRIC where it is required for compliance with the regulations.
3.5	**Example: Checking into a hotel** Charlotte has booked a room to stay at Hotel ABC. Hotel ABC requires Charlotte to provide her NRIC number upon check-in as a record of her identity. Under regulation 27(1) of the Hotels Licensing Regulations, every hotel must require every guest seeking accommodation in the hotel to furnish the full name and identification number in the NRIC[12] held by the guest. Regulation 27(3) further provides that every guest must furnish such particulars when required to do so by the hotel. Hotel ABC may obtain the full name and NRIC number contained in Charlotte's NRIC where as required for compliance with the regulations.
3.6	**Example: Subscribing to a mobile telephone line** Shankar would like to sign up for mobile phone service with Telecommunication Company ABC. Telecommunication Company ABC requires Shankar to provide his NRIC details when signing up for the mobile phone subscription as it needs to maintain a register of subscribers as required under its licence conditions for the provision of mobile services. The licences issued under S(5) of the Telecommunications Act require telecommunication companies who provide mobile phone services to collect their customers' NRIC information and keep a copy of the NRIC as evidence of identity, among other documents. Telecommunication Company ABC may obtain the information contained in Shankar's NRIC where it is required for compliance with the licence conditions.

[12] The full name, nationality and identification assigned to the passport or other travel or personal identification document will be required.

3.7	**Example: Receiving massage services at a massage establishment** Alvin wishes to obtain massage services at Massage Establishment ABC. Massage Establishment ABC requires Alvin to furnish details of his NRIC number, which will be recorded in a client register. R14 of the Massage Establishments Rules 2018 under the Massage Establishments Act states that before providing any massage services to any individual seeking massage in an establishment for massage, the licensee of the establishment for massage must require the individual to furnish his or her identity card number or the particulars of his or her passport or other travel document. The licensee must enter the particulars in a register, and keep the records for at least a year. Massage Establishment ABC is allowed to obtain Alvin's NRIC number since it is required for compliance with the regulations.
3.8	**Example: Enrolling into a private education institution** Cathy wishes to enrol into Private Education Institution XYZ. Private Education Institution XYZ requires Cathy to provide her NRIC number during enrolment. Under regulation 21(1)(c)(ii) of the Private Education Regulations, registered private education institutions are required to keep proper records of their enrolled students' NRIC number, amongst other information. Private Education Institution XYZ may obtain Cathy's NRIC number where it is required for compliance with the regulations.
3.9	**Example: New employee joining an organisation** Benny wishes to apply for a job with Organisation XYZ and fills in a job application form. The application form does not require Benny to provide his NRIC number. Subsequently, when Organisation XYZ wishes to hire Benny, it requires Benny to provide his NRIC number, among other information, for its employment records. Under section 95 of the Employment Act, all employers must maintain detailed employment records of employees covered by the Employment Act, which includes employees' NRIC number and other relevant information.

	Organisation XYZ may obtain Benny's NRIC number where it is required for compliance with the Employment Act. There is no requirement under the law to ask for NRIC numbers for the purpose of job applications.

3.10 In addition, there could be situations where there is an applicable exception under the Second, Third or Fourth Schedule of the PDPA such that the consent of the individual to collect, use or disclose his or her NRIC number (or copy of NRIC) is not required. Nonetheless, organisations must still ensure that its conduct is reasonable in the circumstances.

3.11	**Example: Disclosure of NRIC numbers without consent in an emergency situation** An individual at Medical Centre ABC becomes unconscious after sustaining a fall at the centre and has to be admitted to hospital. The staff at the Centre provides the hospital with the individual's personal data including his name, NRIC number and medical allergies, without his consent as there is an applicable exception[13] in the Fourth Schedule to the PDPA for the disclosure of an individual's personal data, without consent, that is necessary to respond to an emergency that threatens his health.

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

3.12 Where an organisation finds it necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it may collect, use or disclose his or her NRIC number with notification and consent.

3.13 PDPC would generally consider it necessary to accurately establish or verify the identity of individual to a high degree of fidelity in the following situations –

a) Where the failure to accurately identify the individual to a high degree of fidelity may **pose a significant safety or security risk.** For example, visitor entry to preschools where ensuring the safety and security of young children is an overriding concern; or

b) Where the inability to accurately identify an individual to a high degree of fidelity may **pose a risk of significant impact or harm[14] to an individual and/or the**

[13] Paragraph 1(b) of the Fourth Schedule of the PDPA.
[14] For example, reputational, financial, personal or proprietary damage.

organisation (e.g. fraudulent claims). Such transactions typically relate to healthcare, financial or real estate matters, such as property transactions, insurance applications and claims, applications and disbursements of substantial financial aid, background credit checks with credit bureau, and medical check-ups and reports.

3.14 The above are illustrative and not intended to be exhaustive as to the types of situations that would be considered necessary to accurately establish or verify the identity of the individual to a high degree of fidelity. Organisations should assess whether their specific situation meets the above considerations before collecting the individual's NRIC number (or copy of NRIC). In collecting the NRIC number (or copy of NRIC), organisations should be able to provide justification[15] on request of either the individual or the PDPC as to why the collection, use or disclosure of the NRIC number (or copy of NRIC) is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

3.15 Organisations should note that when they collect a copy of the NRIC, they are considered to have collected all the personal data on the NRIC, and will be subject to the Data Protection Provisions of the PDPA for that collection. Organisations should assess whether they are collecting excessive personal data contained in the copy of the NRIC for the intended purpose, and if they could adopt alternatives to the individual's NRIC number or copy of NRIC.

3.16 Where the collection of the NRIC number (or copy of NRIC) is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it would generally be considered reasonable for the organisations to require the consent of the individual to collect, use or disclose his or her NRIC number for the stated purpose[16].

4 Retention of Physical NRIC

4.1 Given the importance of the NRIC as a national identification document that is issued to all citizens and permanent residents of Singapore, and the impact to the individual should the physical NRIC be misplaced, stolen or used for illegal activities such as identity theft and fraud, organisations should generally not retain an individual's physical NRIC unless the retention of the physical NRIC is required under the law.

[15] Section 12(a) and 12(d)(i) provides that an organisation shall develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA, and make them available on request.

[16] Section 14(2)(a) provides that organisations must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide the product or service.

5 Alternatives to NRIC

5.1 PDPC does not prescribe the types of identifiers that organisations should adopt in place of NRIC numbers. Organisations should assess the suitability of alternatives to NRIC numbers based on their own business and operational needs. Some alternatives that have been adopted by organisations include organisation or user-generated ID, tracking number, organisation-issued QR code, or monetary deposit. Organisations should also consider whether the alternatives provided are reasonable, and avoid collecting excessive personal data as an alternative to the individual's NRIC number (or a copy of NRIC).

Partial NRIC numbers

5.2 PDPC recognises that organisations may wish to collect partial NRIC number when other alternatives are not satisfactory. PDPC considers that organisations that collect partial NRIC number **up to the last 3 numerical digits and checksum** of the NRIC number (e.g. "567A" from the full NRIC number of "S1234567A") in this manner would not be considered to be collecting the full NRIC number, and therefore not subject to the treatment for NRIC numbers set out in these guidelines. For more information on partial NRIC numbers, please refer to PDPC's Technical Guide to these Guidelines.

5.3 To be clear, partial NRIC numbers are considered personal data under the PDPA to the extent that an individual can be identified from the partial NRIC number, or from the number and other information to which the organisation has or is likely to have access[17]. The risks associated with the permanent and irreplaceable nature of the NRIC and the potential to unlock large amounts of information relating to the individual are diminished but still exist. These risks together with the safeguards put in place to protect the personal data in an organisation's possession will be taken into consideration by the PDPC in determining whether the collection, use or disclosure of partial NRIC numbers is reasonable. Organisations that collect partial NRIC numbers must still comply with the Data Protection Provisions of the PDPA, such as making reasonable security arrangements to protect the data in their possession or under their control from unauthorised disclosure.

5.4 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:

[17] Section 2 of the PDPA provides that "personal data" means 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.

5.5	**Example: Redemption of free parking** Mall ABC allows shoppers who spend a certain amount at the Mall to make a redemption for free parking. Mall ABC intends to keep a record of the identities of shoppers who make the redemptions in order to limit the number of redemptions that can be made by each shopper. Mall ABC should not collect shoppers' NRIC numbers for this purpose. Mall ABC could consider other appropriate means of limiting the number of redemptions that can be made by each shopper, for example by checking the shopper's physical NRIC and recording his or her name, partial NRIC number, vehicle number or mobile phone number.
5.6	**Example: Online purchase of movie tickets** Cinema DEF wishes to verify the identity of customers who purchase movie tickets online when they collect the movie tickets, to ensure the tickets are issued to the right customers. Cinema DEF should not collect the NRIC numbers of customers for this purpose. Cinema DEF could consider other appropriate means of verification, such as issuing customers a booking reference number or an SMS confirmation.
5.7	**Example: Signing up for retail membership and lucky draw** Retail Store GHI wishes to create a unique identifier for each customer who signs up for its membership programme for the purpose of managing the customer's membership account and reward points. Retail Store GHI could consider allowing its members to use identifiers, such as their mobile numbers, email address, user-generated identifier or partial NRIC number (up to last 3 numerical digits and checksum) for its customers' membership accounts. Retail Store GHI also wishes to conduct a lucky draw for its customers where the top prize is valued at $10,000. It collects the full name, partial NRIC number (i.e. last 3 numerical digits and checksum) and contact information (e.g. mobile number, email address, mailing address) of participating customers for the purpose of contacting the winners of the lucky draw and verifying the identities of the winners who claim the lucky draw prizes. Retail Store GHI verifies the identity of the winners by checking their full names and partial NRIC number against the information on their physical NRIC.

5.8	**Example: Registering interest in a product and submitting feedback** Retail Store JKL is releasing a new product for sale in the following month. To ensure that priority to purchase the product is given to customers who indicate their interest in the new product, Retail Store JKL allows customers to register their interest in advance. Retail Store JKL also allows individuals to submit feedback regarding its store catalogue. Retail Store JKL should not collect the NRIC number of individuals for the purposes of obtaining interest in its new product as well as receiving feedback from customers. Instead, Retail Store JKL can consider collecting individuals' names and contact details, such as their mobile numbers or email addresses.
5.9	**Example: Establishing identity of visitors to a private condominium** Condominium MNO's MCST wishes to record the identity of visitors as part of providing security to the condominium residents. The MCST could adopt the approach of checking a visitor's NRIC or other photo identification to record the visitor's full name, partial NRIC number (i.e. last 3 numerical digits and checksum), contact details (e.g. mobile number) and/or vehicle registration number. MCST should consider adopting a visitor management system that stores such information electronically and is protected by passwords instead of an open visitor log book. It could also consider other security solutions such as installing CCTV as a way of providing security to its residents. The MCST must also cease to retain the NRIC number, or to remove the means by which the NRIC number can be associated with a particular individual, as soon as the purpose for which the NRIC number was collected is no longer served by its retention, and retention is no longer necessary for business or legal purposes.
5.10	**Example: Establishing identity and issuance of visitor badges to visitors to a secured data centre** Although there are no laws that provide for the collection of NRIC numbers or physical NRIC for entry into Data Centre DEF, the MCST of the building in which Data Centre DEF is sited assesses that it is necessary to accurately establish the identity of every visitor to a high degree of fidelity in order to safeguard the critical information infrastructure within its premises as they pose significant security risks. The MCST must be able to provide justification to individuals and/or PDPC why the collection of visitors' full NRIC number is necessary to address these security risks. The MCST must

	also comply with the obligations in the PDPA when collecting the NRIC numbers of visitors, including the obligation to make reasonable security arrangements to protect the NRIC numbers collected from unauthorised use or disclosure, and could consider adopting technological solutions for scanning visitors' physical NRICs to capture and store the NRIC numbers in a secure manner. In addition, the MCST wishes to issue visitor badges and collect the physical NRIC of visitors as collateral to ensure that the visitor badges are returned after their visit. As the retention of physical NRIC for entry into Data Centre DEF is not required under any law, Data Centre DEF should not retain visitors' physical NRICs as collateral for the visitor badges. Instead, the MCST may wish to consider alternative ways of ensuring the visitor badges are returned which would not require the retention of any identification document. For example, Data Centre DEF could designate a single point of exit for visitors to return the visitor badges before leaving the premises.
5.11	**Example: Renting a bicycle** Bicycle Rental Company ABC wishes to collect the physical NRIC of customers as collateral to ensure that they would return the rented bicycles. As the retention of the customers' physical NRIC for the rental of bicycles is not required under any law, Rental Company ABC should not retain customers' physical NRICs. It could consider using other forms of collateral, such as a monetary deposit of a reasonable amount, for the rental of bicycles. Where possible, it could also consider other ways of managing its fleet such as the use of tracking devices or mobile apps.

5.12 In certain circumstances, an organisation may merely have sight of an individual's physical NRIC and the information on it for verification purposes. Where there was no intention to obtain control or possession of the physical NRIC in checking the physical NRIC for the purpose of establishing or verifying the identity of the individual, and no personal data will be retained once the NRIC is returned immediately to the individual, PDPC does not consider it a collection of personal data on the physical NRIC.

5.13	**Example: Verifying age of a customer who wishes to purchase tobacco** Damien would like to purchase a packet of cigarettes at Convenience Store ABC. At the point of sale, the cashier at the Convenience Store ABC requests for a proof of identity (e.g. NRIC, driving license or passport) in order to check Damien'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, Convenience Store ABC is allowed to request Damien to produce one such identification document for this purpose.

PART III: IMPLEMENTATION

6 Implementation timeframe

6.1 The interpretation of the PDPA in Part II of these Guidelines clarifies the applicable standard for the permissible collection, use or disclosure of NRIC numbers (or copies of NRIC) and retention of physical NRICs. To allow organisations time to review and implement any necessary changes to align their existing business practices and processes with these Guidelines, the PDPC will apply the interpretation of the PDPA in Part II of these Guidelines from 1 September 2019. Organisations collecting, using or disclosing NRIC numbers (or copies of NRIC) should continue to ensure that they protect personal data in their possession or control, in compliance with their obligations under the PDPA.

6.2 Organisations may refer to the Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers for guidance on replacing the NRIC number for identifying individuals in websites and other public facing computer systems.

END OF DOCUMENT