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

Published 31 August 2018

TABLE OF CONTENTS

PURPOSE OF THIS GUIDE

This Guide aims to provide organisations with some tips for the replacement of national identification numbers as a way of identifying individuals, in their websites and other public facing computer systems.

For ease of reference, NRIC numbers are used as an example in this Guide. Unless otherwise specified, the treatment of NRIC numbers described in this Guide also applies to Birth Certificate numbers, Foreign Identification Numbers ("FIN") and Work Permit numbers (collectively referred to as 'other national identification numbers').

While the topics listed in this Guide aim to provide suggestions for organisations to replace NRIC numbers for identifying individuals in their websites and other public facing computer systems, the topics are not exhaustive and do not address every obligation in the Personal Data Protection Act ("PDPA").

PDPC does not prescribe the types of identifiers that organisations should adopt in place of NRIC or other national identification numbers. Organisations should assess the suitability of alternatives based on their own business and operational needs.

INTRODUCTION

The NRIC number of an individual is considered personal data as it can be used to identify the individual, and can be used to access large amounts of information relating to the individual, such as the individuals' name, address, contact numbers, income information and health information. Organisations should thus avoid the use of NRIC numbers as user names or unique identifiers in their applications, websites or public facing systems.

Examples of applications, websites and public facing systems that should use alternatives in place of NRIC numbers to identify individuals include:

- Club membership
- Loyalty programmes
- Event management
- Online shopping
- In-store retail membership
- Shopping mall car park redemption kiosks

Key Considerations for Choosing a Replacement Identifier for NRIC Numbers

- ✓ **Be easily remembered by the individual**
- ✓ **Be unique to each individual**
- ✓ **Does not contain sensitive information**
- ✓ **Cannot be easily guessed by others**

ALTERNATIVES TO NRIC NUMBERS

This section describes some alternatives that can be used instead of the NRIC number. This includes suggestions to consider when implementing identifiers in **new** systems, and replacing the NRIC number with new identifiers in **existing** systems.

User Selected Identifier/User Name

- Allow users to enter their own identifiers (e.g. user defined nickname).
- Ideal for systems that currently use NRIC Numbers as user names.

For New Systems	For Existing Systems
✓ Allow each user to enter their user name during registration/account creation, or after their identity has been verified. ✓ Check that the user name is not used by another user. ✓ Check that the user name meets the organisation's system requirements, e.g. the number of characters, use of special characters. ✓ Include function(s) to help users remember or find their user name, in case they forget them e.g. option for user to request user name to be sent designated user email account or telephone number.	✓ Verify the user's identity (e.g. by getting them to log in to the system). ✓ Request the user to enter their new user name, after their identity has been verified. ✓ Check that the new user name is not currently in use ✓ Check that the user name meets the organisation's system requirements, e.g. the number of characters, use of special characters. ✓ Include function(s) to help users remember or find their user name, in case they forget them, e.g. option for user to request user name to be sent designated user email account or telephone number.

For New Systems	For Existing Systems
✓ Allow each user to enter their user name during registration/account creation.	✓ Verify the user's identity (e.g. by getting them to log in to the system). ✓ Request the user to enter their new user name, after their identity has been verified.

Organisation Selected Identifier

- Organisation selects the identifier for each user.
- Ideal for organisations that use the NRIC number internally.

For New Systems	For Existing Systems
✓ Automatically generate the identifier during or after registration/account creation. ✓ Check that the identifier is not used by another user in the system. ✓ If the identifier is also a user name, inform users of their user name after registration/account creation. ✓ Include function(s) to help users remember or find their user name, in case they forget them e.g. option for user to request user name to be sent designated user email account or telephone number.	✓ Generate a new identifier for each user, automatically. Check that the new user name is not assigned to another user. ✓ If the identifier is also a user name, inform the user of their new user name, after their identity has been verified (e.g. after they log in). ✓ Consider a parallel run for both old and new user names to be able to be used. The duration of the parallel run may be determined based on the number of affected individuals and the frequency of access.

Email Address

- Organisation uses the email address supplied by the user as an identifier and user name.
- Easily remembered by the user.

New Systems	Existing Systems
✓ Confirm email address during registration/account creation by getting user to enter the same email address twice, without the ability the use cut-and-paste function. ✓ Check that the email address is not already used by another user in the system. ✓ Validate email address by sending a confirmation link to the address. ✓ Provide functions/processes for user to change their email address.	✓ Inform users that their email addresses will replace their NRIC numbers as their user names. ✓ Provide functions/processes for user to provide their email addresses if not available in existing database. Check that the email address provided is not already used by another user in the system. ✓ Validate email address supplied by user, by sending a confirmation link to the address. ✓ Only start accepting the user's email address as their user name, after their email address has been validated. ✓ Provide functions/processes for user to change their email address.

Mobile Number

- Organisation uses the mobile number supplied by the user as identifier.
- Like the email address, is easily remembered by the user.

New Systems	Existing Systems
✓ Validate mobile number during registration/account creation by sending a One-Time Password (OTP) to it, and requesting the user to enter the OTP into the system. OTPs are usually randomly generated, with 6 or more digit numbers. ✓ Check that the mobile number is not already used by another user in the system. ✓ Provide functions/processes to handle cases where a new user has the mobile number of an existing user. This might occur when the previous user terminated the number and it is reassigned to the new user by the telco. ✓ Provide functions/processes to allow users to change their mobile numbers.	✓ Check that no mobile number is replicated in different user records. If there are multiple user records with similar mobile number, to verify with user on updated mobile number. ✓ Inform each user that their mobile number will replace their NRIC as their user name. ✓ Provide functions/processes for user to provide their mobile number if not available in existing database. Check that the mobile number is not already used by another user in the system. ✓ Validate mobile number supplied by user, by sending an OTP and checking the OTP entered by the user. ✓ Only start accepting the user's mobile number as their user name, after their mobile number has been validated. ✓ Provide functions/processes to handle cases where a new user has the mobile number of an existing user. This might occur

	when the previous user terminated the number and it is reassigned to the new user by the telco. ✓ Provide functions/processes to allow users to change their mobile numbers.

Combination of Identifiers

- Organisation uses a combination of information provided by the user as identifier.
- E.g. first name + last name, initials + last name, part name + part phone number, date of birth + part phone number
- Combination should not contain sensitive personal information.

New Systems	Existing Systems
✓ During account creation/registration, check that the combination is not already used. ✓ Check that the combination meets the organisation's system requirements such as number of characters, use of special characters, etc.	✓ Check that the combination does not belong to any other user. ✓ Check that the combination meets the organisation's system requirements such as number of characters, use of special characters, etc. ✓ Inform the user that the combination will replace NRIC as their user name.

Partial NRIC Number

- Organisation uses the last 3 digits + last alphabet of the user's NRIC number, in combination with other strings of data.
- E.g. use "567A" if the NRIC number is S1234567A.
- Other strings of data could include the first part of email address, partial mobile number of an individual, etc.

New Systems	Existing Systems
✓ During account creation/registration, check that the combination of partial NRIC + other information is not already used. ✓ Ensure that the information required to form the identifier is collected during account creation/registration.	✓ Check that the system has the required information (i.e. name, postal code, mobile number, date of birth etc.) to form the unique identifier. ✓ Check for uniqueness of the new ID formed from the combination. ✓ Inform the user that the combination will replace NRIC as their user name.

REPLACING NRIC NUMBER IN EXISTING SYSTEMS

The process of replacement of NRIC numbers as identifiers and user names in websites and other public facing systems can be divided into 3 separate phases:

1. Preparation
2. Implementation
3. Post-Implementation

This section describes some suggested steps during each phase, for organisations to consider. **The steps are not exhaustive and may not apply to all organisations.**

Preparation

- ✓ Choose the NRIC number replacement, and ensure that they meet the key considerations mentioned in the Introduction.
- ✓ Plan the implementation timeline, e.g. design changes to the system, system testing, notifying users, changeover period.
- ✓ Plan the steps that users will take when they replace their NRIC number with the new user name, e.g. login to the system first, then enter their new username.
- ✓ Look for screens or online forms where the NRIC number is displayed, and consider whether it is required. For cases where the display is absolutely necessary, organisations should consider displaying masked NRIC numbers instead.
- ✓ Plan and design the changes to the system, e.g. new database fields for the identifier, new forms for user to enter their username, updated forms with the NRIC number removed.
- ✓ Plan and design the changes required for other systems and processes that rely on the NRIC number as a unique identifier.

Preparation (continued)

- ✓ Perform thorough system and user testing, to check that all functions for replacing the NRIC number work as designed and are user-friendly.
- ✓ Make a backup of all affected data.
- ✓ Notify and educate affected parties within the organisation, e.g. customer service, so that they can plan changes to their workflow and are able to help customers during the transition.
- ✓ Plan when and how to notify users e.g. by announcement after they login.
- ✓ Ensure that the system has sufficient capacity to handle any increase in usage.

Implementation

- ✓ Ensure that all user queries are answered promptly and clearly.
- ✓ Provide processes to assist those users who have difficulties, including procedures to verify the identity of users.
- ✓ Address feedback provided by users.
- ✓ Check that users' alternate identifiers are recorded and assigned correctly.
- ✓ Monitor the number of users who have replaced their NRIC number and remind those who have not.
- ✓ Plan the processes for handling users who could not be contacted, or who could not provide their alternate identifiers during the implementation period.
- ✓ Ensure that related systems that depend on the NRIC number have also been enhanced to handle the alternate identifier.

Post Implementation

- ✓ Remind users of the new identifier, and that their NRIC numbers are no longer used.
- ✓ Conduct a review to determine whether the NRIC numbers are still required in the system as well as in the organisation.
- ✓ If not required, to remove the NRIC numbers from the system.
- ✓ Disable user accounts that do not have replacement identifiers.
- ✓ Put up a notice on the website/system, to notify users who did not change their identifiers, that their accounts have been disabled, and the process to reactivate their accounts (e.g. to contact the system administrator).

REPLACING EXISTING NRIC NUMBERS IN DATABASES

Databases hold the data that are used by the organisation's websites and systems. This section lists some steps for organisations to consider when modifying their databases to replace existing NRIC numbers with alternate identifiers.

Replacing existing NRIC numbers in databases should be performed together with the modification of websites and systems. **The following steps are not exhaustive and may not apply to all organisations.**

- ✓ Create test databases for testing of scripts, functions and processes.
- ✓ Identify all the database locations where NRIC numbers are stored.
- ✓ Consider whether to create new database fields for the replacement identifier, or to replace the existing NRIC numbers in their current fields.
- ✓ Create database scripts, or programs, to perform the replacement.
- ✓ Test these scripts on the test database, to ensure that the replacement identifiers are assigned to the correct user.
- ✓ Create backups of the database before running the actual replacement.
- ✓ Consider when to delete the backups, after the actual replacement is completed. This could be after the organisation has verified that all website and system issues relating to the replacement of NRIC numbers, have been resolved.

REPLACING THE PRIMARY KEY

The primary key is a unique identifier for each record in a database, and is used by the database to link records together. For example, the individual's contact details and account details may be kept in separate records. Although most systems use a database generated unique value as the primary key, some organisations have been using the NRIC number as a primary key instead.

Some suggestions and considerations for organisations who are replacing the NRIC number as the primary key in their databases include:

- ✓ Use a database generated primary key value. The database will automatically ensure that all primary key values are unique.
- ✓ If the organisation wishes to use values other than the database generated value, then the new primary key should ideally be a value that will not change over time.
- ✓ Prior to changing the primary key, organisations should identify all records that use the primary key and plan carefully for these records to be updated with the new primary key. An update to the primary key can lead to the update of potentially a lot of database tables.
- ✓ Organisations should also make the necessary enhancements to the systems and applications that use the database, e.g. CRM system, to ensure that the new primary key does not affect the functionalities of these systems and applications.
- ✓ When changing the primary key, organisations should utilise built-in database functions wherever possible.

SCANNING OF NRIC NUMBERS

While using barcode scanners to scan NRIC numbers is more efficient than manual input, organisations should take care to ensure that complete NRIC numbers are not stored permanently.

This section describes some considerations for organisations when building systems that scan NRIC/FIN barcodes from physical documents containing NRIC/FIN barcodes (e.g. identity card, work permit, driver's licence). Examples of such systems include visitor access or building management systems.

- ✓ When a barcode scanner scans an NRIC barcode, it will typically send the complete NRIC number to the system. Organisations should thus ensure that the system does not permanently store (e.g. in a database) the scanned NRIC number.
- ✓ Convert the scanned NRIC number to a final format, immediately after scanning. The NRIC number can be stored permanently after conversion.
- ✓ Final formats may include partial NRIC number (last 3 digits + last alphabet), masked NRIC number (only showing last 3 digits + last alphabet) or hashed NRIC number. The complete NRIC number should not be stored.
- ✓ Hashing refers to converting the NRIC number to another string of text, by applying a cryptographic hashing algorithm. Hashed NRIC numbers will be unique, and cannot be converted back to actual NRIC numbers.
- ✓ When a visitor's NRIC is scanned, the system can create a hash of the NRIC number, and then compare the hashed NRIC number against the existing hashed NRIC numbers in the database. The visitor's record can then be retrieved this way.

ADDITIONAL RESOURCES

Organisations and their vendors are encouraged to refer to the following resources on the PDPC website, which provide more information on the areas that are mentioned briefly in this Guide.

Advisory Guidelines

- Can be found on the PDPC website at https://www.pdpc.gov.sg/ag
- Chapter 17 (The Protection Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 18 (The Retention Limitation Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 19 (The Transfer Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 7 (Online Activities) of the Advisory Guidelines on the Personal Data Protection Act for Selected Topics

Other Guides

- Can be found on the PDPC website at https://www.pdpc.gov.sg/og
- Guide to Securing Personal Data in Electronic Medium
- Online resources on changing database primary key

    a. IBM DB2 https://www.ibm.com/support/knowledgecenter/en/SSEPGG_9.5.0/com.ibm.db2.luw.admin.gui.doc/doc/t0023772.html
    b. Microsoft Access https://support.office.com/en-us/article/Add-or-change-a-table-s-primary-key-in-Access-07b4a84b-0063-4d56-8b00-65f2975e4379
    c. Microsoft SQL https://docs.microsoft.com/en-us/sql/relational-databases/tables/primary-and-foreign-key-constraints

d. MySQL https://www.techonthenet.com/mysql/primary_keys.php
e. Oracle https://docs.oracle.com/javadb/10.8.3.0/ref/rrefsqlj81859.html
f. Sybase http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.1/dbusage/managingprimarykeys-sql.html
g. TechOnTheNet https://www.techonthenet.com/oracle/primary_keys.php
h. W3Schools https://www.w3schools.com/sql/sql_primarykey.asp

END OF DOCUMENT

BROUGHT TO YOU BY

PERSONAL DATA PROTECTION COMMISSION SINGAPORE