ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS

ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

24 SEPTEMBER 2013

PART I: INTRODUCTION AND OVERVIEW 5

1 Introduction 5

2 Overview of the PDPA 6

PART II: SELECTED TOPICS 8

3 Analytics and Research 8

How does the PDPA apply to organisations that want to conduct analytics and research activities? 8

4 Anonymisation 10

What is Anonymisation? 10

Why anonymise personal data? 10

Anonymisation techniques 11

Challenges and limitations in anonymising data 12

Re-identification and its risks 12

Assessing and managing re-identification risks 15

Factors in re-identification 18

Anonymisation testing 20

5 Closed-circuit television cameras (“CCTVs”) 23

Do organisations always have to provide notifications when CCTVs are deployed? 23

Where should notices be placed? 23

What should such notices state? 23

Is notification still required if CCTVs are there to covertly monitor the premises for security reasons, and notification would defeat the purpose of using the CCTVs? 23

If my organisation installs CCTVs that also capture video footage beyond the boundaries of our premises, is that allowed? 24

Access to CCTV footage 24

Is an organisation required to provide access to CCTV footage if it shows other individuals and the organisation doesn't have the technical ability or it is too costly to mask the other individuals? 24

Is an organisation required to provide a copy of CCTV footage pursuant to an access request for the footage? 25

Can compromising an organisation's security arrangements or competitive position be sufficient reason to deny access to CCTV footage? 25

Can individuals make joint access requests for CCTV footage containing their images, if they consent to their own images being viewed by the others making the joint request? 26

Is an organisation required to accede to requests to delete CCTV footage? 26

Is there a requirement that CCTV footage or video stills be of minimum resolution when provided to individuals upon request? 26

Can the organisation require that the individual sign a contract to agree not to disclose to any third party the CCTV video to be provided to him? 26

6 Employment 27

Does an organisation need to seek the consent of a job applicant for the collection and use of his personal data? 27

Can organisations collect and use personal data on the job applicant from social networking sources (e.g. Facebook or Twitter)? 27

Can organisations or recruitment agencies collect and use personal data on individuals from social networking sites or publicly available sources to contact them for prospective job opportunities? 28

Can organisations use the information in business cards for recruitment? 28

How long can an organisation keep the personal data of job applicants who are not hired? 29

Can job applicants ask the organisation to reveal how much information the organisation has on them or find out why they were not selected? 29

How does the PDPA apply to recruitment agencies? 29

Personal Data of Employees 30

How does the PDPA apply to employment records of employees? 30

Collecting, using and disclosing employee personal data for evaluative purposes 31

Collecting, using and disclosing personal data for the purpose of managing or terminating an employment relationship between the organisation and the individual 31

What is the difference between the exception for evaluative purposes and the exception for the purpose of managing and terminating an employment relationship? 33

How long can organisations continue to hold personal data of former employees? 34

Are organisations responsible if their employees do not comply with the PDPA? Are volunteers considered employees? 34

Do the exceptions to the Consent Obligation for the collection, use and disclosure of personal data of employees also apply to individuals that may act on behalf of an organisation, but are not the organisation's employees? 35

7 NRIC Numbers 36

How does the PDPA apply to NRIC numbers? 36

Can organisations collect NRIC cards? 36

For what business purposes are organisations allowed to use NRIC numbers? 37

How does the PDPA apply to organisations publishing NRIC numbers for purposes such as to publish the results of lucky draws or other contests? 37

8 Online Activities 38

Are IP addresses personal data? 38

Must consent be obtained for the use of cookies? 39

Are organisations allowed to use cookies for behavioural targeting? . 40

PART I: INTRODUCTION AND OVERVIEW

1 Introduction

1.1 The Personal Data Protection Act 2012 (the "PDPA") establishes a new general data protection law in Singapore which governs the collection, use and disclosure of individuals' personal data by organisations. The Personal Data Protection Commission (the "Commission") is established under the PDPA with the key functions, amongst others, of promoting awareness of data protection in Singapore and administering and enforcing the PDPA.

1.2 These advisory guidelines (these "Guidelines") are issued by the Commission pursuant to section 49(1) of the PDPA to provide guidance on the manner in which the Commission will interpret provisions of the PDPA. Where relevant, reference is made to the provisions of the regulations to be made under the PDPA ("Regulations").

1.3 These Guidelines are advisory in nature and are not legally binding on the Commission or any other party. They do not modify or supplement in any way the legal effect and interpretation of any laws cited including, but not limited to, the PDPA and any subsidiary legislation (such as regulations and rules) issued under the PDPA. Accordingly, these Guidelines shall not be construed to limit or restrict the Commission's administration and enforcement of the PDPA. The provisions of the PDPA and any regulations or rules issued thereunder will prevail over these Guidelines in the event of any inconsistency. The Guidelines do not constitute legal advice.

1.4 These Guidelines should be read in conjunction with the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines"), which explain in greater detail the obligations which organisations have to comply with under the PDPA, as well as other relevant Advisory Guidelines that the Commission may issue from time to time.

2 Overview of the PDPA

2.1 The PDPA governs 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 and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. The PDPA contains two main sets of provisions, covering data protection and the Do Not Call registry, which organisations are required to comply with.

2.2 The PDPA's data protection obligations are set out in Parts III to VI of the PDPA (the "Data Protection Provisions"). In brief, the Data Protection Provisions deal with the following matters:

a) Having reasonable purposes, notifying purposes and obtaining consent for collection, use or disclosure of personal data;

b) Allowing individuals to access and correct their personal data;

c) Taking care of personal data, which relates to ensuring accuracy, protecting personal data (including protection in the case of international transfers) and not retaining personal data if no longer needed; and

d) Having policies and practices to comply with the PDPA.

2.3 The PDPA provides a number of exceptions to various Data Protection Provisions to address situations where organisations may have a legitimate need, for example, to collect, use or disclose personal data without consent or to refuse to provide an individual with access to his or her personal data.

2.4 The PDPA's Do Not Call registry provisions are set out in Part IX of the PDPA (the "Do Not Call Provisions"). These deal with the establishment of Singapore's national Do Not Call registry (the "Do Not Call Registry") and the obligations of organisations relating to the sending of certain marketing messages to Singapore telephone numbers. The Do Not Call Registry will initially comprise 3 separate registers kept and maintained by the Commission under section 39 of the PDPA (the "Do Not Call Registers") which cover telephone calls, text messages and faxes. Users and subscribers will be able to register a Singapore telephone number on one or more Do Not Call Registers depending on what their preferences are in relation to receiving marketing messages through telephone calls, text messages or fax.

2.5 Organisations have the following obligations in relation to sending certain marketing messages to Singapore telephone numbers:

a) Checking the relevant Do Not Call Register(s) to confirm if the Singapore telephone number is listed on the Do Not Call Register(s);

b) Providing information on the individual or organisation who sent or authorised the sending of the marketing message; and

c) Not concealing or withholding the calling line identity of the sender of the marketing message for voice calls.

2.6 The PDPA recognises that organisations may not need to check the Do Not Call Registers in certain circumstances, in particular, when the user or subscriber of a Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the marketing message to that number.

PART II: SELECTED TOPICS

3 Analytics and Research

How does the PDPA apply to organisations that want to conduct analytics and research activities?

3.1 Where the research activities carried out by the organisation requires the collection, use or disclosure of personal data, the organisation is required to comply with the PDPA. In particular, under the PDPA, individuals have to be informed of and consent to the purposes for which their personal data are collected, used, and disclosed by organisations, unless any exception under the PDPA applies. Please see the sections on "The Consent Obligation" and "The Notification Obligation" in the Key Concept Guidelines for more details.

3.2 In respect of the Notification Obligation, an organisation may specify research itself as a purpose and an individual can give consent specifically for the use of his personal data for research.

3.3 Alternatively, an organisation may rely on consent given by an individual for a purpose that does not explicitly cover analytics and research if the purpose of the analytics and research falls within the original purpose for which consent was given.

Example:

John signs up for a mobile service with a telecommunications service provider. John consents to his personal data being collected and used by the service provider for the purposes of providing him the mobile service. The service provider collects and analyses some of John's personal data for the purposes of managing its network and short term planning enhancements to improve the quality of mobile services provided to him. Such activities would likely fall within the original purpose John consented to.

An adventure camp company requires all camp participants to provide emergency contact information of an individual, which includes personal data like name, telephone number and address, with consent from the individual. The purpose stated was to use that personal data to contact the individual in the event of an emergency relating to the camp participant. The company subsequently analyses the personal data for the purpose of determining if the individual(s) listed would be a potential participant for adventure camps. This purpose would not fall within the original purpose for which the consent was obtained.

3.4 Organisations may also use personal data without consent for a research purpose under paragraph 1(i) of the Third Schedule to the PDPA, if all the conditions referred to in that paragraph are fulfilled. Paragraph 1(i) says that an organisation may use personal data about an individual without the consent of the individual if the personal data is used for a research purpose, including historical or statistical research, subject to the conditions in paragraph 2. Paragraph 2 sets out that Paragraph 1(i) shall not apply unless:

a) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

b) it is impracticable for the organisation to seek the consent of the individual for the use;

c) the personal data will not be used to contact persons to ask them to participate in the research; and

d) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

3.5 Alternatively, organisations could consider using anonymous data to conduct research. Anonymised data is not personal data and thus would not be governed by the PDPA. Please refer to the section on “Anonymisation” in these Guidelines for more details.

4 Anonymisation

What is Anonymisation?

4.1 In general, anonymisation refers to the process of removing identifying information such that the remaining data does not identify any particular individual.

4.2 For purposes of these Guidelines, anonymisation has to be understood in the context of the definition of personal data under the PDPA. The definition of personal data under section 2(1) of the PDPA is: "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". Please see the section on "Personal Data" in the Key Concepts Guidelines for more details.

4.3 Anonymisation therefore refers to the conversion of personal data into data that cannot be used to identify an individual whether from that data itself, or from that data and other information to which the organisation has or is likely to have access.

Why anonymise personal data?

4.4 Since anonymised data is not personal data, the Data Protection Provisions in Parts III to VI of the PDPA will not apply.

4.5 Generally, anonymisation of personal data is carried out to render the resultant data suitable for more uses than its original state would permit under data protection regimes. For example, anonymised data may be used for research and data mining where personal identifiers in the data are unnecessary or undesired. Anonymised datasets could also be a protection measure against inadvertent disclosures and security breaches.

4.6 In general, where individuals need not be identifiable for the purposes in question, it is good practice to collect data in an anonymised form or to anonymise the data prior to disclosure.

4.7 The following sections seek to assist organisations in identifying the issues that they should take into account in the anonymisation of data.

Anonymisation techniques

4.8 For general information, anonymisation techniques include but are not limited to the following:

a) *Pseudonymisation*: replacing personal identifiers with other references. For example, replacing an individual's name with a tag or reference number which is randomly generated.

b) *Aggregation*: displaying values as totals, so that none of the individual values which could identify an individual is shown. For example, displaying the sum of the individual ages of the total number of individuals in a group, rather than the age of each individual.

c) *Replacement*: replacing values or a subset of the values with a computed average or a number derived from the values. For example, replacing the individuals with ages of 15, 20 and 18 with an age value of 17 to blur the distinction, if the exact age is not required for the desired purposes.

d) *Data reduction*: removing values that are not required for the purpose. For example, removing 'ethnicity' from a data set of individuals' attributes.

e) *Data Suppression*: banding or hiding the value within a given range. For example, replacing age '43' with the range '40-50'.

f) *Data shuffling*: mixing up or replacing values with those of the same type so that the information looks similar but is unrelated to the actual details. For example, the surnames in a customer database could be sanitised by replacing them with those drawn from another database.

g) *Masking*: removing certain details while preserving the look and feel of the data. For example, representing a full string of NRIC numbers as 'S0XXXX45A' instead of the original 'S0122445A'.

4.9 After such techniques are applied to personal data such that an individual cannot be identified from the resultant dataset "dataset X" itself, an organisation should still be mindful of the possibility that an individual can be identified when dataset X is combined with other information the organisation has access to, or when the anonymisation process is reversed with the right algorithm. To the extent that an organisation can still identify individuals from dataset X, it is still considered personal data to the organisation. Dataset X, however, would cease to be personal data if the organisation is no longer

able to identify an individual from it. The following section elaborates on the challenges and limitations of anonymisation.

Challenges and limitations in anonymising data

4.10 The nature of the original data affects how much identifying information needs to be removed so that it is no longer personal data. Factors such as the uniqueness of data points with respect to other data points and the availability of other '*complementary'* data contribute to the challenge of its anonymisation. Some data types are inherently 'rich' and full of information (e.g. portrait photographs taken for facial recognition purposes), such that the amount of alteration required for anonymisation might render the data useless for its intended purposes. There are also cases where the use of particular methods may anonymise the personal data for some but not all individuals, because data points for certain individuals remain unique. For example, a data set containing the ages of individuals has one outlier of age 89 while the other ages are below 50. No matter how the ages are suppressed into ranges, the data point for the 89 year old stands out.

4.11 There are often conflicting needs for anonymity and data integrity. Stripping data of too many identifiers may not preserve the usefulness of the data, or might deny potential uses for the data. Data anonymised for specific purposes might not be useful for others because its functionality is reduced.

4.12 For example, a retail organisation possesses a database of their customers' personal data (age, residential address, income, and occupation). From a marketing research perspective, these identifiers may yield information that is essential for profiling the customers. If the dataset were anonymised such that the ages were aggregated and incomes were shuffled, and the occupations removed, then the functionality would likely have been lost as the anonymised database would not yield conclusions about customers' profiles, unlike the original database. An organisation will therefore have to consider whether the anonymised data would still be suitable for its intended purposes.

Re-identification and its risks

4.13 Although an organisation may consider a data set anonymised, it should consider the risk of re-identification if it intends to publish or disclose the data set to another organisation.

4.14 Re-identification is the process by which anonymised data is combined with other information such that an individual can be identified from that data, hence rendering the "anonymised" data personal data again.

Example[1]: Unique Identification by Combining Zip Code, Sex, Birth date

Latanya Sweeney, a computer science professor, conducted a study in 1990 which found that 87% of the United States population could be uniquely identified by combining datasets containing zip codes, birth dates, and gender. In particular, Sweeney was able to identify a Massachusetts governor by combining two data sets. The first data set was gathered from Group Insurance Commission (GIC), a purchaser of health insurance for employees. In the data set that was disclosed by GIC, names, addresses, social security numbers had been removed but not the zip codes, sex and birth dates of the employees.

Sweeney then purchased voter rolls, which included name, zip code, address, sex, and birth date of voters in Cambridge, where the governor resided, and combined the information contained in the rolls with GIC's data. She easily re-identified the governor from the combined data. This was possible because from GIC's databases, only six people in Cambridge were born on the same day as the governor, half of them were men, and the governor was the only one who lived in the zip code provided by the voter rolls. The resultant data that re-identified the governor revealed information about his health and medical diagnosis.

Example[2]: Study on Netflix

As part of a competition in 2006, Netflix released data on user ratings for its movies over a six-year period. In consultation with computer scientists, Netflix applied anonymisation techniques to the data before releasing it, which included removing usernames and assigning unique identification numbers in place of the usernames in order to continuously track user ratings and trends. Despite Netflix's anonymisation attempts, researchers at the University of Texas at Austin were able to cross-relate this information with a publicly available movie database (IMDb) and uniquely identify individual Netflix users. The results of their study showed that 99% of users in the Netflix database can be identified if a person has information on when and how a user rated at least six movies.

[1] Source: http://dataprivacylab.org/dataprivacy/projects/kanonymity/index.html
[2] Source: http://epic.org/privacy/reidentification ("Netflix Cancels Contest over Privacy Concerns")

4.15 In the above cases, individuals were identified when two 'anonymised' datasets with different information were combined. One of the datasets contained information that on its own would appear to be anonymised; the other contained other information (accessible to the data recipient or publicly available), collected on a routine basis (such as voter registration information), and which includes identifying information (e.g. name). If the two datasets have at least one type of information that is the same (e.g. birth date), the anonymised information can be more easily linked to an individual. By combining information from each of these datasets, researchers can narrow down individuals, and very often, uniquely identify them. While organisations tend to focus on removing personal data identifiers, the Netflix study shows that re-identification can occur even by using non-personal data like movie ratings.

4.16 Hence, while data can be anonymised, it is not guaranteed that data will stay anonymised[3]. Re-identification of individuals by combining anonymised datasets with other information presents a significant challenge to the protection of personal data.

4.17 The autonomy of entities that may obtain the data therefore poses challenges in keeping the data anonymised. An organisation may not control, or know of other data that might potentially identify an individual when combined with the 'anonymised' data that the organisation intends to disclose. While the organisation may be satisfied that the data is not personal data, other organisations might possess information that, when combined with the 'anonymised' data, can lead to the identification of the individual. In this regard, organisations are advised to take into consideration the information that is likely to be accessed by its various divisions or business units in determining whether data has been anonymised. When determining if the data has been anonymised, there is a tendency for individual divisions to make the determination with incomplete or inaccurate information about other information or personal data held by other divisions or business units. For example, two divisions of an organisation each published what they believed to be anonymised data sets. However, the divisions were unaware of each other's publication, and therefore did not anticipate that these data sets when combined with each other, and with publically available information, yielded personal data again.

[3] Hence, the process of anonymisation is sometimes referred to as '*de-identification*', so as to reflect the process of attempting to remove personal data identifiers rather than its goal, since the goal of anonymisation may not be achieved or maintained, in which case the data therefore cannot be said to be truly 'anonymised'.

4.18 Where an organisation has collected personal data and subsequently de-identifies such personal data for processing or storage, while retaining the ability to re-identify individuals from the de-identified data, the organisation will be considered to be holding personal data. That said, the Commission does not expect an organisation to take active steps to attempt to re-identify individuals from anonymised data in order to make a determination as to whether such data is personal data held by the organisation in view of the information to which the organisation has or is likely to have access. In any case, the data should be properly safeguarded from unintended recipients, whether they are within or outside the organisation.

Assessing and managing re-identification risks

4.19 Assessing the risks of re-identification therefore goes towards determining if individuals can be re-identified from a particular set of anonymised data. Good management of re-identification risks reduces the likelihood that anonymised data will become personal data.

4.20 In reality it may be difficult to assess the availability of other data that makes re-identification possible. The likelihood of re-identification for any given anonymised data set is likely to also change over time in tandem with relevant factors. Relevant factors include greater ease of access to and volume of other information, increase in computing power and improvement in data-linking techniques. Factors like these all increase the likelihood that an individual can be identified by combining an anonymised dataset with other available information.

4.21 However, not all anonymised data bears the same risks of re-identification. The risks vary depending on factors such as the amount of alteration the data has been subject to in the course of anonymisation, the availability of other information, and the motivations for re-identification. For example, when anonymisation techniques are robust, re-identification would be more costly. The impracticality of re-identification is an important deterrent to any motivation for re-identifying anonymised data, and consequently lowers the risk of re-identification.

4.22 Furthermore, the risks of re-identification are likely to differ depending on the organisation in possession of the anonymised data. An organisation in possession of complementary information, specialised skills or technologies would more likely be capable of re-identifying individuals from the data than one who does not, assuming both have similar motivations. For example, if anonymised dataset Y were a specialised type of data (e.g. fingerprints) not easily understood by the layman, the risks of re-identifying the data would be more trivial in the hands of a person with no knowledge on that type of data, compared to one who is an expert in identifying individuals from their

fingerprints. To the lay person, it is likely that dataset Y would not be personal data but the same may not be true for the expert, who could have the skills, technologies, and complementary information for re-identification. Hence, when disclosing anonymised data to another organisation, it is important to also consider the capabilities and resources of the other organisation when ascertaining if the data is likely to be personal data to the other organisation.

Example:

Company V is an online retailer selling consumer products. As part of its effort to understand customer needs and improve its product delivery times, it analyses customer purchases to identify linkages between what products are sold at various times of the year and at which geographic locations. Company V outsources its marketing research function to Company Z. Before disclosing data on customer purchases, V anonymises the data so that only the times, locations and items purchased were left unmodified.

In this scenario, V would still be expected to protect the entire dataset as personal data if it retains the ability to re-identify a customer's purchasing patterns from that data. However, it is unlikely that Z would be considered to have collected personal data about V's customers, if Z does not possess or is unlikely to have access to any other information which can identify V's customers when combined with the purchase history provided by V.

If Z possess complementary information, for example, another dataset correlating the times of purchases made from V and the names of the individuals who made those purchases, and is able to match these information with the data provided by V, then the data provided by V is also considered personal data to Z.

4.23 Even if one has the requisite skills and information for re-identification, it does not necessarily mean that the risks of re-identification are high. The motivation to re-identify data must also be considered. The motivation to re-identify an individual may be low if there are disincentives such as legal (e.g. contractual obligations) or regulatory consequences for re-identifying individuals from data, or simply no incentive or benefit for an organisation to re-identify an individual.

4.24 Thus, in assessing the risks of re-identification when disclosing anonymised data, factors that organisations should consider include the nature or the type of data de-identified, the degree or standard of the anonymisation process, the complementary data (likely to be) available, and depending on the circumstances of disclosure, the capability of the receiving organisation as well as its motivation in re-identifying individuals from the particular data set disclosed.

4.25 Re-identification risks may be lowered in the following ways:

a) Employing robust anonymisation techniques;

b) Limiting the number of people the information is disclosed to;

c) Imposing additional enforceable restrictions on the use and subsequent disclosure of the data;

d) Implementing processes, including access restrictions, to govern proper use of the anonymised data in line with the restrictions; and

e) Implementing processes and measures for the destruction of data as soon as they no longer serve any business or legal purpose.

4.26 Various jurisdictions have considered the issue of anonymisation and re-identification risks in the context of data protection. Like many jurisdictions, the Commission will take a practical approach towards anonymisation and risks of identification. If the risk of re-identification is high, then the data will be considered personal data. If the possibility of re-identification is trivial, the Commission will consider the data anonymised.

Factors in re-identification

4.27 In this section, the Commission has adapted some of the concepts published by the UK Information Commissioner's Office (ICO) on re-identification, which it has found useful in assessing the factors that enable re-identification. First, re-identification involves identifying an individual beyond doubt. While it is possible to lower the possibility that the derived data relates to individual X rather than Y**,** it is not re-identification if there is still a possibility that the data relates to individual Y.

4.28 However, the factors that give rise to narrowing down the possibilities may contribute to re-identification, as the following sections illustrate. Another concept that is useful in ascertaining the risk of re-identification is the approach of establishing whether the other information is available publicly and if so, how easy it is to obtain the other information and how widely known the other information is.

Educated guessing

4.29 Suffice to say, re-identification involves more than making an educated guess. While matching public or established information with anonymised data can narrow down the possible identities and perhaps lead to a successful guess, this does not mean that the data is therefore personal data.

Example:

Organisation CBA published masked NRIC numbers of the winners of its recent lucky draw. The masked numbers only revealed the first 3 digits of their NRIC numbers. Since the first two digits typically reveals one's birth year, it could be ascertained that one of the winners was 28 years of age.

Around the same time, a newspaper article on the lucky draw reported that the two youngest participants were both 28 years of age. However, insofar as it was only a guess as to which of the two youngest participants might be the winner, re-identification did not occur.

However, the ability to narrow down possible identities is a factor that increases the probability of re-identification. In this example, if CBA had also published the full names of the winners, the data published by CBA could be found to have a non-trivial risk of re-identification.

Cross-relating anonymised data sets to the same unknown individual

4.30 Realising that one set of anonymised data relates to the same unknown individual in another data set does not mean that re-identification has taken place, or that personal data has been created. If that individual is singled out from the others in the set but cannot be identified, the Commission will not consider that as a case of identification or re-identification.

4.31 However, since the combination of the cross-related data sets has yielded more information than either of the data sets alone, this contributes to the information available for matching with other information that may lead to the identification of an individual.

Example:

You may know that data set A relates to the same individual X as data set B, but you may still be unable to identify who X is from the two datasets.

For example, the same person volunteers for two separate medical studies. A person administering both studies may be able to tell that the anonymised data sets below relate to the same individual, although he might not be able to identify the subject. He has simply established a connection between the two data sets.

Data Set A	Data Set B
Subject Tag: #14001	Subject Tag: #10301
Gender: Male	Gender: Male
Blood type: AB	Blood type: AB
Age: 45	Weight: 88.8kg
Weight: 88.8kg	Condition: Hypertension
Dates visited: 14, 18, 22 Jan	Dates visited: 14, 18, 22 Jan

Public knowledge and personal knowledge

4.32 The people very close to the individual or the individual himself will possess unique personal knowledge about the individual and are therefore more likely than a stranger to identify the individual from an anonymous dataset. However, just because an individual himself or someone close to him is able to identify him from an anonymised dataset does not amount to a high re-identification risk for the anonymised dataset.

4.33 Organisations should consider the types of other information required for combination with the anonymised data, and whether such information would be public knowledge (such as established facts) or must be personal knowledge, in order to assess re-identification risks. If an individual can be easily re-identified based on information that is readily available to the public, for example information in telephone directories or society membership listings, then the re-identification risks are likely to be significant. Practically speaking, if the use of personal knowledge is necessary for re-identification, it would be less likely that re-identification risks would be significant. In ascertaining the re-identification risks of an anonymised data set, one should take into account the use of public knowledge for re-identification, but not necessarily personal knowledge of the individual or the people close to the individual.

Information about groups of people

4.34 Information about groups of people may not constitute personal data if it does not identify any particular individual within the group. However such information may reveal the personal data of an individual when combined with other information, and thereby present re-identification or other risks. For example, an anonymised data set relating to a group of individuals living within a postal code reveals that they are all HIV-positive. While no individual was identified, the information reveals the personal data of one of the individuals known to be living there. Hence, if it was known that B lives in that postal code, then it would also be known that B is HIV-positive. In such cases information about groups of people is considered personal data when its combination with other information or knowledge can reveal personal data of an individual.

Anonymisation testing

4.35 To assess the robustness of anonymisation, it is recommended that organisations test anonymised datasets to determine the risk of re-identification.

4.36 For organisations that wish to publish anonymised data or employ a standard 'test' to determine whether data is sufficiently anonymised, the UK Information Commissioner's Office (ICO)'s Code of Practice "Anonymisation: Managing Data Protection Risk Code of Practice" highlights a 'motivated intruder test' that the Commission considers a useful test for the purposes of assessing re-identification risks.

4.37 The motivated intruder test considers whether individuals can be re-identified from the anonymised data by someone who is motivated, reasonably competent, has access to standard resources such as the Internet and published information such as public directories, and employs standard investigative techniques such as making enquiries of people who may have additional knowledge of the identity of the data subject. In practice, a motivated intruder test may vary in terms of 'effort' - from carrying out a few simple web searches to discover whether a combination of date of birth and postal codes can be used to reveal a particular individual's identity, to obtaining and processing publicly available but limited (e.g. national archives) resources to try to link anonymised data to an individual's identity.

4.38 In particular, the motivated intruder test would be a viable method for assessing the re-identification risks for anonymised data to be made publicly available, or where there is non-trivial risk that the anonymised data will be made publicly available through security breaches and inadvertent disclosures. The test can be applied to gauge how likely an average individual is able to successfully identify a unique individual from the anonymised data.

4.39 The motivated intruder test assumes that no particular individual has been targeted for identification and that the intruder does not resort to criminality or any specialist equipment or skills. Where disclosure of a particular dataset is to a specific recipient whose motivations, re-identification capabilities, and other information in possession of that recipient are known or can be reasonably inferred, these should also be accounted for. In addition, the risk assessment for re-identification should also consider the other risks[4] that subject the anonymised data to re-identification risks.

[4] This includes all other 'residual' risks that are not directly related to a recipient's motivation and capability to re-identify – for example, risks of the data being compromised or mistakenly disclosed to unintended recipients such as people with better ability of re-identification. The risk assessment could take into account what kind of safeguards the data is accorded, or how long the data is to be retained, among others.

4.40 As the motivated intruder test is a generic test, it is recommended that organisations carry out more robust assessments if it intends to publish data that relates to personal data of a confidential nature (e.g. sensitive medical or financial records), or where there would be negative consequences for individuals or organisations if re-identification were to happen.

4.41 While robust anonymisation is an important component of data protection, the Commission recognises that the risks of re-identification increases with the availability of other data, the sophistication of technology, as well as the motivation of re-identifying individuals from the anonymised data. A dataset that is seemingly anonymous based on current technology might be easily used to re-identify individuals with technological advancements. While organisations are expected to perform reasonable assessments of re-identification risks when disclosing anonymised datasets, commensurate with the nature of the data being anonymised and other factors described above, the Commission does not expect organisations to anticipate what is yet unknown in such risk assessments. The Commission may take into consideration an organisation's efforts to reduce re-identification risks as a mitigating factor in assessing its liability in cases where the PDPA was breached as a result of re-identification.

5 Closed-circuit television cameras ("CCTVs")

Do organisations always have to provide notifications when CCTVs are deployed?

5.1 The PDPA requires organisations to inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. Organisations should thus provide notifications in order to fulfil their obligation to obtain consent for the collection, use or disclosure of CCTV footage. Please see the sections on "The Consent Obligation" and "The Notification Obligation" in the Key Concept Guidelines for more details.

5.2 However, where consent is not required (e.g. if the collection, use or disclosure falls within an exception in the Second, Third or Fourth Schedule respectively), the PDPA does not require organisations to provide notification (unless the collection, use or disclosure is for the purpose of managing or terminating the employment relationship between the individual and the organisation). Organisations may still wish to provide notifications in such instances as good practice.

Where should notices be placed?

5.3 Notices or other forms of notifications should generally be placed so as to enable individuals to have sufficient awareness that CCTVs have been deployed for a particular purpose. For example, they could be placed at points of entry or prominent locations in a venue or a vehicle.

What should such notices state?

5.4 The PDPA does not prescribe the content of notifications. Generally, organisations should indicate that CCTVs are operating in the premises, and the purpose of the CCTVs if such purpose may not be obvious to the individual.

Is notification still required if CCTVs are there to covertly monitor the premises for security reasons, and notification would defeat the purpose of using the CCTVs?

5.5 The Commission does not require the placement or content of notifications to reveal the exact location of the CCTVs. Organisations may provide notice that CCTVs are deployed in the general locale instead of indicating the specific points where the CCTVs are installed. Where personal data may be collected without consent (e.g. where the personal data is publicly available), notification will not be required by the PDPA, although organisations are advised to provide notification as good practice.

Example:

XYZ deploys CCTVs for security purposes at the entrance to its office premises. It provides a notification at the entrance to its office, which clearly and prominently states the use and purpose video surveillance. Such notification would be considered sufficient for the XYZ's purpose.

If my organisation installs CCTVs that also capture video footage beyond the boundaries of our premises, is that allowed?

5.6 The PDPA requires that an organisation consider what a reasonable person would consider appropriate under the circumstances in meeting its obligations under the PDPA. An organisation may not be prohibited by the PDPA from having CCTVs that collect footage beyond the boundaries of its premises. Organisations should however consider the extent of coverage that is reasonable for the purpose of installing the CCTVs. Organisations should put in place appropriate notification in all areas where personal data would be collected by the CCTV, and obtain consent for such collection, unless consent is not required because one of the exceptions in the Second Schedule of the PDPA apply.

5.7 However, the organisation should bear in mind that there may be other considerations that may affect its ability to collect CCTV footage of areas beyond its premises (e.g. limits on filming of restricted areas).

Access to CCTV footage

Is an organisation required to provide access to CCTV footage if it shows other individuals and the organisation doesn't have the technical ability or it is too costly to mask the other individuals?

5.8 Generally, an organisation is required to provide for standard types of access requests. In the case of CCTV footage, this would include being able to provide access to CCTV footage where the images of other individuals present in the CCTV footage are masked as required (e.g. where consent of the individuals for such disclosure is required, but has not been obtained).

5.9 An organisation should provide access so long as the applicant agrees to pay the minimal fee for the access request, unless a relevant exception in the Fifth Schedule applies. For example, organisations are not required to provide access if the request is frivolous or vexatious, or if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest. If an organisation intends to rely

on this or other exceptions from the requirement to provide access provided for in the Fifth Schedule, it should be able to provide supporting evidence to justify its decision.

Is an organisation required to provide a copy of CCTV footage pursuant to an access request for the footage?

5.10 Organisations should provide a copy of the CCTV footage and have the option of charging the individual a minimal fee for producing the copy.

5.11 If the CCTV footage resides in a form that cannot be provided to the individual in physical or electronic copies, (e.g. the data cannot be extracted from a special machine owned by the organisation), or if it is prohibitively costly to provide the footage in the aforementioned formats, then the organisation may provide the individual a reasonable opportunity to examine the requested data in person, with appropriate masking of the images of other individuals where required.

Can compromising an organisation's security arrangements or competitive position be sufficient reason to deny access to CCTV footage?

5.12 The Commission's view is that compromising an organisation's security arrangements or harming an organisation's competitive position could be a sufficient reason to deny access to CCTV footage. An example would be where the provision of the personal data in the CCTV footage could reasonably be expected to threaten the safety of another individual. However, where an organisation denies access on this basis, the Commission expects an organisation to be able to provide strong justifications as to why it is unable to accede to the request. The Commission will have to make a determination based on the facts of the particular case, should a complaint be received.

Can individuals make joint access requests for CCTV footage containing their images, if they consent to their own images being viewed by the others making the joint request?

5.13 Yes. The PDPA does not specifically prescribe whether joint access requests are permissible. However, the Commission is of the view that it would be reasonable for certain groups of individuals (e.g. a married couple, parents of a class of students etc.) to jointly make an access request. Organisations may apply the same considerations in determining whether to provide access as they would for a request made by a single individual.

Is an organisation required to accede to requests to delete CCTV footage?

5.14 No. The PDPA does not require an organisation to delete personal data upon request from an individual. Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

Is there a requirement that CCTV footage or video stills be of minimum resolution when provided to individuals upon request?

5.15 The PDPA does not prescribe any minimum resolution. However, given that the requirement is for the organisation to provide the personal data in its possession or under its control, the organisation should provide the CCTV footage in the form and of the resolution it holds for its purposes.

Can the organisation require that the individual sign a contract to agree not to disclose to any third party the CCTV video to be provided to him?

5.16 The PDPA does not prohibit this. However, such a contract would not override any rights or obligations under the PDPA. Organisations should also note that individuals acting in a personal or domestic capacity are not subject to the Data Protection provisions of the PDPA.

6 Employment

Does an organisation need to seek the consent of a job applicant for the collection and use of his personal data?

6.1 Organisations may receive personal data from job applicants who provide it voluntarily through a job application, either in response to a recruitment advertisement or otherwise.

6.2 When an individual voluntarily provides his personal data to an organisation in the form of a job application, he may be deemed to consent to the organisation collecting, using and disclosing the personal data for the purpose of assessing his job application. If the individual is subsequently employed, it would be reasonable for the organisation to continue to use the personal data provided by the individual in the job application form for the purpose of managing the employment relationship with the individual, if required. If the organisation wishes to use the personal data for purposes for which consent may not be deemed or to which there is no applicable exception under the PDPA, the organisation must then inform the individual of those purposes and obtain his consent, unless relevant exceptions apply. Please see the section on The Consent Obligation in the Key Concept Guidelines for more details.

Can organisations collect and use personal data on the job applicant from social networking sources (e.g. Facebook or Twitter)?

6.3 The PDPA does not require organisations to obtain the consent of the individual when collecting personal data that is publicly available. Examples of publicly available sources are newspapers, telephone directories and websites containing content which is generally available to the public. Where social networking sources are publicly available, the PDPA does not prohibit organisations from collecting personal data about the individual without his consent. Please refer to the section on “The Consent Obligation” in the Key Concept Guidelines for more explanation of the ‘publicly available data’ exception.

Can organisations or recruitment agencies collect and use personal data on individuals from social networking sites or publicly available sources to contact them for prospective job opportunities?

6.4 The PDPA does not require organisations to obtain the consent of the individual when collecting or using personal data that is publicly available. Where the personal data is not publicly available, but is voluntarily made available by the individual on a job-search portal for being contacted for prospective job opportunities, the individual may be deemed to have consented to the collection, use and disclosure of his personal data for such purpose.

Can organisations use the information in business cards for recruitment?

6.5 The Data Protection Provisions in the PDPA do not apply to "business contact information", which is defined in the PDPA as:

"an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

6.6 If the individual provided his business card for purposes other than solely for personal purposes, then the organisation is not required to comply with the Data Protection Provisions of the PDPA in respect of the contact information set out in the business card.

Example:

At the registration booth of a corporate seminar, Sharon drops her business name card into a glass bowl by the side of the registration booth as she wishes to be on the seminar organiser's mailing list for future invitations to similar seminars.

Sharon's business name card contains her name, position, business telephone number, business address, business electronic mail address and business fax number. As Sharon did not provide her business name card solely for personal purposes, the information on it will be considered business contact information. The PDPA does not apply and the seminar organiser does not need to seek Sharon's consent to use the information on her business name card.

How long can an organisation keep the personal data of job applicants who are not hired?

6.7 After an organisation has decided which job applicant to hire, the personal data that the organisation had collected from the other job applicants should only be kept for as long as it is necessary for business or legal purposes. Organisations should note that job applicants have the right to obtain access and request corrections to their personal data held by the organisation. Please see the section on "The Access and Correction Obligation" in the Key Concept Guidelines for more details.

Can job applicants ask the organisation to reveal how much information the organisation has on them or find out why they were not selected?

6.8 Under the PDPA, individuals have the right to obtain access and request corrections to their personal data held by organisations. Upon request, the organisation must also inform the individual of the ways in which the personal data had been used for the past year. Thus, organisations must reveal to the job applicant who requests so, the personal data the organisation has on them. There are however exceptions to this obligation to provide access to personal data, including several mandatory exceptions. Please refer to the section on "The Access and Correction Obligation" in the Key Concept Guidelines for more details.

6.9 For example, if the personal data in question is opinion data kept solely for an evaluative purpose, organisations are not required to provide the requested information to the individual. This means that organisations will not need to inform a job applicant of the opinions which were formed about him in the course of determining his suitability and eligibility for the job.

How does the PDPA apply to recruitment agencies?

6.10 Recruitment companies, employment agencies, head-hunters and other similar organisations (henceforth 'recruitment agencies') are subject to the Data Protection Provisions of the PDPA. Accordingly, unless an exception under the PDPA applies, recruitment agencies will have to inform job applicants of the purposes for which they are collecting using or disclosing their personal data, and obtain consent before doing so.

6.11 Recruitment agencies that are acting as data intermediaries are required to comply with fewer obligations under the PDPA. The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the provisions in the PDPA relating to the safeguarding and retention of personal data in respect of such processing. In certain circumstances these recruitment agencies could qualify as data intermediaries. For more information on data intermediaries, please refer to the section on "Excluded Organisations" in the Key Concept Guidelines.

6.12 Recruitment agencies should also note that a message sent solely to promote an employment opportunity would not be regarded as a specified message and would not be subject to the Do Not Call Provisions. Please refer to the section on the "Do Not Call Provisions" in the Key Concept Guidelines for more information.

Personal Data of Employees

How does the PDPA apply to employment records of employees?

6.13 Most organisations maintain some form of employment records on their current employees, which may include contact information, resumes, performance indicators and remuneration histories. Organisations should inform the employees of the purposes for the collection, use and disclosure of their personal data and obtain their consent prior to the collection, use and disclosure (as the case may be).

6.14 In many cases, consent could be obtained at the point of appointing the new employee. It may, however, also be necessary to obtain consent at various points during the employment relationship when the organisation requires more personal data or intends to use or disclose the employee's personal data for other purposes. Please also note that even if consent is given, employees may withdraw that consent under the PDPA.

6.15 Employers should also note that even if an exception applies such that consent need not be sought, the exception does not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, employers are required to comply with their other legal obligations, for example, to protect confidential information of their employees or under the employment contract.

Collecting, using and disclosing employee personal data for evaluative purposes

6.16 Organisations may collect, use and disclose personal data without consent where this is necessary for evaluative purposes. (This is set out as exception 1(f) in the Second Schedule, 1(f) in the Third Schedule and 1(h) in the Fourth Schedule respectively). The term "evaluative purpose" is defined in section 2(1) of the PDPA and includes, amongst other things, the purpose of determining the suitability, eligibility or qualifications of an individual for employment, promotion in employment or continuance in employment.

6.17 Hence, the evaluative purpose exception allows employers to collect, use and disclose personal data without the consent of the individual or employee concerned for various purposes that are common in the employment context, for example:

a) Obtaining a reference from a prospective employee's former employer to determine his suitability for employment; or

b) Obtaining performance records or other relevant information or opinions to determine the performance of an employee.

Collecting, using and disclosing personal data for the purpose of managing or terminating an employment relationship between the organisation and the individual

6.18 Under the PDPA, the collection by organisations of personal data from their employees that is reasonable for the purpose of managing or terminating their employment relationships, and the use or disclosure of such personal data for consistent purposes would not require the consent of their employees. This is pursuant to exception 1(o) in the Second Schedule, 1(j) in the Third Schedule and 1(s) in the Fourth Schedule respectively. While consent is not required, employers are required to notify their employees of the purposes of such collection, use or disclosure.

6.19 The PDPA does not prescribe the manner of notification and organisations should determine the form and manner that would provide the individual with the required information that allows him to understand the purposes for which his personal data would be collected, used and disclosed. For example, organisations may determine in the particular circumstances if it would be appropriate to inform their employees of these purposes through employment contracts, employee handbooks, or notices in the company intranet. Organisations should also keep their employees updated about new purposes for which an employee's personal data may be collected, used and disclosed without consent. For the avoidance of doubt, where an organisation has sufficiently provided a general notification to employees on the purposes for which their personal data may be collected, used and disclosed, for example for performance appraisals, the Commission does not expect organisations to notify employees of the same purpose prior to each time that the organisation engages in such activities. Please refer to the section on "The Notification Obligation" in the Key Concept Guidelines for more details.

6.20 Purposes that could fall within the purpose of managing or terminating an employment relationship can include:

a) Using the employee's bank account details to issue salaries;

b) Monitoring how the employee uses company computer network resources;

c) Posting employees' photographs on the staff directory page on the company intranet; and

d) Managing staff benefit schemes like training or educational subsidies.

6.21 Employers would need to seek consent for purposes that are not related to, or the collection of personal data that is not relevant to the management or termination of an employment relationship (unless any other exception under the PDPA applies). In particular, employers would need to obtain consent when collecting, using or disclosing employee personal data for business or client purposes not related to managing or terminating an employment relationship.

Example:

Organisation ABC engages a courier company to deliver a parcel to organisation XYZ. XYZ requires the full name and NRIC number (personal data) of the employee which will be dispatched by the courier for this

delivery for the purposes of allowing the courier to enter XYZ's office premises. Before disclosing the personal data of its employee, the courier company should obtain the employee's consent to do so.

Such consent can be obtained on a case by case basis, or once-off through the employment contract or other appropriate means.

What is the difference between the exception for evaluative purposes and the exception for the purpose of managing and terminating an employment relationship?

6.22 There are instances where employers have to collect the same set of personal data for both the purposes of (i) managing or terminating the employment relationship and (ii) evaluation. The difference between the two purposes lies in the requirement to notify individuals for purpose (i) but not for purpose (ii). In other words, employers need only inform employees of the purpose for managing and terminating the employment relationship, and not of the evaluative purpose.

Example:

An employer collects information about the projects an employee has worked on to determine whether to promote him (an evaluative purpose), and to conduct audits on his finance claims (a purpose for managing and terminating an employment relationship)**.**

The employer need only notify the employee that his personal data is being collected for audit purposes. The employer does not need to obtain consent from the employee for the collection of his personal data or inform him that he is being evaluated for promotion to a higher job grade.

6.23 Employers should note that even though some exceptions in the PDPA can apply in the employment context, organisations should still act based on what a reasonable person would consider appropriate in the circumstances. Please see the section on "Reasonableness" in the Key Concept Guidelines for more details.

How long can organisations continue to hold personal data of former employees?

6.24 Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes. The Retention Limitation Obligation does not specify a fixed duration of time for which an organisation can retain personal data as each organisation has its own specific business needs.

6.25 Organisations may continue to retain personal data about the former employee that was collected during his employment period for as long as there is a valid business or legal purpose. For example, organisations that have a policy of retaining personal data of former employees for the purpose of considering them for future job opportunities can continue to do so as a valid business purpose. However, organisations should not retain personal data without a clearly defined purpose. Organisations should note that holding personal data for an indeterminate duration of time increases the risk of a contravention of the Data Protection Provisions, as organisations have other obligations in relation to the personal data held. Please see the section on the "Retention Limitation Obligation" in the Key Concepts guidelines for more information.

Are organisations responsible if their employees do not comply with the PDPA? Are volunteers considered employees?

6.26 Under the PDPA, an organisation is responsible for the personal data in its possession or under its control, including for any breaches of the PDPA caused by their employees acting in the course of their employment. In particular, any act done or conduct engaged in by an employee in the course of his employment shall be treated as done or engaged in by his employer, whether or not it was done or engaged in with the employer's knowledge or approval.

6.27 In relation to offences under the PDPA by an employee of an organisation, the organisation will not be liable if it took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct that constitutes the offence. Organisations should develop and implement policies and practices that comply with the PDPA, and communicate such policies and practices to their employees.

6.28 Organisations should note that the PDPA defines "employee" to include a volunteer, and "employment" to include working under an unpaid volunteer work relationship.

Do the exceptions to the Consent Obligation for the collection, use and disclosure of personal data of employees also apply to individuals that may act on behalf of an organisation, but are not the organisation's employees?

6.29 The exception relating to "managing or terminating an employment relationship" only apply when there is an employment relationship. Where an organisation is collecting the personal data of individuals that are not its employees for a specific purpose, this specific exception would not apply. However, other exceptions may apply, for example where the organisation is required under written law to collect personal data of such individuals in order to assess whether the qualifications of such individuals comply with regulatory requirements.

7 NRIC Numbers

How does the PDPA apply to NRIC numbers?

7.1 The Commission is aware that NRIC numbers are of special concern to individuals as they are unique to each individual and are used in many official transactions with the government.

7.2 Under the PDPA, individuals have to be informed of and consent to the purposes for which their personal data, including NRIC numbers, are collected, used, and disclosed by organisations.

7.3 As NRIC numbers are widely used for various business purposes, organisations are advised to review their processes which involve NRIC numbers to ensure compliance with the PDPA. For example, organisations should ensure that they protect NRIC numbers from accidental disclosure using appropriate security measures.

7.4 As a best practice, organisations should avoid over-collecting personal data, including NRIC numbers, where this is not required for their business or legal purposes. Organisations should consider whether there may be alternatives available that address their requirements.

7.5 The Commission notes that there are situations where the collection of NRIC numbers by organisations for verification or identification purposes leads to a reduced need to collect other forms of personal data. Such situations would be in line with the good practice of not over-collecting personal data.

> Example:
>
> John calls his service provider to make some queries concerning the services he has subscribed for. Instead of asking for John's NRIC number, the service provider could ask for other information such as John's account number or mobile number to verify his identity, if the service provider would already have such other information about John in the course of providing the service.

Can organisations collect NRIC cards?

7.6 Policies governing the collection and retention of the physical NRIC card are not governed by the PDPA. However, NRIC cards contain personal data and hence organisations that collect NRIC cards and the personal data on it would be subject to the PDPA in relation to the collection of such personal data.

For what business purposes are organisations allowed to use NRIC numbers?

7.7 The PDPA allows organisations to use NRIC numbers collected for reasonable purposes for which consent has been obtained validly under the PDPA. However, organisations should consider the potential consequences of using NRIC numbers for a particular purpose.

7.8 For example, organisations that use NRIC numbers as user names or membership numbers might be disclosing personal data to third parties without consent.

> Example:
>
> Jane is visiting her friend who lives in a private condominium. The security guard asks for Jane's full name and NRIC number, for the purpose of checking it against the guest list provided by the residents.
>
> In this situation, the security guard is collecting Jane's personal data for a reasonable purpose. The security guard should make reasonable security arrangements to protect Jane's personal data – for example, to prevent unauthorised disclosure to subsequent visitors.

How does the PDPA apply to organisations publishing NRIC numbers for purposes such as to publish the results of lucky draws or other contests?

7.9 Organisations may publish NRIC numbers if consent had been obtained from the individual(s) concerned. However, as a good practice organisations should only publish as much personal data as necessary to fulfil the relevant purpose. For example, when publishing personal data of the winners of a lucky draw, organisations are advised to reveal only a portion of the NRIC number such as the last three digits and the letter. Organisations should use the full NRIC number only when necessary, for example to confirm the identity of someone who is coming forth to receive the winning prize.

8 Online Activities

Are IP addresses personal data?

8.1 IP addresses of networked devices are automatically captured whenever a connection is made over the Internet. An IP address, or any other network identifier such as an IMEI number, may not be personal data when viewed in isolation, because it simply identifies a networked device. However, IP addresses have the potential of identifying unique individuals through their activities, especially when combined with traces of information that individuals leave on these networked devices as they interact with the Internet. Depending on how a device is used, the traces of information are collected and the presence of other available information affects the possibility of identifying an individual from his device's IP address.

8.2 For instance, a shared computer may be used by several individuals in an office or home with the same login account and it is therefore unlikely for the IP address to be connected to a single individual. However, if each individual has separate login accounts, then the online activities will relate to that login identity. Along with other information such as cookies (addressed below), IP addresses can identify individuals, and are likely to be personal data in such context.

8.3 The Commission notes that organisations do engage in the collection of data points tied to an IP address for various purposes. For example, such purposes could include determining the number of unique visitors to a website in a month, or the number of unique responses to a once-off online survey about consumer preferences, organisations may track activities tied to an IP address. Such tracking may not result in the collection of personal data, if the organisation is unable to identify an individual from the data collected or from that data and other information that the organisation has or is likely to have access. However, organisations should note that the more data points associated to a unique IP address an organisation collects, the more likely that the data may be personal data. For example, if an organisation profiles the websites visited by an IP address, the items purchased by the same IP address and other online activities associated to the IP address for a long period of time, and is able to ascertain that the particular IP address is associated with a unique person with a specific surfing profile, the organisation may be found to have collected personal data.

8.4 For more details on what constitutes personal data is, please refer to the section on "personal data" in the Key Concepts guidelines.

Must consent be obtained for the use of cookies?

8.5 Cookies are text files created on a client computer when its web browser loads a website or web application. Often encrypted for protection against unauthorised access, they are used to store information for performing certain functions such as completing forms, facilitating website navigation, authentication, and enabling advertising technology. Depending on the purpose(s) for which they are used, the durations which cookies are stored differ. Session cookies typically expire at the end of a browser session, while persistent cookies can be stored for some duration in a browser folder until they are deleted, either manually, or upon browser exit. Also depending on the purpose of the cookies is the type of information that they store. The PDPA applies to the collection, use, or disclosure of personal data using cookies.

8.6 Many Internet activities today are dependent on the use of cookies, such that unnecessarily restricting the use of cookies will impede the usability of the Internet. However, because cookies can potentially collect personal data, organisations should be mindful of the concern surrounding the use of cookies for individuals' online activities. It is thus important to strike a balanced approach on the need for consent in the use of cookies.

8.7 First, not all cookies collect personal data. For example, session cookies may only collect and store technical data needed to play back a video on a website. Consent is not needed for cookies that do not collect personal data.

8.8 Second, for Internet activities that the user has clearly requested, there may not be a need to seek consent for the use of cookies to collect, use, and disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provided his personal data for such purposes. Such activities include (but are not limited to) transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase. For activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he would do so. Please refer to the section on "The Consent Obligation – Deemed Consent" in the Key Concept Guidelines for more details.

8.9 Consent may also be reflected in the way a user configures his interaction with the Internet. If the individual configures his browser to accept certain cookies but rejects others, he may be found to have consented to the collection, use and disclosure of his personal data by the cookies that he has chosen to accept. For example, if the individual has configured his browser settings to reject all cookies except those from his online banking website and his email websites, it is clear that he has consented to the collection, use and disclosure of his personal data by his banking and email websites for their stated purposes, but not other websites. However, the mere failure of an individual to actively manage his browser settings does not imply that the individual has consented to the collection, use and disclosure of his personal data by all websites for their stated purpose.

8.10 For avoidance of doubt, the obligation to obtain the individual's consent for the collection of his personal data rests with the organisation that is collecting such personal data, whether by itself or through its data intermediaries. Where an organisation operates a website which a third party uses to collect personal data, and the website operator itself is not collecting such personal data, the obligation is on the third party organisation to obtain the consent required to collect such personal data.

Are organisations allowed to use cookies for behavioural targeting?

8.11 Where behavioural targeting involves the collection and use of personal data, the individual's consent is required.

END OF DOCUMENT