PUBLIC CONSULTATION ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

PROPOSED ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS

05 FEBRUARY 2013

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.

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 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.

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 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.

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 in its original state. 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 identified 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 identifiers with other references. For example, replacing an individual's name with a tag or reference number.

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 X 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 numbers on a credit card as 4346 XXXX XXXX 5379 instead of '4346 6454 0020 5379'.

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 it could still identify individuals from dataset X. For example, an organisation could identify individuals by combining dataset X with other information the organisation is likely to have access to, or by reversing the anonymisation process 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.

4.10 Dataset X, however, would cease to be personal data if the organisation is no longer able to identify an individual from it.

Challenges and limitations in anonymising data

4.11 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 the 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.

4.12 The autonomy of entities controlling the data also 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 or disclose information that, when combined with the 'anonymised' data, can lead to the identification of the individual. Further details on the risks of re-identification are discussed below.

4.13 Organisations are advised to take into consideration the information controlled by its various divisions in determining whether data has been anonymised. There is a tendency for individual divisions to consider only local factors when determining if the data has been anonymised, or to make the determination with incomplete or inaccurate information about other information or personal data held by other divisions.

4.14 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.

4.15 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 and incomes were suppressed in ranges, the residential addresses substituted with a generic geographical area, and the occupations removed, then useful information would have been lost, and the anonymised database would not yield conclusions about customers' profiles that are as useful as those derived from the original database. An organisation will therefore have to consider whether the anonymised data would still be suitable for its intended purposes.

The effectiveness of anonymisation

4.16 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.

4.17 Re-identification is the process by which anonymised data is combined with other information such that an individual can be identified and therefore becomes 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

[1] Source: http://dataprivacylab.org/dataprivacy/projects/kanonymity/index.html

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.

4.18 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). The two datasets will usually have at least one type of information that is the same (e.g. birth date), which links the anonymised information 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.

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

[2] Source: http://epic.org/privacy/reidentification

Managing re-identification risks

4.20 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.

4.21 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 cannot be pre-determined as the risks 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 information.

4.22 However, not all anonymised data bears the same risks of re-identification. Depending on factors such as the amount of alteration the data has been subjected to in the course of anonymisation, the availability of other information, and the motivations for re-identification, the risks vary.

4.23 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.

4.24 In assessing the risks of re-identification when disclosing anonymised data, organisations should consider the risk of the receiving organisation being able to re-identify an individual. The likelihood that the receiving organisation would attempt to re-identify an individual from the anonymised data is also a consideration.

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

a) Limiting disclosure to restricted persons;

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

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

d) Implementing processes and measures for the destruction of data as soon as possible.

4.26 For organisations that wish to publish anonymised data or employ a '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.

4.27 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 resources such as the Internet and published information, and employs standard investigative techniques such as making enquiries of people who may have additional knowledge of the identity of the data subject. 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.

4.28 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. The test may not be relevant when it is known who the data recipient is, what his re-identification capabilities are, and what other information he possesses. In this case, the risk assessment for re-identification should take these into account. In addition, as the motivated intruder test is a generic test, it is recommended that organisations carry out more stringent assessments for publishing data that relates to personal data of a confidential nature (e.g. medical records), or where there would be negative consequences for individuals or organisations if re-identification were to happen.

Factors in re-identification

4.29 In this section, we have adapted some of UK ICO's concepts on re-identification, which we have 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.

4.30 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

4.31 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 a disclosure of personal data has taken place.

4.32 For example, the newspapers published an anonymised story of a blue sports car running a red light at Marina Bay Sands area. Although it may be public knowledge that a popular local actor, Actor X, drives a blue sports car and frequents Marina Bay Sands, guessing that the actor ran the red light does not mean re-identifying him from the anonymised newspaper report. Even though the guess might turn out to be correct, re-identification did not occur because it was not proven who ran the red light. However, the ability to narrow down possibilities is a factor that increases the probability of re-identification.

Cross-relating anonymised data sets to the same unknown individual

4.33 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.

4.34 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 identify 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

4.35 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.

4.36 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

4.37 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

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

5 Employment

How the PDPA applies to recruitment processes

5.1 During the process of recruitment, organisations often collect large amounts of personal data from job applicants. Generally, organisations must comply with the Data Protection Provisions in respect of such personal data. In particular, organisations should notify individuals of the purposes for which the organisation is collecting, using or disclosing their personal data and obtain consent to do so, unless any exception under the PDPA applies. Please refer to the sections on "The Consent Obligation" and "The Notification Obligation" in the Key Concept Guidelines for more details.

5.2 Organisations should therefore ensure that the policies and practices they develop and implement will enable them to meet their obligations under the PDPA during recruitment processes.

How does the PDPA apply to reference checks during recruitment?

5.3 The PDPA provides for certain exceptions where organisations are not required to obtain the consent of the individual to collect, use or disclose personal data. One of those exceptions applies where the collection, use or disclosure of personal data is necessary for 'evaluative purposes'. Please refer to the PDPA for the full definition of this exception.

5.4 The 'evaluative purpose' exception allows organisations to collect, use or disclose personal data without consent if is for the purposes of determining the suitability, eligibility or qualifications of the job applicant for a job. For example, an organisation is not required to obtain consent to collect information about the job applicant from their referees or from ex-employers, if such collection is necessary for the organisation to evaluate the job applicant for employment.

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

5.5 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.

5.6 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 organisation wishes to use the personal data for other purposes, 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)?

5.7 The PDPA does not require organisations to obtain the consent of the job applicant 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 use the information in business cards for recruitment?

5.8 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".

5.9 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 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 her personal data for recruitment purposes.

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

5.10 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?

5.11 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.

5.12 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?

5.13 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.

5.14 For recruitment agencies that are acting as data intermediaries, there may be a partial exclusion from the 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.

Personal Data of Employees

How does the PDPA apply to employment records of employees?

5.15 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).

5.16 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.

5.17 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.

How does the PDPA apply to employers assessing the performance of employees for promotion or for termination?

5.18 The collection of the personal data of an employee that is necessary for determining the suitability, eligibility or qualifications of the employee for promotion, continuing their employment contract, or for terminating their employment contract is an exception to the requirement for consent. An organisation may obtain information about the employee from their manager or from ex-employers without the consent of the employee, if such collection is necessary for the organisation to evaluate the employee.

Can organisations monitor their employees' use of company equipment or network?

5.19 Under the PDPA, the collection by organisations of personal data from their employees 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. Using the employee's bank account details to issue salaries, or monitoring how the employee uses company computer network resources are possible purposes which may fall under this exception. However, the PDPA requires organisations to inform their employees of the purposes of such collection, use or disclosure, even though their consent is not required.

5.20 The PDPA does not prescribe the manner of notification and as a general guide, an organisation should determine the form and manner that would provide the individual with the required information that allows him to understand the purposes. Organisations may consider if it would be appropriate in the circumstances to inform their employees through employment contracts, employee handbooks, or notices in the company intranet. As and when organisations have new purposes related to managing and terminating employment relationships, organisations may also have to notify their employees through corporate email accounts and internal memos or otherwise. Please refer to the section on "The Notification Obligation" in the Key Concept Guidelines for more details.

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

5.21 The exception for personal data necessary for evaluative purposes is meant to apply only in cases where the suitability, eligibility and qualifications of the employee is being evaluated, resulting in an analysis or an opinion of the employee. The exception for managing and terminating employment relationships is meant to apply to more administrative operations, such as the use of personal data for payment.

5.22 There are however instances where the collection of the personal data is necessary for an evaluative purpose and also reasonable for the purpose of managing or terminating the employment relationship, for example, the collection of performance assessments may be necessary for both an evaluation of the employee for a promotion, and reasonable for the determination of his salary. In such overlaps, the organisation need not obtain consent from the employee nor inform him of the evaluation being carried out, but would still be required to notify the employee that the performance assessments are to be collected for purposes of managing the employment relationship with him.

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

5.23 Even after the employee is no longer working with the organisation, the organisation may continue to retain personal data about the former employee that was collected during his employment period for a period of time. The organisation should cease to retain such personal data if it has no business or legal purposes to do so.

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

5.24 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.

5.25 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 NRIC Numbers

How does the PDPA apply to NRIC numbers?

6.1 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.

6.2 While the PDPA does not contain provisions which apply exclusively to NRIC numbers, they are generally considered personal data and are thus governed by the PDPA. Under the PDPA, individuals have to be informed of and consent to the purposes for which their NRIC numbers are collected, used, and disclosed by organisations. Organisations are not allowed to use NRIC numbers for any purpose unless prior consent from the individual has been obtained

6.3 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.

6.4 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.

6.5 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 telecom service provider, Operator X to make some queries concerning the services he has subscribed for. Instead of asking for John's NRIC number, Operator X could ask for other information such as John's account number or date of birth to verify his identity.

Can organisations collect NRIC cards?

6.6 The PDPA does not govern organisations' collection of the physical NRIC card. However, NRIC cards contain personal data and hence organisations which collect NRIC cards would be subject to the PDPA.

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

6.7 The PDPA allows organisations to use NRIC numbers collected for 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.

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

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

6.9 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.

7 Online Activities

Are IP addresses personal data?

7.1 IP addresses of networked devices are automatically captured whenever a connection is made over the Internet. An IP address in isolation may not be personal data, 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.

7.2 For example, a shared computer may be used by several individuals in an office 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.

7.3 The Commission will not consider an IP address in itself as personal data unless an individual can be identified from the IP address and other available information such as recorded information (e.g. information recorded on the devices), established fact, and personal knowledge.

7.4 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?

7.5 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.

7.6 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.

7.7 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.

7.8 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.

7.9 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 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.

Are organisations allowed to use cookies for behavioural targeting?

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

END OF DOCUMENT