PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS

Issued 24 September 2013
Revised 17 May 2022

TABLE OF CONTENTS

PART I: INTRODUCTION AND OVERVIEW

1 Introduction

1.1 The Personal Data Protection Act 2012 (the "PDPA") establishes a 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 Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines" and are subject to the disclaimers set out therein[1].

1.3 It should be noted that the examples in these Guidelines serve to illustrate particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario.

[1]Available at http://www.pdpc.gov.sg/ag

PART II: SELECTED TOPICS

2 Analytics and Research

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

2.1 Where the analytics and research activities carried out by the organisation involve the collection, use or disclosure of personal data, the organisation is required to comply with the PDPA. We encourage organisations to use anonymised data as far as possible for analytics and research as anonymised data is not personal data and thus would not be governed by the PDPA. This would minimise any risk for the organisation of a data breach. Please refer to the chapter on "Anonymisation" in these Guidelines for more details.

2.2 If personal data is used, 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 Chapters 12 and 14 on "The Consent Obligation" and "The Notification Obligation" in the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines") for more details.

2.3 However, the PDPA provides several exceptions for organisations to use personal data without consent of the individual for analytics and research provided that organisations can meet the requirements and put in place safeguards. Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule ("business improvement exception") allows organisations to use, without consent, personal data that they had collected in accordance with the Data Protection Provisions of the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes[2]:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

[2] "Relevant purposes" are defined in paragraph 1(2) under Part 5 of the First Schedule to the PDPA.

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

2.4 In order to rely on the business improvement exception, organisations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and

b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

2.5	**Examples:** 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 analytics to improve operations and services would likely fall within the business improvement exception which the company can leverage to conduct research for service or product enhancements.
2.6	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. Such analysis to identify suitable services would likely fall within the business improvement exception. However, the company cannot send direct marketing messages to the emergency contact, unless it has obtained consent to do so.

2.7 The PDPA also allows organisations to use personal data without consent for more upstream research that may not be immediately directed at business improvements. Division 3 under Part 2 of the Second Schedule to the PDPA ("research exception") provides that organisations may **use** personal data for a research purpose, including historical and statistical research, subject to the following conditions:

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

b) There is a clear public benefit to using the personal data for the research purpose;

c) The results of the research will not be used to make any decision that affects the individual; and

d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual.

2.8 For more details on the research and business improvement exceptions, please refer to Chapter 12 of the Key Concepts Guidelines.

Are organisations allowed to retain personal data of individuals for analytics and research?

2.9 Organisations should not retain personal data for longer than is necessary unless they have legal or business reasons to do so. Retention of personal data for analytics and research purposes is a valid business reason, if there is an immediate and demonstrable intent to perform analysis or conduct research. Organisations may demonstrate their intention through relevant programmes or departmental functions. Organisations should establish policies and practices when retaining personal data for analytics and research, such as the retention period and considering ways to anonymise the personal data. Please refer to Chapter 18 of the Key Concepts Guidelines for more details on the Retention Limitation Obligation.

3 Anonymisation

What is anonymisation?

3.1 The term 'anonymisation' refers to the process of converting personal data into data that cannot identify any particular individual and, depending on the specific process used, can be reversible or irreversible. The reversibility of the specific process used would be a relevant consideration for organisations when managing the risk of re-identification.

3.2 Some jurisdictions use 'anonymisation' and 'de-identification' interchangeably to refer to the process of converting personal data into data that can no longer be used to identify an individual, whether alone or in combination with other available information. Others use 'anonymisation' to refer to de-identification that is irreversible. PDPC views 'de-identification' as referring to only the removal of direct identifiers and does not equate it with 'anonymisation'. A de-identified dataset may be easily re-identified when combined with data that may be publicly or easily accessible.

3.3 A data record typically comprises different data attributes with varying degrees of identifiability and sensitivity levels to an individual:

a) Direct identifier: this refers to a data attribute that is unique to an individual (e.g. full name or mobile number and can be used as a key data attribute to re-identify an individual in a dataset). This data attribute is typically publicly or easily accessible.

b) Indirect identifier: this refers to a data attribute that is not unique to an individual but may re-identify an individual when combined with other information (e.g. age and postal code). This data attribute is typically publicly or easily accessible.

c) Target attributes: in the context of assessing adequacy of anonymisation, this refers to a data attribute that may be sensitive in nature and may result in a high potential adverse effect to an individual when disclosed. This data attribute is usually not publicly or easily accessible (e.g. health or credit information).

3.4 Anonymisation involves a set of risk management controls. Data would not be considered anonymised if there is a serious possibility that an individual could be re-identified, taking into consideration both:

a) the data itself, or the data combined with other information to which the recipient organisation has or is likely to have access to; and

b) the measures and safeguards (or lack thereof) implemented by the organisation to mitigate the risk of re-identification.

3.5 Data that has been anonymised is no longer considered personal data for the purposes of the PDPA. As the effectiveness of anonymisation may degrade over time, periodic reviews should be conducted to be assured that the data remains anonymised and measures that deal with re-identification risks remain adequate.

3.6 Re-identification refers to the identification of individuals from a dataset that was previously de-identified or anonymised. It can occur as a result of combining separate datasets. When determining whether a dataset is anonymised, the organisation should consider whether there is a serious possibility that an individual can be identified from the dataset when it is combined with other information that the data recipient has or is likely to have access to, by carrying out an assessment of the risk of re-identification. In general, factors affecting the risk of re-identification include the amount of alteration the data has been subjected to in the course of anonymisation, the extent of disclosure, the availability of other relevant information, and the recipients' ability and motivation to re-identify the data.

3.7 For data to be considered anonymised, the following criteria should be met:

a) All **direct identifiers** should be removed[3].

b) All **indirect identifiers** that can be used to re-identify individuals when matched with publicly available or proprietary information that the organisation knows the data recipient has access to should be altered or removed to prevent re-identification from the data.

c) Additional **safeguards**[4] may be implemented by the data recipient to restrict access and use of the **anonymised data** to reduce the risks of disclosure and thus risks of re-identification, depending on the extent of anonymisation performed and assessed re-identification risks, such as –

[3] Use of pseudonyms to replace direct identifiers would be considered as removal of direct identifiers. For example, an organisation may remove the direct identifier of a customer's name by replacing it with a randomly generated number.

[4] Refer to PDPC's "Guide on Data Protection Practices for ICT Systems" for relevant basic or enhanced safeguards.

(i) limiting the number of data recipients to whom the information is disclosed and the number of persons that can access the information;

(ii) imposing restrictions on the data recipient(s) on the use and subsequent disclosure of the data;

(iii) requiring the data recipient(s) to implement processes to govern the proper use and disclosure of the anonymised data in line with the imposed restrictions; and/or

(iv) requiring the data recipient(s) to implement processes and measures for the destruction of data as soon as the data no longer serves any business or legal purpose.

d) **Stringent internal safeguards** should be implemented on the **set of information** (e.g. identity mapping tables or other datasets containing linkable information) that can be used to re-identify individuals from the anonymised data, such as –

(i) organisational structures;

(ii) policies, administrative rules or processes;

(iii) technical measures (e.g. using encryption to restrict access to the information, limiting access to only authorised users, and controlling access through passwords); and/or

(iv) physical measures (e.g. restricted access to information storage areas).

e) **Periodic reviews**[5] should be conducted, particularly where anonymised data is disclosed over a period of time in an ongoing relationship, to ensure that the risk of re-identification from the anonymised data is minimised and acceptable. The review should assess –

(i) the adequacy of anonymisation techniques and risk management controls in relation to the current state of technology; and

[5] Refer to PDPC's "Guide to Developing a Data Protection Management Programme" for good practices in risk management.

(ii) the robustness of organisational, legal, processes and other non-technical measures to manage the risks of re-identification, considering technological developments over time.

Assessing risks of re-identification

3.8 Organisations should understand that anonymisation is a risk-based process, which includes **applying both anonymisation techniques and safeguards to prevent re-identification**. In anonymising data, organisations should assess the sensitivity and potential harms of the target attributes should they be disclosed and/or re-identified. If the nature of data is highly sensitive to individuals, the organisation should reduce the granularity of such data to reduce any potential harms arising from disclosure or re-identification.

3.9 In general, where data is anonymised to achieve a minimum k-anonymity value of 5[6], together with the relevant safeguards in place, the data can be considered sufficiently anonymised for sharing with external parties. For use cases or data sharing within an organisation, i.e. internal data sharing, data achieving a lower minimum k-anonymity value of 3, together with relevant internal controls in place, may be considered reasonably anonymised. Organisations should also consider the types of information that could enable re-identification if combined with the anonymised data, as well as the ease with which such information can be accessed, to implement the safeguards or perform further anonymisation. While organisations may use other methods to assess re-identification risk, they should be able to demonstrate a similar or lower risk of re-identification.

3.10 Where data cannot be anonymised further due to the need to preserve the granularity of the data for the use cases and k-anonymity value of 5 or its equivalent cannot be achieved, organisations should put in place more stringent safeguards to ensure that the anonymised data will not be disclosed to unauthorised parties and re-identification risks are mitigated (e.g. tracking the lineage of the data (i.e. its movement, transformation and usage) and to properly dispose of the data post its use as soon as practically possible).

3.11 Where possible, organisations should practise data minimisation and share only the minimally necessary anonymised data attributes and an extract from, instead of their full, database. As a good practice, organisations should also conduct a "motivated intruder" test to assess any residual risks of re-identification of the anonymised data (refer to para 3.36 for more info).

[6] Reference from "The De-identification Decision-Making Framework" by Office of the Australian Information Commissioner, CSIRO and Data 61.

3.12 Where the anonymised data is **aggregated** to the extent that the anonymisation is irreversible and there is no serious possibility of re-identification of individuals, the anonymised data may be publicly disclosed (e.g. open data). Organisations should take care when doing so as the open data cannot be recovered. The effectiveness of technical and process safeguards will be limited but organisations should consider appropriate legal safeguards (e.g. prohibit unauthorised intentional re-identification, unless for research purposes).

3.13 Organisations may refer to PDPC's guide[7] which provides a general introduction to various basic anonymisation techniques. It is not necessary that the most technically sophisticated anonymisation technology be used all the time. Rather, what is required is one that is sufficiently robust to manage the risk of re-identification, given the circumstances (e.g. the extent of disclosure, the intended recipient(s) and existing controls). Organisations may also consider hiring anonymisation experts, statisticians, or independent risk assessors to aid in their assessment of the appropriate anonymisation techniques to apply or assessment of re-identification risks, particularly where the anonymisation issues are complex (e.g. large datasets containing longitudinal or a wide range of personal data).

Why anonymise personal data?

3.14 Anonymisation of personal data enables businesses to tap on data for insights and innovation while at the same time provides protection to individuals. It also reduces the impact of harm to individuals in the event of a data breach. Where possible, Organisations should adopt such practices for external sharing of data. It can even be adopted when sharing data internally, particularly where individuals need not be identified for the purposes of processing.

3.15 In the event of a data breach, the level of data anonymisation, corresponding safeguards implemented and proper assessment by organisations in considering the harms of the anonymised data would be taken into consideration to assess if data has been properly anonymised.

Managing anonymised data within an organisation

3.16 There may be circumstances where an organisation wishes to convert personal data into anonymised datasets to safely use the data for a particular purpose within the organisation. However, the organisation may need to retain the original dataset or other information (e.g. identity mapping table) that can re-identify the individuals from the anonymised datasets for other purposes. In such instances, organisational

[7] Refer to PDPC's "Guide to Basic Anonymisation"

structures should establish effective barriers to access, by a group (or groups) of users within the organisation, to the original dataset or other information (e.g. the decryption key or algorithm that could reverse the anonymisation) held by the organisation that could be used to re-identify an individual. Examples of such effective barriers to access could be a set of effective access controls as part of a comprehensive information security program by the organisation.

3.17	**Example: Data sharing between departments in an organisation** Department A and Department B are two departments within Organisation JKL. Department A manages personal data collected by the organisation for the purpose of customer relations. Department B wishes to use the data for business analytics purpose but does not require individually identifiable data. Department A proceeds to anonymise the data such that the anonymised dataset can no longer identify any individual. Organisation JKL puts in place controls on Department B to prevent re-identification of the anonymised dataset. This includes access restrictions to prevent data users in Department B from gaining access to other information held by Department A that can lead to re-identification, as well as administrative restrictions to prevent Department B from attempting re-identification. Organisation JKL also makes the unauthorised attempt to re-identify individuals from the anonymised dataset a breach of the terms of employment. Department B could be considered to be using anonymised data given that effective controls are imposed on Department B to prevent re-identification.

Sharing anonymised data with other organisations

3.18 Where only the anonymised data is shared with a third party recipient and the third party recipient has no means of re-identification, the Data Protection Provisions in the PDPA do not apply to the third party recipient. However, there is still the possibility that the recipient may subsequently obtain the means and attempt to re-identify individuals from the anonymised dataset or disclose it to others. As such, organisations will still need to put in place contractual safeguards to prevent any re-identification or unauthorised disclosures. In addition, the unauthorised re-identification of anonymised information is also an offence under Part 9B of the PDPA.

3.19	**Example: Enriching customer data from an external source** Organization ABC engages market research and analytics company XYZ to enhance its customer dataset. Before sharing its data with XYZ, ABC anonymises the dataset and ensures that as part of its contractual agreement, XYZ undertakes not to make any attempts to re-identify the dataset. ABC still retains the original dataset and the ability to re-identify the individuals from the anonymised dataset. In processing the data, XYZ augments the anonymised data with other market trending information and aggregated customer segmentation data from its market research to provide additional insights on ABC's customer profiles and interests. In processing the anonymised data and combining with aggregated market research information, XYZ is not considered to be processing or disclosing personal data and the PDPA does not apply to XYZ. ABC receives the enriched dataset and does further analysis to match customer profiles with its products and services and to design promotional packages and marketing campaigns. As ABC is processing its customers' data to understand its customers and improve their experience when using its services, ABC can process the personal data without consent by leveraging on the Business Improvement Exception. For clarity, ABC must ensure that it has the relevant consent from its customers before sending direct marketing messages.
3.20	**Example: Inferring additional attributes of common customers** Organisation DEF and Organisation GHI sign a data sharing agreement to leverage each other's customer datasets to enrich the customer profile of common customers. In the agreement, both parties agree that they will not re-identify each other's dataset and will only use the analysed insights in marketing campaigns. In sharing their datasets, both organisations pseudonymise their dataset with the same hash keys to facilitate the subsequent data merger and analysis by a data intermediary contracted by both organisations. Based on agreed business rules, both organisations develop a set of customer profiles. The data intermediary will merge the datasets and, in accordance with the business rules, associate customers with the appropriate profiles. Under its contract with both organisations, the data intermediary is committed not to re-identify any of the datasets. It also implements technical controls to prevent access by or disclosure to any unauthorised parties. The data intermediary returns to each organisation the processed pseudonymised

	dataset. Each organisation does further analysis to match the derived profiles with its customers, and to design promotional packages and marketing campaigns. As each organisation is processing its customers' data to understand its customers and improve their experience when using its services, it can process the personal data without consent by leveraging on the Business Improvement Exception. For clarity, each organisation must ensure that it has the relevant consent from its customers before sending direct marketing messages.

Disclosing multiple datasets to the same recipient

3.21 If an organisation intends to disclose multiple anonymised datasets to the same recipient (e.g. by publishing seemingly unrelated datasets as part of an open data initiative), it should carry out a careful assessment of the risk of re-identification from such a disclosure, particularly if those datasets are extracted from the same database. The organisation would have to take particular care to ensure that risk management controls are adequate to prevent re-identification of individuals by the recipient organisation, particularly when the datasets are combined with each other or with additional datasets previously released by the organisation. The organisation could consider maintaining a centralised record to track datasets that have been disclosed or published.

3.22	**Example: Publishing multiple datasets** As part of an open data initiative, two divisions in Company WXY have independently decided to release related datasets, unaware of the other division's intentions. Both divisions then carried out assessments with incomplete and inaccurate information about the datasets being released by other divisions in the company. If each division then proceeds to publish their own dataset, this may increase the risk of re-identification where the two datasets are related.

3.23 In view of the above risks, organisations should ensure that third party recipients do not have any other data to enable the re-identification of the anonymised data, and/or that proper contractual obligations are placed on third party recipients to have in place relevant safeguards to prevent unauthorised disclosure or re-identification of the anonymised data. For example, they could put in place contractual safeguards, or require an undertaking from the data recipients not to attempt to re-identify the anonymised data. They could also require that the data recipients put in place additional measures, such as governance frameworks,

processes, and controls, to ensure the proper handling of the anonymised data and further reduce the risk of re-identification.

3.24	**Example: Sharing with third party recipients** Organisation JKL (disclosing organisation) intends to disclose an anonymised dataset to Organisation XYZ (data recipient) and has assessed, based on its own and any publicly available information at the point of disclosure, that XYZ is unlikely to hold any data that will allow it to re-identify individuals within the anonymised dataset. As part of its contractual agreement, XYZ has committed not to attempt re-identification of the dataset or to further disclose the anonymised data to another organisation. JKL also contractually requires that XYZ puts in place governance frameworks and controls to ensure the proper handling of the dataset, including: a) limiting the number of XYZ's employees who can access the anonymised dataset; b) requiring XYZ's employees authorised to access the dataset to be trained on data protection practices; and c) applying appropriate technical solutions to ensure better access controls (e.g. technical measures that limit employees' access to the dataset and the copying of or number of copies of the dataset). JKL follows through with periodic reviews of the governance frameworks and controls that XYZ has put in place.

Considerations for anonymising data

3.25 When deciding whether to anonymise data for use or disclosure, organisations should keep in mind that not all datasets can be effectively or meaningfully anonymised. The following section elaborates on some relevant considerations.

Nature and type of data

3.26 The nature of the dataset affects how much identifying information needs to be removed so that it no longer can be used to identify individuals. Some data types are inherently 'rich' and full of information (e.g. portrait photographs taken for facial recognition purposes), such that any alteration to anonymise the data might render it useless for its intended purposes.

3.27 The uniqueness of a record or data point within a sample dataset or population also contributes to the challenge of anonymisation. There are instances where the use of particular methods may not anonymise the dataset, because data points for certain individuals remain unique. For example, a dataset containing the ages of individuals has one outlier of age 89 while the other ages are below 50. No matter how the ages are generalised or recoded into ranges, the data point for the 89-year-old stands out. Where there are records or data points that are unique to the population or sample (i.e. population unique or sample unique)[8] the risk of re-identification increases. Organisations must be careful to manage these risks and ensure that the dataset is effectively anonymised.

Potential impact on individuals

3.28 When deciding whether to anonymise personal data for use or disclosure, organisations should also consider any potential negative impact on the individuals if they were to be re-identified. This is particularly important if the personal data involved is of a highly sensitive nature, (e.g. records of individuals with HIV, records of adopted children and their biological parents). In such circumstances, even if the organisation assesses that there is a less than serious possibility of an individual being identified from the data, the organisation should carefully consider whether using or disclosing such data would be appropriate.

Nature of use and extent of disclosure

3.29 Organisations should consider how the nature of use and extent of disclosure of the anonymised data can affect the risk of re-identification. In general, where an organisation intends to use the anonymised data within the organisation itself, or where the organisation intends to disclose anonymised data only to a restricted group (or groups) of users (e.g. a closed community of researchers), re-identification risks can be managed better, compared to the situation where the organisation discloses the anonymised data to any user publicly.

Public knowledge and personal knowledge

3.30 It is necessary to understand the intended use and recipient of the anonymised data to assess the risk of re-identification of a disclosed anonymised data and tailor an appropriate set of risk management controls for the intended use and recipient. For example, the risk of re-identification in a disclosure of data to a single entity for research and development of new products and services under a non-disclosure

[8] "Population unique" refers to a record within a dataset which is unique within the population on a given key. "Sample unique" refers to a record within a dataset which is unique within that dataset on a given key. Source: OECD Glossary of Statistical Terms

agreement, would likely differ from the risk of re-identification in publishing the data to the world at large.

3.31 Even after the risks of re-identification have been assessed and appropriate controls implemented, the risk of spontaneous re-identification of data by persons with special knowledge of a particular individual can occur. For example, a patient's attending physician, who is also conducting medical research using datasets containing the patient's data, may be able to recognise the patient's medical profile from the data (even if such data may be assessed to be anonymised if the recipient did not have such special knowledge). If it is known or foreseeable to the organisation that the data might be accessed by any persons with special knowledge that could be used to re-identify any individual from the data, such risk must be accounted for in the risk assessment exercise.

Data recipient's ability and motivation to re-identify

3.32 The risk of re-identification is likely to differ depending on the ability and the motivation of the data recipient to re-identify individuals from the dataset. A data recipient in possession of complementary information, specialised skills or technologies would more likely be capable of re-identifying individuals from the data than one that does not, assuming both have similar motivations.

3.33	**Example: Risk of re-identification due to expert knowledge** Anonymised dataset Y contains complex genome sequencing, a specialised type of data not easily understood by the layman. If the data recipient is an expert in genome sequencing and understands how to identify individuals from such a dataset, the risk of re-identification may be higher. In contrast, if the data recipient has no knowledge of that data type, the risk re-identification would be comparatively lower.

3.34 Even if the data recipient has the requisite skills and information for re-identification, it does not necessarily mean the risk of re-identification is high. The motivation to re-identify must also be considered. The motivation to re-identify an individual may be low if there are barriers to re-identification, such as legal (e.g. via contractual obligations) or regulatory consequences (e.g. pursuant to government regulations or legally binding industry codes issued by regulators), for the data recipient, or if there is simply no incentive or benefit for a data recipient to re-identify individuals.

Changing environment

3.35 While a dataset may be anonymised at a particular point in time, it is not guaranteed that the dataset will stay anonymised permanently. The likelihood of re-identification for any given anonymised dataset is likely to increase over time, due to greater ease of access to and volume of other relevant information, increase in computing power, and improvements in data-linking techniques. A dataset that is sufficiently anonymised based on current technology might be more easily re-identified with technological advancements over time. As such, a periodic review of the risks of re-identification of the anonymised dataset is important to minimise any risk.

"Motivated Intruder" Test

3.36 As a general test for assessing any residual risks of re-identification and the robustness of the anonymisation, a useful starting point is the 'motivated intruder' test highlighted in the ICO's Code of Practice *Anonymisation: Managing Data Protection Risk Code of Practice*, which we adapt to our vernacular.

3.37 The 'motivated intruder' test considers whether individuals can be re-identified from anonymised data by someone who is motivated, reasonably competent, has access to standard resources (e.g. the Internet and published information such as public directories), and employs standard investigative techniques (e.g. making enquiries of people who may have additional knowledge of the identity of the data subject).

3.38 As anonymisation is a package of risk control measures tailored to the purpose of disclosure and the recipient, the 'motivated intruder' test has to take into consideration the known and possible motivation and resources of the intended recipient organisation.[9]

a) The assessment should include the totality of the risk management controls that are applicable to the recipient organisation. This refers to technical measures as well as legal, regulatory or organisational measures. For example, the risk assessment could consider the kind of safeguards accorded to the data, or how long the data is to be retained, among others.

b) 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.

[9] This can include disclosures to the public in cases where the dataset is published as part of open data efforts or in a publication that is freely available.

c) Where disclosure of a particular dataset is to a specific recipient whose motivations, re-identification capabilities, and other information available to that recipient are known or can be reasonably inferred, these known characteristics should also be accounted for.

d) In addition, the risk assessment for re-identification should also consider the other factors (not specific to anonymised data) that subject the anonymised data to re-identification risks. This includes all other 'residual' risks that are not directly related to a recipient's motivation and capability to re-identify or the risk management controls for the disclosed anonymised data; for example, risk of the data being compromised or mistakenly disclosed to unintended recipients.

3.39 There may be situations where the re-identification is unintentional. Generally, unintentional re-identification is not considered collection of personal data. However, the organisation should immediately delete the personal data or re-identifying information. If the organisation uses or discloses such unintentionally re-identified personal data, its actions will be considered to be the use or disclosure of personal data and it will have to comply with the relevant obligations under the PDPA.

3.40 Further, offences under Part 9B of the PDPA hold individuals accountable for knowing or reckless unauthorised re-identification of anonymised information in the possession of or under the control of an organisation (including a public agency). Please see Chapters 22 and 23 of the Key Concepts Guidelines for more information.

<u>Assessing the adequacy of anonymisation and the responsibilities of disclosing and receiving organisations</u>

3.41 In assessing the anonymisation and risk of re-identification of any dataset, the Commission will take a holistic view, including all relevant facts of the case. For example, whether data recipient has robust data protection practices that meet industry standards or that are verified by independent assessors.

3.42	**Example: Assessing breach of anonymised dataset** Organisation JKL (disclosing organisation) discloses an anonymised dataset to Organisation XYZ (data recipient). JKL lowers the risk of re-identification at the point of disclosure by: a) Ensuring that the anonymisation techniques applied to the data set are robust;

	b) Contractually requiring XYZ not to attempt re-identification or further disclosure of the anonymised data to another organisation; c) Contractually requiring XYZ to put in place governance frameworks and controls to ensure proper handling of the dataset; d) Contractually requiring XYZ to maintain its data protection certification under the Data Protection Trust Mark. After receiving the dataset, XYZ suffers a data breach and a copy of the anonymised data is exfiltrated. An individual is subsequently re-identified from the published dataset. Following this incident, JKL and XYZ conduct a review of the safeguards to identify areas for improvement. Generally, when determining whether JKL disclosed personal data or anonymised data at the point of disclosure, the Commission would consider whether JKL had implemented appropriate measures and safeguards, such that there was no serious possibility that individuals would have been identifiable, at the time of the disclosure. When investigating the re-identification incident, the Commission will assess the adequacy of measures and safeguards in place before the incident as well as take into consideration the remediation that JKL and XYZ undertook.

Archiving anonymised data

3.43 Where an organisation anonymises data for the purposes of archival post retention period, information that allows it to re-identify the individuals should not be kept. This ensures that data can remain anonymised and hence not subject to any obligations under the PDPA. Organisations are still required to implement safeguards to protect such anonymised dataset from unauthorised access, and periodically review the adequacy of anonymisation. Where possible, organisations are encouraged to keep only data insights for archival.

Transferring anonymised datasets

3.44 Where organisations intend to transfer anonymised data out of Singapore, organisations have to verify whether the data satisfies the definition of anonymised data in the receiving destination(s) before determining if they are subject to data protection obligations under the jurisdiction of each destination. This is because different jurisdictions may take different approaches to what constitutes anonymised data and organisations may have to take on different obligations when processing such data in different jurisdictions.

4 Photography, Video and Audio Recordings

4.1 Photography, video and audio recordings are increasingly ubiquitous with such capabilities being included in more devices. While not all photographs, video and audio recordings capture personal data, some clearly do.

4.2 An image of an identifiable individual captured in a photograph or video recording is personal data about that individual. An audio recording may comprise personal data if an individual can be identified from that audio recording, or from that recording and other information that the organisation has or is likely to have access to. For example, an individual may be identified from his voice[10], or voice and other information disclosed in or related to the audio recording, or from his voice coupled with his image captured in a video recording of the individual.

4.3 The Commission does not expect that the PDPA will greatly affect adoption of such technologies. Nevertheless, the Commission considers it useful to provide guidance on certain applications of the Data Protection Provisions in the PDPA to photography, video and audio recordings, including those recorded through the use of Closed-Circuit Television Cameras ("CCTVs").

4.4 The following sections and examples outline certain concepts and the application of some of the Data Protection Provisions in the PDPA to photography, video and audio recordings. It should be noted that the scenarios provided address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario.

[10] An individual may be identified from his voice, for example, where the voice clip is sufficiently clear and of a sufficient duration.

Photography and Videography

Does a photographer or videographer need to obtain an individual's consent to take a photograph or video recording of the individual?

4.5 Among other obligations, the Data Protection Provisions require consent from the individual to be obtained for the purposes of the collection, use or disclosure of his personal data. Exceptions to this Consent Obligation may apply depending on the circumstances, for example where the photographer is acting in his personal or domestic capacity, such as when he takes photographs or video recordings for his own personal purposes at a gathering for family and friends.

4.6 A professional photographer or videographer who takes people or event photographs or video recordings of identifiable individuals such as at private events/spaces in the course of his business will be required to obtain consent; unless he is taking the photograph or video recording on behalf of and for the purposes of an organisation or individual pursuant to a contract in writing. In such a situation, the photographer or videographer would be acting as a data intermediary of that organisation or individual. Similarly, if the photographer or videographer is an employee acting in the course of his employment with an organisation, he will not be required to comply with the Data Protection Provisions and instead his employer will be required to comply[11]. In this regard, it would be advisable for employers to put in place systems and processes to prevent employees from engaging in conduct that could cause the organisation to breach the Data Protection Provisions.

4.7	**Example: Photo-taking by an individual acting in a personal or domestic capacity** Diana, an employee of Organisation XYZ, attends XYZ's corporate social responsibility event. At the event, she meets her friend Dawn. During a break in the programme, they have a personal chat and catch up on each other's personal lives. During the chat, Diana takes a photograph of the two of them to update her friends of the encounter via social media. Diana then uploads the photograph and displays it on her personal social media page. In this instance, Diana would likely be considered to be an individual acting in a personal or domestic capacity, and would not be required to comply with the Data

[11] Section 53(1) of the PDPA provides that any act done or conduct engaged in by a person in the course of his employment shall be treated as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval. In reality, whether the individual is acting in the course of employment may not always be clear and may require a factual inquiry.

	Protection Provisions in respect of the photo-taking and subsequent disclosure of the photograph via her social media account. Notwithstanding the above, the Data Protection Provisions may apply in other contexts where Diana is not acting in a personal or domestic capacity. For example, if the photograph is subsequently published for XYZ's publicity purposes (such as in XYZ's corporate brochures or website) instead of for Diana's personal purposes, the Data Protection Provisions are likely to apply to XYZ in respect of the collection, use and disclosure of the photograph. For example, XYZ will have to obtain Dawn's consent before publishing her photograph for XYZ's business purpose.
4.8	**Example: Video recording by an individual acting as an employee** Eric, another employee of Organisation XYZ, is tasked by the management of XYZ to take video recordings at the corporate social responsibility event and make them available on XYZ's webpage. In this instance, as Eric is an employee acting in the course of his employment with XYZ where he takes video recordings for his assigned purpose, the PDPA does not impose the Data Protection Provisions on him directly. XYZ would be required to comply with the Data Protection Provisions instead. As a practical measure, XYZ may assign Eric to ensure its compliance with certain obligations, such as obtaining consent from the individuals that Eric takes video recordings of. In this regard, please refer to subsequent sections of these guidelines for information on obtaining consent.

<u>Does a photographer or videographer need to obtain an individual's consent to take a photograph or video recording of the individual in a public place?</u>

4.9 The PDPA sets out various exceptions to the Consent Obligation. An organisation may wish to evaluate whether any exception applies in respect of its particular circumstances. In particular, there is an exception for the collection, use and disclosure of personal data that is publicly available[12]. For example, when the individual appears at an event or location that is open to the public, taking a photograph of the individual would likely be collection of personal data that is publicly available for which consent is not required. In this regard, the Commission has set out that a location or event would be considered "open to the public" if members of the public can enter or access the location with few or no restrictions, and generally a location would less likely be considered "open to the public" if there

[12] Under the PDPA, "publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

are more restrictions to access. Further, there can be private spaces within public spaces, and a location is not open to the public merely because members of the public may look into the premises or location. As good practice, an organisation that collects, uses or discloses personal data that is publicly available may still wish to obtain consent from the individuals in question. Please refer to the Key Concepts Guidelines for a more detailed discussion on this exception.

How may an individual's consent be obtained for photo-taking or video recording at a private event/space?

4.10 The Data Protection Provisions do not prescribe the ways in which consent may be obtained for photo-taking or video recording. As set out in the Key Concepts Guidelines, consent can be obtained in various ways. Generally, as good practice, an organisation should obtain consent that is in writing or recorded in a manner that is accessible for future reference, for example, as the organisation may be required to prove that it had obtained consent.

4.11 In addition, consent may be deemed to have been given by an individual in situations where the individual voluntarily provides his personal data to an organisation for a purpose, and it is reasonable that he would voluntarily provide the data. In the context of photo-taking or video recording, deemed consent may apply where the individual voluntarily permits a photograph or video recording to be taken of him for the organisation's intended purpose, and it is reasonable that he would do so.

4.12 Please refer to the Key Concepts Guidelines for further elaboration on the Consent Obligation.

4.13	**Examples: Consent for photo-taking at a private function** Organisation ABC holds a private function for a select group of invited clients and wishes to take photographs of attendees for its internal newsletter with their consent. In fulfilling its obligation to obtain consent, the measures that ABC may take to better ensure that the attendees are aware of the purpose for which their photographs are collected, used and disclosed, could include: a) Clearly stating in its invitation to clients that photographs of attendees will be taken at the function for publication in its internal newsletter; or b) Putting up an obvious notice at the reception or entrance of the function venue to inform attendees that photographs will be taken at the event for publication in its internal newsletter.

	Alternatively, ABC may obtain consent from the attendees by clearly indicating that photographs will be taken at the event for its corporate purposes on the confirmation of attendance form which guests would sign and return to the organisation. In this case, ABC would be considered to have obtained consent from the guests who signed and returned the form.
4.14	Kevin attends Organisation DEF's private function. During the function, DEF's photographer informs Kevin that she is taking photographs for publication in DEF's internal newsletter, and asks Kevin if he would like to have his photograph taken. By allowing his photograph to be taken, Kevin would be considered to have given consent for the photograph to be collected, used or disclosed for the stated purpose. To better ensure that guests are aware of the purpose of photo-taking, DEF may wish to take actions such as those in paragraph 4.13. For avoidance of doubt, DEF's photographer would not need to separately obtain consent from attendees if their consent had already been obtained by DEF for such photo-taking at the function, e.g. in the circumstances described in paragraph 4.13 above.

Is a photographer or videographer required to obtain consent from individuals in the background when a photograph or video recording is taken?

4.15 As noted above, consent will generally be required for taking a photograph or video recording of an identifiable individual although consent may be deemed to have been given, or an exception may apply, depending on the circumstances. This is true as well for identifiable individuals who are in the background when a photograph or video recording is taken. It should also be noted that where an individual in the background is not identifiable from the photograph or video recording (such as if the image is too small or obscured), the photograph or video recording will not constitute personal data of that individual.

Do professional photographers or videographers [13] need to sign contracts with the event organiser before they can provide photography or videography services at an event?

4.16 The PDPA does not prescribe the contractual arrangements that organisations may wish to enter into in order to ensure that they comply with their obligations under the PDPA. Where they do enter into such a contract, the PDPA provides that the performance of a contractual obligation shall not be an excuse for contravening the PDPA[14].

4.17 The PDPA does not require a professional photographer or videographer to enter into a contract with an event organiser. However, it would be a good practice for the parties to enter into a contract. Generally, if a professional photographer or videographer is engaged by an organisation to take photographs or video recordings of identifiable individuals, and wishes to be considered a data intermediary processing personal data on behalf of and for the purposes of the organisation pursuant to a contract that is evidenced or made in writing[15], the photographer or videographer should enter into such a contract, which may set out (among other things) each party's responsibilities and liabilities, including the scope of the photographer's or videographer's obligation to process personal data on behalf of and for the purposes of the organisation that engaged him. The organisation on whose behalf the photographer or videographer is acting may also wish to stipulate in a contract security and other data protection obligations on the photographer or videographer in order to ensure that the organisation does not contravene its obligations under the PDPA.

4.18 Where the photographer or videographer is not a data intermediary processing personal data on behalf of and for the purposes of the organisation pursuant to a contract that is evidenced or made in writing, he would be subject to all the obligations under the Data Protection Provisions, unless any relevant exception applies. For example, the photographer or videographer would be required to obtain consent on or before taking a photograph or video recording of an identifiable individual, unless an exception to the Consent Obligation applies.

[13] The term "professional photographer or videographer" in this section encompasses self-employed individuals as well as organisations that provide professional photography or videography services.

[14] Section 4(6)(a) of the PDPA.

[15] In such instances, the professional photographer or videographer would only be required to comply with the Protection, Retention Limitation and Data Breach Notification Obligations, and would not be required to comply with the remaining obligations under the Data Protection Provisions (including the Consent Obligation).

4.19	**Example: Whether a professional videographer is a data intermediary processing personal data on behalf of and for the purpose of another organisation pursuant to contract evidenced or made in writing** Abel, a freelance videographer, is hired by Organisation ABC to be its videographer at its private function. Abel and ABC sign a contract that clearly states (among other things) that Abel will be taking video recordings at the function on behalf of and for the purposes of ABC, and that ABC will obtain consent from the attendees. In such an instance, Abel will be considered a data intermediary processing personal data on behalf of and for the purposes of another organisation pursuant to a contract that is evidenced or made in writing, and Abel need not obtain consent from the individuals he takes video recordings of at the event. After the function, Abel selects some of the video recordings and publishes them on his webpage to promote his work. Abel will not be considered a data intermediary and will be required to comply with the Data Protection Provisions, including obtaining consent from the individuals in the video recordings in order to use or disclose the video recordings for this purpose. In another engagement, Abel is hired by Alice, an individual acting in her personal or domestic capacity, to be her videographer at her private function. Abel will be considered a data intermediary subject only to the Protection, Retention Limitation and Data Breach Notification Obligations where he processes personal data on behalf of and for the purposes of Alice, pursuant to a contract that is evidenced or made in writing. In the absence of such contract, Abel will be required to comply with all the Data Protection Provisions.

<u>Does the exception for collection of personal data "solely for artistic or literary purposes" apply to the taking of photographs or video recordings of individuals?</u>

4.20 In accordance with paragraph 3 under Part 2 of the First Schedule, an organisation is permitted to collect personal data about an individual without the individual's consent if the personal data is collected solely for artistic or literary purposes. Such collected data may also be used or disclosed for purposes consistent with the purpose of collection.

4.21 The terms "artistic" and "literary" are not specifically defined in the PDPA. The Commission is of the view that it would likely be in line with the purpose of the PDPA for these terms to take their ordinary meanings. However, the Commission notes that the parameters as to what would constitute "artistic" purposes may be strongly subjective. Accordingly, while organisations taking photographs or video recordings

solely for artistic or literary purposes may rely on the exception, where it is feasible for organisations to obtain the individual's consent before taking a photograph or video recording of the individual or where it is uncertain that an organisation's purpose would be considered solely "artistic" or "literary", the Commission would advise organisations to obtain the individual's consent as best practice.

Is an individual who submits a photograph or video recording taken when acting in a personal or domestic capacity for a competition, still acting in a personal or domestic capacity?

4.22 An individual's submission of a photograph or video recording for a competition is, on its own, insufficient to determine whether he is acting in a personal or domestic capacity. Such a determination would have to be made based on all the material facts of the case.

4.23	**Examples: Submission of photographs for a competition** Alan is a professional photographer. He takes a photograph of his aunt Betty at a family event, and subsequently submits it for a competition for professional freelance photographers organised by Organisation ABC. The winner of the competition will receive a contract to provide services as the official photographer at an event conducted by ABC. Alan is unlikely to be considered to be acting in a personal or domestic capacity, and the Data Protection Provisions will apply to his use or disclosure of the personal data unless any other exceptions apply.
4.24	Alan submits the same photograph of his aunt Betty for a photography competition organised by Social & Recreational Club DEF on the club member's favourite family member. The competition is open to all members of the social and recreational club and the prize is a free holiday for the winner and his favourite family member. Alan is likely to be considered to be acting in a personal or domestic capacity, and the Data Protection Provisions will not apply to his use or disclosure of the personal data.

Can individuals withdraw consent for the publication of photographs or video recordings, or request under the PDPA for the removal of photographs or video recordings that have been published?

4.25 The PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA for the collection, use or disclosure of their personal data for any purpose by an organisation by giving reasonable notice

to the organisation[16]. An organisation that receives notice of the withdrawal of consent must (among other things) cease, and cause its data intermediaries and agents to cease, to collect, use or disclose the photographs or video recordings, as the case may be (unless an exception applies).

4.26 Where an organisation has already collected the personal data, the withdrawal of consent will only apply to its continued use or future disclosure. However, this does not affect an organisation's collection, use and disclosure of personal data without consent where this is required or authorised under the PDPA or other written law. In such cases, organisations may consider refraining from any future collection, use or disclosure of the personal data as a matter of discretion. Paragraph 4.30 below provides an example of how an organisation may give effect to an individual's withdrawal of consent when it relates to a photograph or video recording of a group of individuals.

4.27 Where photographs or video recordings of an identifiable individual have been taken (for example, where the photographs or video recordings are taken for marketing purposes) but have yet to be published, the individual may withdraw consent for the collection, use or disclosure of the photographs or video recordings in accordance with the PDPA. The withdrawal of consent would affect all continued use and future disclosure. For avoidance of doubt, the withdrawal of consent would not affect any requirement or authorisation under any written law to collect, use or disclose personal data without consent. For example, under the PDPA, organisations are not required to obtain consent for the collection, use or disclosure of publicly available personal data. In such cases, an organisation that receives a withdrawal of consent may wish to cease further use or disclosure of the photographs or video recordings in question as good practice.

4.28 The PDPA does not provide a right for individuals to request that an organisation ceases to retain their personal data per se. Thus, an organisation which receives a notice of withdrawal of consent for publication of a photograph or video recording is not necessarily required to delete that photograph or video recording from all its records and documents, and may retain personal data in accordance with the Retention Limitation Obligation (e.g. where retention is necessary for legal or business purposes). However, where the organisation's activities involving the personal data are in breach of the Data Protection Provisions, the organisation may be directed by the Commission to (among other things) cease retaining such personal data.

[16] Please refer to Chapter 12 in the Key Concepts Guidelines relating to withdrawal of consent for more details.

4.29	**Example: Withdrawal of consent for publication in an annual report** Organisation ABC publishes a photograph of a client, Mr Y, in its annual report distributed to shareholders and clients. Mr Y subsequently withdraws his consent to the publication of the photograph. ABC is required under the PDPA to cease future publication of the photograph, unless such disclosure without Mr Y's consent is required or authorised under the PDPA or other written law, for example, if the photograph is already publicly available. However, it is not required to recall copies of its annual report, which had been circulated prior to the withdrawal, so as to remove the photograph. It may also be able to continue to retain the photograph subject to the Retention Limitation Obligation.
4.30	**Example: Withdrawal of consent by an individual in a group photograph** Organisation ABC obtains consent from and takes a photograph of a group of individuals at a private event, for publication in its internal newsletter. A member of that group, Mr Z, subsequently withdraws his consent for the publication of the photograph. ABC is required under the PDPA to cease future publication of the photograph, unless such disclosure without Mr Z's consent is required or authorised under the PDPA or other written law, for example, if the photograph is already publicly available, or ABC is able to effect the withdrawal of consent (e.g. by masking the image of the individual) before publishing the photograph.
4.31	**Example: Collection in breach of Data Protection Provisions** Jessie informs Organisation XYZ that it had collected her personal data without her consent by taking an identifiable video recording of her, and asks it to destroy the video recording. XYZ determines that its collection (and any subsequent use or disclosure) of Jessie's personal data may have been in breach of the Data Protection Provisions. In this case, XYZ should cease any further use or disclosure of Jessie's personal data. Where the purpose for which the personal data was collected is no longer being served by the retention and retention is no longer necessary for legal or business purposes, XYZ should also cease such retention[17].

[17] To be clear, Organisation XYZ's ceasing to retain Jessie's personal data does not necessarily absolve XYZ of any breach of the Data Protection Provisions, nor preclude the Commission from taking action against XYZ if the Commission determines that XYZ had indeed breached the Data Protection Provisions.

Does the PDPA affect the copyright in a photograph or video recording?

4.32 The Data Protection Provisions do not affect any right conferred or obligation imposed by or under other laws, including the Copyright Act. In particular, the PDPA does not affect copyright subsisting in a photograph, video recording or other item in respect of which copyright is protected under the Copyright Act ("copyright item"). Hence, organisations which collect, use or disclose personal data in a copyright item must comply with the Data Protection Provisions in respect of that personal data, except to the extent of any inconsistency between the Data Protection Provisions and other written law. For example, an organisation that seeks to take a photograph or video recording of an individual would need to comply with the Notification Obligation and Consent Obligation, unless an exception under the PDPA applies (as discussed above).

Closed-Circuit Television Cameras ("CCTVs")

4.33 CCTVs are commonly used to capture video recordings, and some of them may also be equipped with audio recording capabilities. The paragraphs below pertain to the use of CCTVs, and generally apply regardless of whether the CCTVs record video only or both video and audio. CCTVs are usually deployed for security monitoring purposes, and may be deployed in publicly accessible places (e.g. lift lobby and reception) or within private premises (e.g. factory floor).

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

4.34 Consent for the collection, use or disclosure of CCTV footage is not required if it falls within an exception in the First or Second Schedules of the PDPA. For instance, when the CCTVs are situated in areas which are open to the public and locations where individuals can reasonably expect CCTVs to be placed, organisations can rely on the publicly available exception to consent in the First Schedule of the PDPA. Nevertheless, it is good practice for organisations to inform individuals that the area is under CCTV surveillance. For private areas, organisations that have a legitimate interest in the deployment of CCTV may do so in reliance and in compliance with the conditions attached to the legitimate interests exception to consent in the First Schedule of the PDPA. If none of the exceptions are applicable, organisations should seek consent and inform individuals of the collection, use or disclosure of CCTV footage.

4.35	**Example:** Organisation XYZ is a Karaoke Television Studio "KTV". XYZ wants to display footage of patrons' activities in private rooms in the open areas of the KTV, as part of the overall mood and atmosphere. It has assessed that it is unable to rely on the legitimate interests exception and decides to proceed on the basis of patrons' consent. XYZ states in its terms and conditions for using a KTV room and requires patrons to acknowledge that CCTVs have been deployed in the private rooms and the footage will be displayed in the open areas of the KTV. XYZ also puts up notices to that effect inside the KTV rooms. Such notification and method of obtaining consent would be sufficient for XYZ's purpose.
4.36	**Example:** Shopping mall ABC deploys CCTVs for security and safety purposes. As shopping mall ABC is considered accessible to the public, it can rely on the publicly available data exception to consent outlined in the First Schedule of the PDPA. As good practice, Shopping mall ABC may wish to put up notices to inform individuals that the area is under CCTV surveillance. The publicly available data exception will not apply to restricted areas in shopping mall ABC such as within the premises of private offices.

4.37 Organisations may choose to rely on the legitimate interests exception[18] to consent to deploy CCTVs for areas not open to the public. When relying on the legitimate interests exception, the organisation must conduct a risk assessment to mitigate the risks of collecting, using or disclosing this data and take reasonable steps to provide the individual with information that it is relying on the exception (e.g. disclosure as part of the organisation's public data protection policy). It is generally a good practice to put up notices informing individuals that an area is under CCTV surveillance even if their consent is not required. For examples of scenarios where organisations may choose to rely on the legitimate interests exception, please refer to the Guide on the Responsible Use of Biometric Data in Security Applications.

[18] Please refer to Chapter 12 of the Key Concepts Guidelines for more information on the legitimate interests exception.

4.38	**Example:** Events organiser EVT wishes to install security cameras at storage areas and corridors on its premises which are not open to the public but are accessible to third party retailers who are renting exhibition booths and their suppliers. The purpose of the security cameras would be to monitor the premises as a deterrent against theft. EVT will also be placing prominent notices below each security camera to provide sufficient notification that security cameras are in operation. Under such circumstances, EVT may consider relying on the legitimate interests exception to consent.

4.39 For the deployment and use of CCTVs in workplaces, organisations may wish to rely on the employment exception to consent outlined in the First Schedule of the PDPA provided it is for the purpose of managing the employment relationship with the individual. Monitoring and enforcing workplace safety and security requirements to provide a safe working environment for employees can be considered a legitimate purpose within the employment relationship. However, to rely on the employment exception to consent, the organisation must inform the individual of the purpose of the CCTV, e.g. through the employee handbook or easily accessible HR policies.

4.40	**Example:** Construction worksite DEF is required to implement safe management measures such as safe distancing at the worksite. DEF deploys CCTVs at locations of the worksite where employees tend to congregate. DEF assesses that the purpose for collection of personal data in this circumstance is reasonable for ensuring a safe working environment and managing the employment relationship, DEF relies on the employment exception to collect employees' personal data instead of seeking consent from employees. As DEF is still required to provide notification to its employees, DEF mentions that CCTVs are being deployed for the purpose of ensuring safe distancing at the worksite in the employee handbook.

<u>Where should notices be placed?</u>

4.41 Notices or other forms of notifications should generally be placed to enable individuals to have sufficient awareness that CCTVs have been deployed. The PDPA does not prescribe the content of notifications. 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 and notification of purposes will not be required by the PDPA (e.g. where the personal data is publicly available[19]), organisations are nevertheless encouraged to provide notification as good practice.

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

4.42 The PDPA requires that an organisation considers what a reasonable person would consider appropriate under the circumstances in meeting its obligations under the PDPA. An organisation is not prohibited by the PDPA from having CCTVs that incidentally collects 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. If an organisation intends to capture footage of public areas beyond the boundaries of its premises, it may rely on the publicly available data exception but is encouraged to display appropriate notifications as a matter of good practice.

What should an organisation do if an individual requests for access to CCTV footage?

4.43 In general, organisations are required to provide an individual access to their requested personal data, unless an exception under the Fifth Schedule applies or the organisation is prohibited from doing so due to the prohibitions under sections 21(2), 21(3) and 21(4) of the PDPA. Such exceptions include provision of the personal data or other information that could reasonably be expected to threaten or cause grave harm to the safety or physical or mental health of an individual other than the individual who made the request.

4.44 Organisations can ask individuals the purpose of their request and for further details (e.g. date, time, location etc.). This will allow organisations to:

[19] Please refer to Chapter 12 of the Key Concepts Guidelines for more information on the concept of "publicly available".

a) identify the relevant CCTV footage pertaining to the individual's request; and

b) determine the most cost-efficient way of meeting the request – e.g. providing a printout from the footage, an extract of the footage or allowing the individual a reasonable opportunity to view the requested footage in person etc.

4.45 Organisations have the option of charging the individual a reasonable fee for providing a copy of the CCTV footage.

4.46 Organisations may advise individuals if their access request can be more effectively made through other channels. For example, if the purpose of the request is for a civil case before the courts, the organisation may wish to inform the individual to consider the option of applying for discovery in those proceedings; and if the purpose is to enable the individual to make a police report, the organisation may wish to inform the individual that the police can obtain footage directly from the organisation after the police report has been filed and investigations have commenced.

4.47	**Example:** John was involved in a minor physical altercation in the office of organisation ABC and the incident was captured by ABC's CCTV. He approaches ABC to request for the footage about the incident as video evidence for a police report. ABC may wish to advise John to proceed to make a police report as the police can obtain the footage from ABC directly after investigations have commenced. John can also rest assured that the CCTV footage is in the hands of the police and will be handled in accordance with standards of custody.

<u>Is an organisation required to mask the images of other individuals in the CCTV footage?</u>

4.48 Pursuant to Section 21(3)(c) of the PDPA, organisations are required to mask the image of the other individual in the CCTV footage unless:

a) any of the exceptions relating to disclosure of personal data without consent listed under the First and Second Schedules to the PDPA apply to the extent that the organisation may disclose personal data of the other individual without consent (e.g. if the personal data of the individual is publicly available or if the organisation can rely on the legitimate interests exception);

b) as permitted or required by any other law and regulation (e.g. exercise of police investigatory powers, compliance with discovery directions in civil

proceedings or regulations governing building maintenance and strata management); or

c) the other individual has given consent to the disclosure of his personal data.

4.49	**Example:** Mary would like to know whether she dropped her wallet at the entrance to Shopping mall ABC. She makes a request to ABC for access to CCTV footage of herself at the entrance to the mall at the date and time she was there. The CCTV footage contains images of other individuals entering the mall. However, as Shopping mall ABC is considered accessible to the public, it can rely on the publicly available data exception to disclose the CCTV footage to Mary without masking the images of other individuals that were seen entering the mall around the time that Mary entered.
4.50	**Example:** Jane applies to Condominium ABC for access to CCTV footage of herself at the Condominium's taxi drop off point where she had an altercation with a third-party. As the taxi drop off point is open to the public, ABC can rely on the publicly available data exception and need not mask the image of the third-party within the footage in providing Jane access to the requested footage.

4.51	**Example:** Jack is a subsidiary proprietor/owner of a unit in Condominium XYZ. Jack applies to Condominium XYZ's management for access to CCTV footage of himself at the condominium's lift lobby as he believes he dropped his personal belongings there. There were other people with Jack at the lift lobby at that time and Jack wishes to approach them for assistance in recovering his personal belongings. Under Section 47 of the Building Maintenance and Strata Management Act "BMSMA", a subsidiary proprietor/owner of a condominium unit may make an access request for the CCTV footage without the need to redact/mask the footage.[20] As PDPA is considered a baseline law, other sectoral regulations, such as BMSMA, which permit the access to unredacted footage will take precedence in this instance.
4.52	**Example:** There is a children's party being held at the function room of Condo KLM where a CCTV is installed. Jessie and her daughter, who do not stay or own a unit in Condo KLM, are guests of the host of the party. Jessie loses her personal belongings at the party. She decides to go directly to Condo KLM's management to request for a copy of the CCTV footage to assist her in locating her belongings. KLM assesses that there is legitimate interest in providing Jessie with access to the footage, without masking the images of other individuals, to assist her in recovering her personal belongings. KLM also assesses that in doing so, there is no adverse effects to individuals present at the party. As such, KLM allows Jessie access to the requested footage. KLM designs an approval process for such requests and addresses risks of abuse by limiting Jessie's access to viewing of the relevant CCTV footage under supervision.

<u>Can compromising an organisation's security arrangements be sufficient reason to deny access to CCTV footage?</u>

4.53 The Commission's view is that, depending on the specific facts and circumstances, compromising an organisation's security arrangements could be a sufficient basis to deny access to CCTV footage if there is an applicable exception in the Fifth Schedule

[20] See the District Court case of *Cheong Yoke Ling @ Zhang Yuling and another v Management Corporation Strata Title Plan No 508 and others* [2020] SGDC 295, in which this issue arose. The Court held that where a request for inspection has been made under Section 47 of BMSMA, the MCST does not have to be concerned with data protection issues and should allow inspection without redacting personal data.

or prohibition in providing access in section 21. However, where an organisation denies access on this basis, the Commission expects the organisation to be able to provide strong justifications as to why it is unable to accede to the access request. The Commission will have to make a determination based on the facts of the particular case, should a complaint be received.

Can two or more individuals make an access request for the same CCTV footage containing their personal data, if they consent to their own personal data being revealed to the others making the access request?

4.54 Yes. It would be reasonable for certain groups of individuals (e.g. a married couple, parents of a class of students etc.) to make an access request for the same footage containing their personal data. Organisations may apply the same considerations in determining whether to provide access as they would for a request made by a single individual. Please refer to Chapter 15 of the Key Concepts Guidelines.

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

4.55 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.

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

4.56 The PDPA does not prohibit this. However, such a contract would not override any rights or obligations under the PDPA.

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

4.57 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. If the individual's purpose for making the request may be met by a lower resolution extract or printout, the organisation may inform the individual of this less costly option.

Where an organisation is providing a copy of the CCTV footage upon request of an individual, must the copy be a video or can it be provided in other formats?

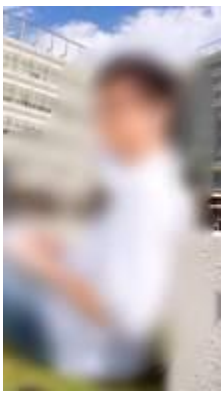
4.58 The PDPA does not specify the format of the personal data to be provided in relation to an access request made by an individual. In the case of personal data captured in CCTV footage, organisations may respond to access requests for CCTV footage by providing either still frames of the footage or the actual footage itself, with appropriate masking of the personal data of other individuals if required.

What does "video masking" or "masking" refer to?

4.59 "Video masking" of images refers to the process of concealing parts of the video from view. This may include masking certain body parts or inanimate objects that could potentially disclose the personal data of an individual. The common types of masking include (i) solid colour masked areas; (ii) blurred masking; or (iii) pixelated masking. Where solid colour masking is used, no details or movement in the scene covered by the masked area can be viewed. However, when pixelated or blurred masking is used, the resulting image enables a partial outline to be seen but with detailed features obscured. This may be a less fool proof method as it is possible for pixelated or blurred images of individuals to still be identifiable. Examples of the different masking techniques are shown below. These can be applied to both video and still imagery.

Solid

Blur



Pixelated

5 Drones

5.1 Increasingly, organisations are making use of drones that may be equipped with photography, video and/or audio recording capabilities. The subsequent paragraphs pertain to the use of drones by organisations, and generally apply regardless of whether the drones are equipped with photography, video and/or audio recording capabilities. To be clear, the Data Protection Provisions do not impose any obligation on an individual acting in his personal or domestic capacity.

What should organisations consider when using drones?

5.2 Organisations will need to consider whether the drones they deploy are likely to capture personal data of individuals, and may wish to evaluate whether any exception under the PDPA applies in respect of its particular circumstances.

5.3 The use of drones with photography, video and/or audio recording capabilities are generally subject to the same considerations and obligations under the PDPA as that of other equipment with similar capabilities. Organisations should also be mindful that the operation of drones is subject to the guidelines and requirements of other authorities. For instance, organisations should not operate a drone within the boundaries of any prohibited area (i.e. protected area or special event area)[21]. Enquiries may be made to the Civil Aviation Authority of Singapore.

What should organisations do if the drones used are likely to capture personal data?

5.4 Among other obligations, the Data Protection Provisions require organisations to inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. An organisation must thus provide notification of the purposes for the collection, use or disclosure of personal data captured by its drones, in order to fulfil the obligation to obtain consent[22]. The notifications should specify if photography, video and/or audio recording is taking place and should generally be placed so as to enable individuals to have sufficient awareness that drones are in operation in the general locale. For example, it may be appropriate to place a notice at points of entry to the area of operation, where individuals are able to read the notice prior to entry.

---

[21] See Division 4 of the Air Navigation Act (Cap 6) and Part III of the Public Order Act (Cap 257A).

[22] Where a drone operator is capturing photographs, video and/or audio recordings on behalf of and for the purposes of another organisation pursuant to a contract in writing, the other organisation is required to comply with the Data Protection Provisions. If the drone operator is an employee acting in the course of his employment with an organisation, he will not be required to comply with the Data Protection Provisions, instead his employer will be required to comply.

5.5 The PDPA sets out various exceptions to the Consent Obligation. In particular, there is an exception for the collection, use and disclosure of personal data that is publicly available[23]. For example, when the individual appears at an event or location that is open to the public, a photograph, video or audio recording taken of the individual at such an event or location would likely be personal data that is publicly available, and organisations may collect, use or disclose such personal data without consent. In such instances, organisations may still wish to provide notifications as good practice. Some possible methods of providing notification include placing signages at entrances to the spaces where the drone is flown, at prominent locations along the approved flight path (or carried/worn by safety marshals), or at the launch site, etc. Please refer to the Key Concepts Guidelines for more details on the Consent Obligation, Notification Obligation and publicly available exception.

What should organisations do if personal data was unintentionally collected by the drones?

5.6 The Commission would encourage organisations to ensure that they adhere to the pre-determined flight path of drones and adopt policies restricting or prohibiting the use of any personal data that is unintentionally collected (e.g. when drones accidentally veer off-course from the pre-determined flight path and collect personal data without consent)[24].

[23] Under the PDPA, "publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

[24] To be clear, the deletion of the personal data does not necessarily absolve an organisation of any breach of the Data Protection Provisions, nor preclude the Commission from taking action against the organisation if the Commission determines that the organisation had indeed breached the Data Protection Provisions.

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 Chapter 12 on "The Consent Obligation" in the Key Concepts 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 Chapter 12 on "The Consent Obligation" in the Key Concepts 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.

6.7	**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?

6.8 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 Chapter 15 on "The Access and Correction Obligations" in the Key Concepts 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?

6.9 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 Chapter 15 on "The Access and Correction Obligations" in the Key Concepts Guidelines for more details.

6.10 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?

6.11 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.

6.12 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 Protection, Retention Limitation and Data Breach Notification Obligations 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 Chapter 6 of the Key Concepts Guidelines for more information on 'excluded organisations'.

6.13 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 Advisory Guidelines on the Do Not Call Provisions for more information.

Personal Data of Employees

How does the PDPA apply to employment records of employees?

6.14 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).

6.15 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.

6.16 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

6.17 Organisations may collect, use and disclose personal data without consent where this is necessary for evaluative purposes. (This exception is set out in paragraph 2 under Part 3 of the First Schedule). 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.

6.18 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 entering into, managing or terminating an employment relationship between the organisation and the individual

6.19 Under the PDPA, the collection, use and disclosure by organisations of personal data from their employees that is reasonable for the purpose of entering into, managing or terminating their employment relationships would not require the consent of their employees. This is pursuant to paragraph 10 under Part 3 of the First Schedule. While consent is not required, employers are required to notify their employees of the purposes of such collection, use or disclosure.

6.20 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 Chapter 14 on "The Notification Obligation" in the Key Concepts Guidelines for more details.

6.21 Purposes that could fall within the purpose of entering into, managing or terminating an employment relationship can include:

a) Conducting pre-employment activities such as health screening; background/reference checks;

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

c) Allocating computer resources and monitoring how the employee uses company computer network resources;

d) Managing work-schedules or work arrangements such as deployment;

e) Conducting checks on conduct/discipline;

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

g) Managing staff welfare/benefits such as training or educational subsidies;

h) Conducting audit checks on employees such as records, taxation, claims etc;

i) Managing health and safety at work; and

j) Performance management.

6.22 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 entry, 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 entering into, managing or terminating an employment relationship.

6.23	**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.

<u>What is the difference between the exception for evaluative purposes and the exception for the purpose of entering into, managing and terminating an employment relationship?</u>

6.24 There are instances where employers have to collect the same set of personal data for both the purposes of (i) entering into, 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 entering into, managing and terminating the employment relationship, and not of the evaluative purpose.

6.25	**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.

6.26 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 Chapter 9 on "Reasonableness" in the Key Concepts Guidelines.

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

6.27 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.

6.28 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 Chapter 18 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?

6.29 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 its 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.

6.30 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.

6.31 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?

6.32 The exception relating to "entering into, managing or terminating an employment relationship" only apply when the individual and organisation are entering into or already have an employment relationship. Where an organisation is collecting the personal data of other individuals without such relationship 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 Online Activities

7.1 A multitude of data is generated and captured during our online activities (including our use of mobile and other lifestyle devices (e.g. activity trackers and smart watches)). Some identifiers are provided by the user (e.g. email address or mobile number) or assigned by the organisation (e.g. customer IDs); other identifiers are programmatically generated and assigned: e.g. hash generated from email address, device fingerprints, IP addresses (see paragraph 7.3 below) and cookies (see paragraph 7.7 below).

7.2 Apart from identifiers, organisations may collect other types of data from and about its customers. For example, payment particulars and billing and delivery information provided by customers during check out; and also, behavioural data generated by the customers' use of the service, such as browsing and search activities. Such data, when linked to an identifier, will form part of the personal data that the organisation is collecting about individuals. For example, an IP address or tracking cookie may be matched with other data elements such as browsing history, purchase history, postal code, mobile numbers and shopping preferences such that the organisation may be able to identify an individual.

Are IP address on their own personal data?

7.3 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.

7.4 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 that are related to that login identity, along with other information such as cookies (addressed below) and IP addresses can identify individuals, and are likely to be personal data in such context.

7.5 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 an individual may be identifiable from the data and thus may constitute as 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 and data associated to the IP address for a long period of time, and is able to ascertain that the particular IP address is associated with an identifiable person, the organisation may be found to have collected personal data.

7.6 For more details on what constitutes personal data, please refer to Chapter 5 on "Personal Data" in the Key Concepts Guidelines.

Must consent be obtained for the use of cookies?

7.7 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.

7.8 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 be used to 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.

7.9 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.

7.10 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):

a) transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase; and

b) reasonable activities that cannot take place without cookies that collect, use or disclose personal data, e.g. authentication and security, user preference, network management, streaming content.

7.11 Please refer to Chapter 12 on "The Consent Obligation" in the Key Concepts Guidelines for more details.

7.12 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.

7.13 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 targeting of advertisements?

7.14 Where targeting of advertisements involves the collection and use of personal data through cookies, the individual's consent is required. As discussed in paragraph 7.127.12 above, consent may be reflected through his browser settings. As good practice, organisations should provide individuals with the ability to set their cookie preferences within the website to enable or disable the use of such cookies for personalised advertisement targeting.

8 Data Activities Relating to Minors

When can a minor give valid consent on his own behalf under the PDPA?

8.1 The PDPA does not specify the situations in which a minor (that is, an individual who is less than 21 years of age) may give consent for the purposes of the PDPA. In general, whether a minor can give such consent would depend on other legislation and the common law. In this regard, organisations should keep in mind that Parts 3 to 6A of the PDPA do not affect any legal rights or obligations under other laws[25].

8.2 It is noted that the ages at which minors may conduct different types of activities on their own or are accorded certain legal protections vary across various local legislation[26].

8.3 For situations where there is no legislation that affects whether a minor may give consent, the issue would be governed by the common law. In this regard, the Commission notes that there is no international norm on when minors may exercise their own rights under data protection laws. The Commission understands that in some countries, some kind of test of maturity is applied, taking into account factors such as the level of maturity of the minor, the minor's capacity to understand the nature of legal rights and whether there is any undue influence exerted on the minor, to determine if a minor can exercise legal rights. In addition, some countries have enacted legislation to specifically protect minors below a certain age. For example, in the United States, the Children's Online Privacy Protection Act ("COPPA") requires certain organisations to obtain verifiable parental consent to collect personal data from children under 13 years of age[27].

8.4 The Commission understands that the applicable test under English common law for

---

[25] Section 4(6)(a) of the PDPA.

[26] Provisions that set out age thresholds for the purpose of according certain legal protections to minors include:

a) section 35(1) of the Civil Law Act (Cap. 43) which provides that, except as otherwise provided in that section or any other written law, a contract entered into by a minor who has attained the age of 18 years has effect as if he was of full age (that is, 21 years of age);

b) section 67A of the Employment Act (Cap. 91), which defines a child as one below 15 years of age and a young person as one between 15 and 16 years of age for the purposes of according varying protections in respect of the different age groups; and

c) section 2 of the Children and Young Persons Act (Cap. 38), which defines a child as one who is below 14 years of age and a young person as one that is between 14 and 16 years of age for purposes of according varying protections under that Act.

[27] See, for example: http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over

when a minor can consent on his own behalf in matters relating to medical treatment (and several other areas)[28] would be the *Gillick* test. In brief, the *Gillick* test sets out that a minor may provide consent if he has sufficient understanding and intelligence to enable him to understand fully what is proposed. To-date, the *Gillick* test has not yet been expressly approved by a Singapore court[29].

8.5 The Commission notes that the age threshold of 13 years appears to be a significant one in relation to according protection to minors. For example, under the Employment Act, a child 13 years of age or older may be employed in light work suited to his capacity in a non-industrial undertaking and no child who is below the age of 13 years shall be employed in any occupation (with a limited exception)[30]. Similarly, some film and video classification ratings set out age thresholds for audiences for such content, including Parental Guidance 13 ("PG13")[31]. In addition, organisations that face exposure to COPPA (e.g. companies that provide online services to individuals in the US) may also already have policies and procedures that are premised on the age threshold of 13 years in relation to consent to the collection, use and disclosure of their personal data.

8.6 The Commission is of the view that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent, in determining if he can effectively provide consent on his own behalf for purposes of the PDPA. It is also noted that, as a practical matter, some organisations may already have policies or practices providing for an age threshold of 13 years in relation to consent. Bearing this in mind, the Commission will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, where, for

---

[28] While the holding in *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112 may be argued to only apply narrowly in the context of consenting to medical treatment and advice, later UK cases have applied the *Gillick* principle to other areas. For instance, it was applied in determining if a minor was able to make a decision on divulging information about herself to the press. The Commission is however not aware of any UK cases which expressly applies the *Gillick* principle in the context of UK's data protection laws and in particular, in determining whether a minor can consent to the sharing of his personal data.

[29] To-date, there are no Singapore cases that have expressly applied *Gillick*, whether in the context of a minor consenting to receiving medical treatment, or in any other context. It therefore remains an open question whether or not the Singapore court will find the *Gillick* principle to have any relevance in determining whether a minor can exercise his legal rights, especially in the context of Singapore's own data protection framework.

[30] Please see section 68(3) of the Employment Act and Regulation 3 of the Employment (Children and Young Persons) Regulations.

[31] PG13 is an advisory rating that means "suitable for persons aged 13 and above but parental guidance is advised for children below 13". More details of the film and video classification system are available at: https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/films.

example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual, such as the minor's parent or guardian, who is legally able to provide consent on the minor's behalf[32].

8.7 Overall, an organisation should take appropriate steps to ensure that the minor can effectively give consent on his own behalf, in light of the circumstances of the particular case including the impact on the minor in giving consent.

Can a minor's parents or other legal guardians provide valid consent on behalf of the minor under the PDPA?

8.8 Section 14(4) of the PDPA provides that consent given or deemed to have been given by an individual for the collection, use or disclosure of the individual's personal data includes consent given or deemed to have been given by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data. In situations where a minor does not have the requisite legal capacity to give consent for purposes of the PDPA, the minor's parents or other legal guardians may give consent on behalf of the minor. In general, the rights of parents in respect of their children are derived from the common law but there may be legislation that affects how and if they may exercise such rights[33].

8.9 Where an organisation requires the consent of a minor for the collection, use or disclosure of his personal data, the organisation should consider whether it would be appropriate for the organisation to obtain consent given on behalf of the minor from an individual who can legally give consent on behalf of the minor. As a general guide, where the minor is under the age of 13 years, organisations may wish to obtain consent for the collection, use and disclosure of the minor's personal data from an individual that can legally give consent on behalf of the minor, such as the minor's parent or guardian.

When is a minor deemed to have given consent on his own behalf under the PDPA?

8.10 Under section 15(1) of the PDPA, an individual may be deemed to have consented to the collection, use or disclosure of his personal data for a purpose if he voluntarily provides his personal data for that purpose (without actually giving consent) and it

[32] For avoidance of doubt, the Commission's position does not affect any right of a parent or legal guardian of a minor to exercise any right or power conferred on the minor under the PDPA on behalf of the minor. Thus, if a parent or legal guardian is empowered to provide consent or refusal on behalf of a minor, an organisation should generally rely on such consent or refusal given by the parent or legal guardian.

[33] For example, Singapore legislation such as the Guardianship of Infants Act and Women's Charter may affect whether an individual has custody over a minor.

is reasonable that the individual would voluntarily provide the data. In the case of a minor, the Commission is of the view that whether a minor provides his personal data for a purpose voluntarily would depend on various factors including the following:

a) the minor's understanding of the purpose for which his personal data is provided;

b) the minor's understanding of the effect of giving his personal data for that purpose; and

c) whether there was any undue influence on the minor with respect to the provision of his personal data.

8.11 As noted in the preceding section, the Commission will, as a general guide, take the view that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. This will similarly apply to deemed consent. In view of the potential difficulties of establishing whether deemed consent applies, the Commission is of the view that organisations that wish to rely on deemed consent in certain situations should take extra care to establish whether a minor has sufficient understanding of the purposes for which the organisation is collecting, using and disclosing personal data and the consequences of giving his personal data in such situations. Organisations should also refrain from exercising any undue influence to obtain personal data from minors.

Should organisations adopt a different treatment for the collection, use or disclosure of personal data about minors?

8.12 The PDPA does not contain provisions that specifically address the collection, use or disclosure of personal data about minors. However, given that there is generally greater sensitivity surrounding the treatment of minors, it may be prudent for organisations to consider putting in place relevant precautions if they are (or expect to be) collecting, using or disclosing personal data about minors. For example, organisations that provide services targeted at minors could state terms and conditions in language that is readily understandable by minors, or use pictures and other visual aids to make such terms and conditions easier to understand. Other good practices could include placing additional safeguards against unauthorised disclosure of, or unauthorised access to, personal data of minors, or anonymising personal data of minors before disclosure, where feasible.

Should organisations take extra measures to verify the accuracy of personal data about minors?

8.13 When establishing measures to comply with the Accuracy Obligation under the Data Protection Provisions, organisations should also consider taking extra steps to verify the accuracy of personal data about a minor, especially where such inaccuracy may have severe consequences for the minor.

Who should organisations notify if there is a data breach involving a minor?

8.14 In the case of a data breach resulting in significant harm to individuals who are minors, the organisation's obligation to inform the affected data subject remains, even though the data subject is a minor. It may be prudent for the organisation to inform the minor's parent or guardian of the data breach where feasible, since this allows the minor's parent or guardian to take steps to mitigate the harm of the data breach.

8.15 There may be cases of notifiable data breaches in which the organisation may not wish to notify the affected individual, such as (but not limited to) information laid out in Parts 1(5), (6) and (23) of the Schedule of the Personal Data Protection (Notification of Data Breaches) Regulations 2021. In such cases, organisations are strongly encouraged to notify the Commission and the relevant sector regulator first to seek guidance on the issue.

9 Cloud Services

What responsibilities do organisations have under the PDPA when using cloud services to process personal data in the cloud?

9.1 When using cloud services, the organisation is responsible for complying with all obligations under the PDPA in respect of personal data processed by the cloud service provider ("CSP") on its behalf and for its purposes. Processing is defined in the PDPA as the carrying out of any operation or set of operations in relation to the personal data, and includes recording, holding, organising, adapting or altering, and retrieval of personal data.

What responsibilities do CSPs have under the PDPA for the personal data they process for organisations?

9.2 Where the CSP is processing personal data on behalf and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing, the CSP is considered a data intermediary and subject to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA. Its Protection, Retention Limitation and Data Breach Notification Obligations extend to personal data that it processes or hosts for the organisation in data centres outside Singapore. The CSP, as an organisation in its own right, remains responsible for complying with all Data Protection Provisions in respect of its own activities which do not constitute processing of personal data under the contract. More information on the obligations of data intermediaries can be found in the Key Concepts Guidelines.

Who is responsible for complying with the Transfer Limitation Obligation for overseas transfers of personal data as part of CSPs' processing of personal data in the cloud?

9.3 An organisation that engages a CSP as a data intermediary to provide cloud services is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data in using the CSP's cloud services. This is regardless of whether the CSP is located in Singapore or overseas.

How should organisations ensure compliance with the Transfer Limitation Obligation for overseas transfers of personal data by their CSPs?

9.4 An organisation should ensure that any overseas transfer of personal data as a result of engaging a CSP will be done in accordance with the requirements under the PDPA, namely, the organisation could ensure that the CSP it uses only transfers data to locations with comparable data protection regimes, or has legally enforceable obligations to ensure a comparable standard of protection for the transferred

personal data. Such issues of compliance can be provided for in the written contract between an organisation and its CSP. The contract should deal with both the standard of protection and the overseas locations

9.5 The organisation may be considered to have taken appropriate measures to comply with the Transfer Limitation Obligation by ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients (e.g. data centres or sub-processors) in these locations are legally bound by similar contractual standards.

9.6	**Example:** Organisation ABC wishes to engage CSP DEF based in Singapore to process personal data in the cloud on its behalf. ABC had assessed that Hong Kong's data protection laws are comparable to the PDPA. Before signing up for its services, ABC conveys to DEF that it only wishes to store the personal data in data centres in Singapore and Hong Kong, and includes a clause in the contract to state so. A data breach subsequently occurs while the personal data is in the possession of DEF. ABC's due diligence in engaging DEF would be taken into consideration in the Commission's assessment of liability when determining whether ABC has breached its obligations under the PDPA. DEF may also be liable for breach of its Protection Obligation.
9.7	**Example:** Organisation GHI wishes to engage CSP JKL based in Singapore to process personal data in the cloud on its behalf. JKL will only store personal data in data centres in Singapore, Japan and South Korea. In engaging JKL's cloud services, GHI ensures that its contract with JKL specifies that the data centres and any sub-processors in Japan and South Korea are legally bound to comply with standards that are comparable to the PDPA. A data breach subsequently occurs while the personal data is in the possession of JKL. GHI's due diligence in engaging JKL would be taken into consideration in the Commission's assessment of liability when determining whether GHI has breached its obligations under the PDPA. JKL may also be liable for breach of its Protection Obligation.

9.8 CSPs based in Singapore have to meet the standards of protection under the Data Protection Provisions when they process personal data as data intermediaries. Industry standards like ISO27001 and Tier 3 of the Multi-Tiered Cloud Security

("MTCS") Certification Scheme could provide assurance of the CSP's ability to comply with the Protection Obligation of the PDPA.

9.9 Where the contract between an organisation and its CSP does not specify the locations to which a CSP may transfer the personal data processed and leaves it to the discretion of the CSP, the organisation may be considered to have taken appropriate steps to comply with the Transfer Limitation Obligation by ensuring that (a) the CSP based in Singapore is certified or accredited as meeting relevant industry standards, and (b) the CSP provides assurances that all the data centres or sub-processors in overseas locations that the personal data is transferred to comply with these standards. For example, the organisation could consider engaging a CSP that is certified as compliant with the ISO27001 standard and can produce technical audit reports such as the SOC-2 upon request.

9.10	**Example:** Organisation MNO wishes to purchase an off-the-shelf cloud service offered by CSP PQR. In its standard end-user agreement, PQR does not specify the locations to which the personal data may be transferred in the course of processing. However, MNO ensures that all data centres and sub-processors to which personal data may be transferred to in using PQR's off-the-shelf cloud service are certified as compliant with the ISO27001. A data breach subsequently occurs while the personal data is in the possession of PQR. MNO's due diligence in engaging PQR would be taken into consideration in the Commission's assessment of liability when determining whether MNO has breached its obligations under the PDPA. In particular, insofar as MNO has taken appropriate steps to ensure that PQR is able to comply with the PDPA in respect of the transferred personal data, MNO is taken to have satisfied the requirements for the Transfer Limitation Obligation. PQR may also be liable for breach of its Protection Obligation.

END OF DOCUMENT