15 The Access and Correction Obligations

15.1 Sections 21 and 22 of the PDPA set out the rights of individuals to request for access to their personal data and for correction of their personal data that is in the possession or under the control of an organisation, and the corresponding obligations of the organisation to provide access to, and correction of, the individual's personal data. These obligations are collectively referred to in these Guidelines as the Access and Correction Obligations as they operate together to provide individuals with the ability to verify their personal data held by an organisation.

15.2 The Access and Correction Obligations relate to personal data in an organisation's possession as well as personal data that is under its control (which may not be in its possession). For example, if an organisation has transferred personal data to a data intermediary that is processing the personal data under the control of the organisation, the organisation's response to an access or correction request must take into account the personal data which is in the possession of the data intermediary. The PDPA does not directly impose the Access and Correction Obligations on a data intermediary in relation to personal data that it is processing only on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing[15]. A data intermediary may (but is not obligated under the PDPA to) forward the individual's access or correction request to the organisation that controls the personal data. The Commission understands that, in some cases, an organisation may wish to enter into a contract with its data intermediary for the data intermediary to assist with responding to access or correction requests on its behalf. In this connection, the Commission would remind organisations that engage the data intermediary, that they remain responsible for ensuring compliance with the Access and Correction Obligations under the PDPA. Please refer to the sections on data intermediaries and their obligations for more information.

<u>Obligation to provide access to personal data</u>

15.3 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible:

a) personal data about the individual that is in the possession or under the

[15] Section 4(2) of the PDPA states that Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

control of the organisation; and

b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

15.4 Section 21(1) allows an individual to submit a request to an organisation for access to personal data about him that is in the possession or under the control of the organisation (an "access request"). Such a request may be for:

a) some or all of the individual's personal data; and

b) information about the ways the personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

15.5 An organisation's obligation in responding to an access request is to provide the individual access to the complete set of personal data requested by the individual which is in the organisation's possession or under its control, unless any relevant exception in section 21 or the Fifth Schedule to the PDPA applies.

15.6 To be clear, an organisation is not required to provide access to the documents (or systems) which do not comprise or contain the personal data in question, as long as the organisation provides the individual with the personal data that the individual requested and is entitled to have access to under section 21 of the PDPA. In the case of a document containing the personal data in question, the organisation may provide only the personal data (or the sections of the document containing the personal data) if it is feasible for it to do so.

15.7 An organisation does not need to provide access to information which is no longer within its possession or under its control when the access request is received. The organisation should generally inform the requesting individual that it no longer possesses the personal data and is thus unable to meet the individual's access request. Organisations are also not required to provide information on the source of the personal data.

15.8 In certain circumstances, the individual making the access request may ask for a copy of his personal data in documentary form. Organisations should provide the copy and have the option of charging the individual a reasonable fee for producing the copy (please see the section on "fees chargeable for access to personal data" for more details). If the requested personal data resides in a form that cannot practicably be provided to the individual in documentary form, whether as physical or electronic copies (for example, the data cannot be extracted from a special

machine owned by the organisation), then the organisation may provide the individual a reasonable opportunity to examine the requested data in person.

15.9 Organisations should note that the obligation to provide access applies equally to personal data captured in unstructured forms such as personal data embedded in emails. Organisations are generally required to implement processes to keep track of the collection, use, and disclosure of all personal data under their control, including unstructured data. Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest or if the request is otherwise frivolous or vexatious. Please see the sections on exceptions to the obligation to provide access to personal data for more details (including on mandatory exceptions relating to situations where an organisation must not provide access).

15.10 If the personal data requested by the individual can be retrieved by the individual himself (e.g. resides in online portals in which access has been granted by the organisation), the organisation may inform the individual how he may retrieve the data requested.

> Example:
>
> Organisation ABC receives a request from John seeking to know what personal data relating to him was disclosed in Organisation ABC's correspondence with Organisation DEF in a specified month within the last one year. Assuming that the request does not fall under any relevant exception (for example, it is not opinion data kept solely for an evaluative purpose), Organisation ABC is required to provide John with his personal data even if its correspondence with Organisation DEF had not been archived in a formalised system such as a database.
>
> To be clear, Organisation ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in their possession or control, and it is not necessarily required to provide John with copies of the actual correspondence with Organisation DEF.

15.11 The PDPA does not expressly state that an access request be accompanied by a reason for making the request. However, an organisation should ask the applicant to be more specific as to what type of personal data he requires, the time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section

21(3) of the PDPA or any exception in the Fifth Schedule[16]. When assessing an access request, the organisation should consider the purpose of the applicant's access request, so as to determine the appropriate manner and form in which access to the personal data should be provided. For instance, the organisation may determine that it will provide the individual a print-out from a video instead of a masked video clip as the most cost effective and efficient way to allow an individual to show that he was present at a particular location at a specific date and time. If the individual is unable or unwilling to provide more details, the organisation should make an attempt to respond to the access request as accurately and completely as reasonably possible.

15.12 Before responding to an access request, organisations should exercise due diligence and adopt appropriate measures to verify an individual's identity. While the Commission does not prescribe the manner in which organisations are to obtain verification from the individual making an access request, organisations are encouraged to have documentary evidence to demonstrate that it is in compliance with the PDPA, and minimise any potential disputes. Organisations may implement policies setting out the standard operating procedures on conducting verification when processing access requests (e.g. this may include the questions that an employee handling the access request may ask the applicant in order to verify his identity)[17].

15.13 In a situation where a third party is making an access request on behalf of an individual, organisations receiving the access request should ensure that the third party has the legal authority to validly act on behalf of the individual.

15.14 In some cases, there may be two or more individuals (e.g. husband and wife) making an access request at the same time for their respective personal data captured in the same set of records. The organisation may obtain consent[18] from the respective individuals to disclose their personal data to each other, so that it may provide the individuals access to a common data set containing their personal data, without

[16] The Commission notes that an access request may be more easily fulfilled if sufficient information is provided by the applicant to enable an organisation to process the request.

[17] Among other things, an organisation must implement policies and practices that are necessary for it to meet its obligations under the PDPA under section 12 of the PDPA.

[18] The organisation may also consider if deemed consent may apply. An individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so. When it is unclear whether consent may be deemed, organisations should obtain consent from the individual to collect, use or disclose his personal data (as the case may be) for the relevant purposes in order to avoid any dispute over whether consent was given.

having to exclude the personal data of the other individuals[19]. If such consent cannot be obtained, an organisation receiving such requests may provide access to the personal data to the individuals separately, for example, by masking the personal data of the other individuals before providing the individual access to his own personal data (i.e. the individual will be provided access to only his own personal data).

Information relating to ways which personal data has been used or disclosed

15.15 As stated in section 21(1) of the PDPA, if an individual requests for information relating to the use or disclosure of his personal data by the organisation, the organisation is required to provide information relating to how the personal data has been or may have been used or disclosed within the past year. In this regard, an organisation may develop a standard list of all possible third parties to whom personal data may have been disclosed by the organisation. In many cases, an organisation may provide this standard list as an alternative to providing the specific set of third parties to whom the personal data has been disclosed, as part of its response to access requests that ask for information relating to how the personal data has been or may have been disclosed within the past year. The organisation should also update the standard list regularly and ensure that the information is accurate before providing the list to the individual. Generally, in responding to a request for information on third parties to which personal data has been disclosed, the organisation should individually identify each possible third party (e.g. 'pharmaceutical company ABC'), instead of simply providing general categories of organisations (e.g. 'pharmaceutical companies') to which personal data has been disclosed. This would allow individuals to directly approach the third party organisation to which his personal data has been disclosed.

15.16 In specifying how the personal data has been or may have been used or disclosed within the past year, organisations may provide information on the purposes rather than the specific activities for which the personal data had been or may have been used or disclosed. For example, an organisation may have disclosed personal data to external auditors on multiple occasions in the year before the access request. In responding to an access request, the organisation may state that the personal data was disclosed for audit purposes rather than describing all the instances when the personal data was disclosed.

15.17 Generally, the organisation's actual response would depend on the specific request,

[19] Obtaining consent from the respective parties may address the prohibition against revealing their personal data under section 21(3)(c) of the PDPA. However, organisations are reminded to also consider if there are other prohibitions or exceptions to providing access that would apply.

and organisations are reminded that in meeting their responsibilities under the PDPA, they are to consider what a reasonable person would consider appropriate in the circumstances.

> Example:
>
> Sarah makes an access request to her spa, requesting for information relating to how her personal data has been used or disclosed. The request was made on 5 December 2015. The spa is only required to provide information on how her personal data has been used or disclosed within the past year – that is, the period from 6 December 2014 to the date of the request, 5 December 2015.

Response time frame for an access request

15.18 Subject to the PDPA and the Personal Data Protection Regulations[20], an organisation is required to comply with section 21(1) of the PDPA and must respond to an access request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30 days[21] after receiving the request, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request.

When not to accede to an access request

15.19 An organisation must respond to an access request by providing access to the personal data requested, or by informing the individual of a rejection of the access request where it has valid grounds not to provide access.

15.20 Organisations are not required to accede to a request if an exception[22] from the access requirement applies.

15.21 Additionally, an organisation shall not inform any individual or organisation that it has disclosed personal data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the personal data is disclosed

[20] Please refer to sections 21(2), 21(3), 21(4) and 21(5) of the PDPA and Personal Data Protection Regulations 2014, Part II.

[21] Generally, this refers to 30 calendar days. This may however be extended in accordance with rules on computation of time under the law, e.g. where the last day of the period falls on a Sunday or public holiday, the period shall include the next day not being a Sunday or public holiday.

[22] The Fifth Schedule of the PDPA specifies the exceptions which apply.

to an authorised[23] officer of the agency. In this regard, an organisation may refuse to confirm or deny the existence of personal data, or the use of personal data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.

15.22 It also does not have to respond to a request unless the applicant agrees to pay the fee for services provided to the applicant to enable the organisation to respond to the applicant's request. This is provided the organisation has provided the applicant a written estimate of the fee. Where applicable, the Commission may review the fee by confirming, reducing or disallowing the fee, or directing the organisation to make a refund to the applicant.

15.23 An organisation shall not accede to an access request if any of the grounds in section 21(3) are applicable, for instance, where the provision of the personal data or other information could reasonably be expected to threaten the safety or physical or mental health of an individual other than the requesting individual, or to cause immediate or grave harm to the safety or physical or mental health of the requesting individual.

15.24 If the organisation searches for the requested personal data but is unable to respond to the access request within the 30-day timeframe (e.g. technical processing of personal data residing in a specific format requires more time), the organisation must inform the applicant within the 30-day timeframe of the date when it will be able to respond to the request, and must still respond to the request as soon as reasonably possible.

Fees chargeable to comply with the access obligation

15.25 An organisation may charge an individual a reasonable fee to process an access request by the individual[24]. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request. This may include the time and costs incurred to search for the personal data requested. An example of such incremental costs is the cost of producing a physical copy of the personal data for the individual requesting it. As organisations are required to make the necessary arrangements to provide for standard types of access requests, costs incurred in capital purchases (e.g. purchasing new equipment in order to provide access to the requested personal data) should not be transferred to individuals.

[23] Paragraph 1(n) of the Fourth Schedule of the PDPA specifies the circumstances under which an officer is authorised.

[24] Regardless of whether or not access to the personal data requested is eventually provided by the organisation.

15.26 The Commission is of the view that it would be difficult to prescribe a standard fee or range of fees at the outset to apply across all industries or all types of access requests. Organisations should exercise proper judgement in deriving the reasonable fee they charge based on their incremental costs of providing access. The Commission may, upon the application of an individual, review a fee charged by an organisation under section 28 of the PDPA (among other matters). In reviewing a fee, the Commission may consider the relevant circumstances, including the absolute amount of the fee, the incremental cost of providing access which may include the time and costs incurred to search for the personal data requested, and similar fees charged in the industry.

15.27 If an organisation wishes to charge an individual a fee to process an access request, the organisation must give the individual a written estimate of the fee[25]. If the organisation wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organisation may refuse to process or provide access to the individual's personal data until the individual agrees to pay the relevant fee.

Example: Company ZYX receives an access request from a customer to view his personal data stored in a format that is readable only by a special machine. The company owns two such machines but both are faulty. In order to respond to the customer's request in a timely manner, Company ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounted to $50,000. Under the PDPA, this would not be considered a reasonable fee as Company ZYX is expected to have the general means to comply with its customers' access requests.
Example: An individual requests from Company TUV a paper copy of his personal data. Company TUV charges a fee of $50 for the information printed out on 50 pages of paper, based on the incremental cost of producing the copy. The fee is reasonable as it reflects the incremental cost of providing the personal data.

<u>Exceptions to the obligation to provide access to personal data</u>

15.28 The obligation in section 21(1) is subject to a number of exceptions in sections 21(2) to 21(4) including some mandatory exceptions relating to situations where an

[25] If the Commission has reviewed a fee under section 28(1)(b) of the PDPA, then the final fee charged should not exceed the amount of the fee allowed by the Commission under section 28(2)(b) of the PDPA.

organisation must not provide access. These exceptions are listed below.

15.29 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to.

15.30 The exceptions specified in the Fifth Schedule include the following matters:

a) opinion data kept solely for an evaluative purpose[26];

b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

e) a document related to a prosecution if all proceedings related to the prosecution have not yet been completed;

f) personal data which is subject to legal privilege;

g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

h) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed[27];

i) the personal data was collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he was appointed to act –

i. under a collective agreement under the Industrial Relations Act (Cap. 136);

[26] The term "evaluative purpose" is defined in section 2(1) of the PDPA.

[27] The terms "investigation" and "proceedings" are defined in section 2(1) of the PDPA.

ii. by agreement between the parties to the arbitration or mediation;

iii. under any written law; or

iv. by a court, arbitral institution or mediation centre; or

j) any request —

i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;

ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;

iii. for information that does not exist or cannot be found;

iv. for information that is trivial; or

v. that is otherwise frivolous or vexatious.

Example:

A shopping centre receives a request from an individual to view all CCTV footage of him recorded at the shopping centre over the past year. In this scenario, reviewing all CCTV footage from the past year to find records of the individual making the request would require considerable time and effort. To the extent that the burden of providing access would be unreasonable to the shopping centre and disproportionate to the individual's interests as the individual is making a general request for all CCTV footage, the shopping centre is unlikely to have to provide the requested personal data under the Access and Correction Obligations.

Example:

A shop in the shopping centre receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently by the shop that the individual was invited to. The individual provides the shop with sufficient information to determine when the event was held. The provision of access in this case would be reasonable and the shop should provide the photo which the individual requested.

Example: An individual sends an email providing feedback to Organisation XYZ. The form contains his personal data including his full name and contact number. A day later, he requests access to the personal data in the form while having full knowledge of the information he is requesting. Such a request is likely to be considered frivolous or vexatious, unless it can be shown otherwise.
Example: An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests.

15.31 In addition to the matters specified in the Fifth Schedule to the PDPA, section 21(3) specifies a number of situations in which an organisation must not provide the personal data or other information specified in section 21(1).

15.32 The situations specified in section 21(3) are where the provision of personal data or other information under section 21(1) could reasonably be expected to:

a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

c) reveal personal data about another individual;

d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

e) be contrary to the national interest[28].

Providing personal data of an individual without the personal data of other individuals

15.33 Section 21(5) of the PDPA provides that if an organisation is able to provide the individual with his personal data and other information requested under 21(1)

[28] The term "national interest" is defined in section 2(1) of the PDPA as including national defence, national security, public security, the maintenance of essential services and the conduct of international affairs.

without the personal data of other information excluded under 21(2), 21(3) and 21(4), the organisation must provide the individual access to the requested personal data and other information without the personal data or other information excluded. For example, if the personal data requested by the individual also contains personal data of other individual(s), an organisation should consider if it is able to provide the requested personal data without the personal data of the other individuals, such as by masking out the personal data of other individual(s) before providing the personal data requested by the individual.

> Example:
>
> Mary makes an access request with Organisation ABC for footage of herself captured by Organisation ABC's CCTV system on a particular date and time.
>
> Organisation ABC looks for the requested CCTV footage, and finds that the requested footage captured personal data of Mary and two other individuals. Organisation ABC then assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data by masking the images of the other individuals in the same footage.

Access that may reveal personal data about another individual

15.34 One of the prohibitions, section 21(3)(c), requires that an organisation must not provide access to the personal data or other information under section 21(1) where the provision of personal data or other information could reasonably be expected to reveal personal data about another individual. The Commission is of the view that this prohibition does not apply in circumstances where:

a) the other individual has given consent to the disclosure of his personal data; or

b) any of the exceptions listed under the Fourth Schedule[29] to the PDPA apply to the extent that the organisation may disclose the personal data of the other individual without consent.

[29] Disclosure of personal data without consent

Example: John applies to School ABC for access to CCTV footage of himself in a classroom when he was having a discussion with another classmate, Peter. Peter provides consent to the school disclosing his personal data (that is part of the CCTV footage requested by John) to John. School ABC is able to provide John access to the requested CCTV footage without masking Peter's image.
Example: Betty applies to Shopping Centre ABC for access to CCTV footage of herself walking through the aisles of the shopping centre on a specific day and time. The CCTV footage contains images of other individuals. Since the images of the other shoppers are recorded in a public area, the data is considered to be publicly available. Shopping Centre ABC does not need to obtain consent of the other shoppers in the CCTV footage or mask their images before providing access to Betty.

Access request relating to disclosure to prescribed law enforcement agency

15.35 Section 21(4) of the PDPA contains an additional obligation of organisations in relation to the Access and Correction Obligations. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule[30] or under any other written law, the organisation must not inform the individual that personal data has been disclosed.

Access request relating to legal proceedings

15.36 Where personal data has been collected for the purpose of prosecution, investigation, civil proceedings and associated proceedings and appeals, Section 1(h) of the Fifth Schedule may apply to exempt such personal data from the access request. Organisations are thus not required to provide the requested information. Further, under Section 1(e) of the Fifth Schedule, access need not be provided in respect of a document related to a prosecution if all proceedings related to the prosecution have not been completed.

[30] Paragraph 1(f): the disclosure is necessary for any investigation or proceedings, or Paragraph 1(n): the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

15.37 Where personal data has been collected prior to the commencement of prosecution and investigations but is nonetheless relevant to the proceedings, an individual should obtain access through criminal and civil discovery avenues rather than through the access obligation under the PDPA. The intent of an access obligation is to ensure that organisations remain accountable for the personal data of individuals in their possession or under their control, including ensuring the accuracy and proper use of the personal data. The Data Protection Provisions of the PDPA do not affect discovery obligations under law that parties to a legal dispute may have (e.g. pursuant to any order of court). For instance, if criminal disclosure of civil discovery regimes are applicable, section 4(6) of the PDPA applies, and any request for access to the personal data should be made pursuant to any other written laws providing for such disclosure or discovery applications. A possible advantage of obtaining access to personal data through the discovery process is that it allows the requestor to obtain un-redacted and complete documents, while and access request would grant the requestor only his personal data, with other content redacted.

Rejecting an access request

15.38 Subject to the PDPA and the Personal Data Protection Regulations[31], an organisation is to provide a reply to the individual even if the organisation is not providing access to the requested personal data or other requested information. In such a situation, and where appropriate, organisations should, as good practice, inform the individual of the relevant reason(s), so that the individual is aware of and understands the organisation's reason(s) for its decision.

Preservation of personal data when processing an access request

15.39 If an organisation has scheduled periodic disposal or deletion of personal data (e.g. the CCTV system deletes the footage every X days, or physical documents containing personal data are shredded every X days), the organisation is to identify the requested personal data, as soon as reasonably possible after receiving the access request, and ensure the personal data requested is preserved while the organisation is processing the access request.

15.40 However, organisations should generally be mindful not to unnecessarily preserve personal data "just in case" to meet possible access requests, and should not retain personal data indefinitely when there is no business or legal purpose to do so.

[31] In particular, see PDPA section 21(2), 21(3), 21(4) and 21(5) and Personal Data Protection Regulations 2014, Part II.

Preservation of personal data after rejecting an access request

15.41 If an organisation determines that it is appropriate under section 21 of the PDPA and Part II of the Personal Data Protection Regulations 2014[32] to not provide some or all of the personal data requested in the individual's access request ("withheld personal data"), the organisation should, as good practice, preserve a copy of the withheld personal data for a period of at least 30 calendar days after rejecting the access request – as the individual may seek a review of the organisation's decision. In the event the individual submits an application for review to the PDPC and the PDPC determines that it will take up the review application, as soon as the organisation receives a Notice of Review Application from the PDPC, it should, as good practice, preserve the withheld personal data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

15.42 Notwithstanding the foregoing, in the event it is determined by the Commission or any appellate body that the organisation did not have appropriate grounds under the PDPA to refuse to provide access to the personal data in question and had therefore contravened its obligations under the PDPA, it may face enforcement action under section 29 of the PDPA.

15.43 As good practice, the organisation should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected.

Example:

Mary makes an access request with Organisation ABC for CCTV footage of herself at a particular date and time. Organisation ABC has a CCTV recording system which typically keeps the CCTV footage for 30 days before the footage is overwritten.

As Mary submitted her access request before the scheduled deletion of the specific CCTV footage, the organisation should search for the requested CCTV footage as soon as reasonably possible before the footage is overwritten by the CCTV system.

a) If Organisation ABC assesses the access request and provides Mary access to the requested personal data captured in the CCTV footage, Organisation ABC must delete the footage thereafter if the purpose for collecting the personal data is no longer served by retention and it has no

[32] Requests for access to and correction of personal data.

other business or legal purpose to retain the footage in accordance with the PDPA[33].

b) If, however, Organisation ABC determines that it is to reject Mary's request to access the personal data captured in the CCTV footage, Organisation ABC should preserve the footage for a reasonable period of at least 30 calendar days after rejecting the request, to allow Mary the opportunity to exhaust any recourse under the PDPA.

Obligation to correct personal data

15.44 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation (a "correction request"). Upon receipt of a correction request, the organisation is required to consider whether the correction should be made. In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should –

a) correct the personal data as soon as practicable; and

b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

15.45 An organisation is not entitled to impose a charge for the correction of personal data required under section 22.

15.46 The obligation in section 22(1) is subject to a number of exceptions in section 22(6) and (7) considered below.

15.47 Regarding the obligation to notify other organisations of a correction, section 22(3) of the PDPA allows an organisation other than a credit bureau, with the consent of the individual concerned, to send the corrected personal data only to specific organisations to which the data was disclosed by the organisation within a year before the date the correction was made.

15.48 The other organisations which are notified of a correction made by an organisation responding to a correction request are required under section 22(4) to similarly correct the personal data in their possession or under their control unless they are

[33] Please refer to Chapter 18 on the Retention Limitation Obligation for more information.

satisfied on reasonable grounds that the correction should not be made.

> Example:
>
> An online retailer receives a request from a customer to update his address (which forms part of the customer's personal data). The retailer decides that there are no reasonable grounds to reject the customer's request and proceeds to correct the customer's address in its database.
>
> The retailer also sends the corrected address to its affiliate which is responsible for servicing the customer's warranty as the affiliate may require such information for its own legal or business purposes. The affiliate determines that it does not require the corrected address for any legal or business purpose as the customer's warranty has expired. The affiliate therefore decides that a correction should not be made to all its records relating to the customer and makes a note that it has not made the correction.
>
> The retailer need not send the corrected address to a courier company which had previously delivered certain products purchased from the retailer by the customer as the courier company was engaged to make the particular delivery and does not require an updated address of the customer for its own legal or business purposes.

15.49 If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is responding to a correction request or has been notified of a correction made by such an organisation), section 22(5) requires the organisation to annotate (i.e. make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As good practice, the organisation may also wish to annotate the reasons and explain to the individual why it has decided that the correction should not be made.

Exceptions to the obligation to correct personal data

15.50 Section 22(6) provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. In addition, section 22(7) provides that an organisation is not required to make a correction in respect of the matters specified in the Sixth Schedule to the PDPA. These are:

a) opinion data kept solely for an evaluative purpose[34];

b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; and

e) a document related to a prosecution if all proceedings related to the prosecution have not been completed.

> Example:
>
> An individual disputes his performance evaluation records kept by his ex-employer, Organisation ABC. In anticipation of background checks to be conducted by his new employer, an individual requests that Organisation ABC amend his performance track record to something he considers to be more favourable and accurate compared to the one kept by Organisation ABC. Organisation ABC is not obligated to make the correction to the extent that the individual's performance evaluation records constitute or contain an opinion.

Response time for a correction request

15.51 Subject to exceptions as described above, an organisation is required to correct the personal data as soon as practicable from the time the correction request is made.

[34] The term "evaluative purpose" is defined in section 2(1) of the PDPA to mean:
(a) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates – (i) for employment or for appointment to office; (ii) for promotion in employment or office or for continuance in employment or office; (iii) for removal from employment or office; (iv) for admission to an education institution; (v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits; (vi) for selection for an athletic or artistic purposes; or (vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;
(b) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;
(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or
(d) for such other similar purposes as may be prescribed by the Minister.
No other such purposes have been prescribed to date.

If an organisation is unable to correct the personal data within 30 days[35] from the time the request is made, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to correct the personal data.

Form of access and correction requests

15.52 While organisations may provide standard forms or procedures for individuals to submit access and/or correction requests, organisations should accept all requests made in writing and sent to the business contact information of its Data Protection Officer or in the case of a body corporate, left at or sent by pre-paid post to the registered office or principal office of the body corporate in Singapore, where sufficient information has been provided for the organisation to meet the requests (among others).

15.53 Notwithstanding the foregoing, organisations remain responsible under section 21(1) of the PDPA to provide access as soon as reasonably possible and under section 22(2) of the PDPA to correct the personal data as soon as practicable.

[35] Generally, this refers to 30 calendar days. This may however be extended in accordance with rules on computation of time under the law, e.g. where the last day of the period falls on a Sunday or public holiday, the period shall include the next day not being a Sunday or public holiday.