

18 The Retention Limitation Obligation

18.1 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. This obligation to cease to retain personal data is referred to in these Guidelines as the Retention Limitation Obligation.

How long personal data can be retained

18.2 The Retention Limitation Obligation prevents organisations from retaining personal data in perpetuity where it does not have legal or business reasons to do so. Holding personal data for an indeterminate duration of time increases the risk of a contravention of the Data Protection Provisions. However, as each organisation has its own specific business needs, the Retention Limitation Obligation does not specify a fixed duration of time for which an organisation can retain personal data. Instead, the duration of time for which an organisation can legitimately retain personal data is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and other legal or business purposes for which retention of the personal data may be necessary.

18.3 It should be noted that although the PDPA does not prescribe a specific retention period for personal data, organisations would need to comply with any legal or specific industry-standard requirements that may apply.

18.4 In practice, the retention period for personal data under the PDPA will depend on the following factors:

- a) The purpose(s) for which the personal data was collected. That is:
 - i. personal data may be retained so long as one or more of the purposes for which it was collected remains valid; and
 - ii. personal data must not be kept by an organisation “just in case” it may be needed for other purposes that have not been notified to the individual concerned.

Example:

A dance school has collected personal data of its tutors and students. It retains and uses such data (with the consent of the individuals), even if a tutor or student is no longer with the dance school, for the purpose of maintaining an alumni network. As the dance school is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation.

A retailer retains billing information, including personal data, collected from its customers beyond the Point of Sale for the purposes of accounting and billing administration. As the retailer is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation.

- b) Other legal or business purposes for which retention of the personal data by the organisation is necessary. For example, this may include situations where:
- i. the personal data is required for an ongoing legal action involving the organisation;
 - ii. retention of the personal data is necessary in order to comply with the organisation's obligations under other applicable laws, regulations, international/regional/bilateral standards which require the retention of personal data; or
 - iii. the personal data is required for an organisation to carry out its business operations, such as to generate annual reports, or performance forecasts.

Example:

Under the Limitation Act (Cap. 163), actions founded on a contract (amongst others) must be brought within 6 years from the date on which the cause of action accrued. Hence an organisation may wish to retain records relating to its contracts for 7 years from the date of termination of the contract and possibly for a longer period if an investigation or legal proceedings should commence within that period.

- 18.5 An organisation should review the personal data it holds on a regular basis to determine if that personal data is still needed. An organisation which holds a large quantity of different types of personal data may have to implement varying retention

periods for each type of personal data as appropriate.

- 18.6 In many instances, organisations may already have their own policies regarding retention of documents, which may touch on the duration for which such documents should be kept. These policies will be subject to the requirements of the Retention Limitation Obligation.
- 18.7 Organisations should develop or adjust relevant processes to ensure that personal data is recorded and stored in a manner which facilitates the organisation's compliance with the Retention Limitation Obligation. In this regard, the Commission recognises that organisations may have retention policies which are applied to groups or batches of personal data.
- 18.8 As good practice, organisations should prepare an appropriate personal data retention policy which sets out their approach to retention periods for personal data. In particular, where personal data is retained for a relatively long period of time, an organisation should set out its rationale for doing so in its personal data retention policy.

Ceasing to retain personal data

- 18.9 Where there is no longer a need for an organisation to retain personal data, it must take prompt action to ensure it does not hold such personal data in either one of the two ways set out under the PDPA. That is, an organisation may cease to retain the documents containing personal data or it may remove the means by which the personal data may be associated with particular individuals (that is, to anonymise the data).
- 18.10 An organisation ceases to retain documents containing personal data when it, its agents and its data intermediaries no longer have access to those documents and the personal data they contain. Examples could include:
- a) Returning the documents to the individual concerned;
 - b) Transferring the document to another person on the instructions of the individual concerned;
 - c) Destroying the documents – e.g. by shredding them or disposing of them in an appropriate manner; or
 - d) Anonymising the personal data.
- 18.11 An organisation would not have ceased to retain documents containing personal data where it has merely filed the documents in a locked cabinet, warehoused the

documents or transferred them to a party who is subject to the organisation's control in relation to the documents. In such circumstances, the organisation would be considered to be retaining the documents. Like physical documents, personal data in electronic form(s) which are archived or to which access is limited will still be considered to be retained for the purposes of the Retention Limitation Obligation.

- 18.12 As far as possible, an organisation should cease to retain documents containing personal data in a manner which renders those documents completely irretrievable or inaccessible to the organisation. However, the Commission recognises that there are certain circumstances where the personal data still remain within reach of the organisation or within the organisation's systems in some form. Examples would include shredded documents lying in the bin, or deleted personal data in an unemptied recycling bin on an organisation's computer. In circumstances where there is doubt about whether an organisation has ceased to retain personal data, the Commission will have regard to the factors articulated in the paragraph below.

Factors relevant to whether an organisation has ceased to retain personal data

- 18.13 In considering whether an organisation has ceased to retain personal data the Commission will consider the following factors in relation to the personal data in question:

- a) Whether the organisation has any intention to use or access the personal data;
- b) How much effort and resources the organisation would need to expend in order to use or access the personal data again;
- c) Whether any third parties have been given access to that personal data; and
- d) Whether the organisation has made a reasonable attempt to destroy, dispose of or delete the personal data in a permanent and complete manner.

Anonymising personal data

- 18.14 An organisation will be considered to have ceased to retain personal data when it no longer has the means to associate the personal data with particular individuals – i.e. the personal data has been anonymised. Anonymisation is the process of removing identifying information, such that the remaining data does not identify any particular individual. More details are available in the section on Anonymisation in the Advisory Guidelines on the PDPA for Selected Topics.