



Personal Data Privacy : *Guidance on Collection of Fingerprint Data*

Introduction

This guidance note is intended to assist data users who, having satisfied themselves that it is necessary to collect personal data, wish to collect fingerprint data. The relevant requirements of the Personal Data (Privacy) Ordinance (“the Ordinance”) are highlighted in this guidance note which serves as a useful reference for data users in their consideration of fingerprint collection.

Fingerprints are unique biological data belonging to an individual from which it is practicable for his identity to be directly ascertained. It falls within the definition of “personal data” under the Ordinance.

The collection of fingerprints was traditionally associated with the investigation of crime. However, the advent of low-costs and high-efficient technologies has given rise to the widespread use of fingerprint scanners for other purposes, such as recording attendance and use of facilities provided by the data users. Given the uniqueness and the unchangeable nature of fingerprint data, this trend of practice has caused privacy concerns on the gravity of harm that may cause the data subjects if such data are handled improperly. A data user should as far as practicable resort to other less privacy intrusive alternatives for fulfilling the purpose of collection.

Data Protection Principle 1(1) of the Ordinance generally requires that personal data shall only be collected where it is necessary for a lawful purpose directly related to the function or activity of the data user and that the data collected shall be adequate but not excessive.

In relation to the collection purpose, a data user should ensure that the collection of fingerprint data is for attaining a lawful purpose relating to its function and activity, for instance, the collection of fingerprint data by law enforcement agencies for investigation of crime, or the control of access to high security and restricted areas by permitted personnel. While a data user may have legitimate purposes to collect fingerprint data, such as for keeping accurate attendance records and for efficient deployment of resources, in order to comply with **DPP1(1)**, a data user must carefully assess whether collection of fingerprint data is necessary but not excessive for achieving the purpose of collection.

Adverse privacy impact

In assessing whether it is necessary to collect fingerprint

data, the first question to ask is -

“Is collection of fingerprint data disproportionate to the degree of intrusion into personal data privacy in attaining the purpose of collection?”

The following are some factors relevant for consideration on the extent of intrusion into personal data privacy and the exposure to personal data privacy risks :

- The number of data subjects affected
- The scope and extensiveness of the act or practice
- The vulnerability of the class of data subjects in question
- The extent of the data that will be collected, e.g. whether only the thumb print or prints of all the fingers and whether the whole image of the fingerprints or only partial characteristics are recorded as template
- The intended use of the data and permitted classes of transferees
- The risk of identity theft and the appropriate level of security measures in place
- The period of retention of the data collected
- The harm that can result in the event of a security breach or leakage
- The adverse actions (e.g. disciplinary action or termination of employment, etc.) that may be taken against the data subjects in reliance of the information generated from collection of the fingerprint data

Mitigating the adverse privacy impact

The next question to consider is -

“Have sufficient measures been taken to lessen or mitigate the adverse privacy impact?”

In handling the personal data privacy risks and lessening the adverse impact on personal data privacy, the following measures should be considered :

- Confine the act or practice only to those data subjects the collection of their fingerprint data are necessary for attaining the lawful purpose of collection. Universal or indiscriminate collection of fingerprint data should be avoided
- Where practicable, do not engage in continuous and wide scale use of fingerprint scanners
- Avoid collecting fingerprints from data subjects who

lack the mental capacity to understand the privacy impact (e.g. children of tender age)

- Inform the data subjects explicitly of all the uses, including the intended purposes of use on the fingerprint data collected and the class(es) of persons to whom the fingerprint data may be transferred
- Steps have to be taken to prevent misuses or “function creeps” of the fingerprint data, for example, through unnecessary linkage with other IT systems or databases
- Ensure that there are sufficient security measures in place to protect the fingerprint data from unauthorized or accidental access. Privacy enhancement technologies, such as proper encryption should be adopted to guard against decryption, or reverse engineering of the full image of the fingerprints. Personnel entrusted with handling the fingerprint data should possess the requisite training and awareness on protection of personal data privacy
- The collected fingerprint data should be regularly and frequently erased upon fulfillment of the purpose of collection; excessive retention and hoarding of the data increases the privacy risk
- Where adverse action, for instance, disciplinary action or termination of employment, may be taken against the data subject in reliance of the fingerprint data, the data subject should as far as practicable, be given a chance to respond and challenge the accuracy of the data so used

It is generally taken to be excessive to collect fingerprint data when the adverse impact on personal data privacy outweighs the benefits to be derived from the purpose of collection. To evidence the mitigating measures undertaken by the data user, it is recommended good practice that the steps taken be documented and data subjects affected be consulted beforehand so that their reasonable expectation of privacy can be ascertained and their privacy concerns can be addressed.

Options to be considered and made available

A data user should as far as practicable provide the data subject with the right to choose freely a less privacy-intrusive alternative other than the collection of his or her fingerprint data, for example, the option of using smart card or electronic access permit, etc. The data user should adopt all practicable steps to lessen the adverse privacy impact and protect the data subjects’ personal data privacy. Any steps so taken will be viewed favorably by the Privacy Commissioner should a complaint come before him.

Consent of data subject

The Privacy Commissioner respects the decision made by a data subject to voluntarily supply his fingerprint data for specific purposes. However, for consent to be voluntarily and expressly given, the Privacy Commissioner regards it as critical that (i) the data subject

does possess the requisite mental capacity to understand the adverse impact on his personal data privacy; and (ii) there be no undue influence on the data subject when his consent is sought.

For data subjects who are of tender age, it is objectionable from the perspective of personal data protection that they be exposed to acts or practices that devalue privacy which may make them less aware of the data privacy risks that may impact upon them in later life. In other situations where a special relationship exists, the data subject should be sufficiently informed of the adverse impact on personal data privacy brought about by the collection of fingerprint data and be given a fair option to choose between giving or withholding the data. The decision of the data subject should be respected. The data user would do well to put itself in a position to dispel any reasonable suspicion of undue influence due to the disparity in bargaining powers.

Proper handling of fingerprint data collected

If fingerprint data are collected, the data user shall implement sufficient privacy protective measures. A privacy policy and procedure need to be devised setting out clearly the rules and practices that are to be followed in collecting, holding, processing and using fingerprint data. The IT system which is used to store and process the data should be carefully assessed and regularly reviewed to ensure that sufficient privacy protective measures are in place. Effective control should also be established to guard against excessive retention, improper use, unauthorized or accidental access and processing. Proper training, guidance and supervision have to be given to the staff responsible for the collection and management of the fingerprint data. It is recommended good practice that regular privacy compliance assessment and reviews be conducted by the data user to verify that the acts done and practices engaged are in compliance with the Ordinance.

[The information provided in this guidance note is for general guidance only.]

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline: (852) 2827 2827

Fax: (852) 2877 7026

Address: 12/F, 248 Queen’s Road East, Wanchai, Hong Kong.

Website: www.pcpd.org.hk

E-mail: enquiry@pcpd.org.hk

© Office of the Privacy Commissioner for Personal Data, Hong Kong
August 2007

Reproduction of all or any parts of this guidance is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in the reproduction.