香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Guidance Note

Guidance on Collection of Fingerprint Data

Introduction

This guidance note is intended to assist data users who wish to collect fingerprint data to comply with the Personal Data (Privacy) Ordinance ("the Ordinance"). This should be read BEFORE they decide whether to collect fingerprint data, and if collected, be regularly referred to.

For the purpose of this guidance note, the term "fingerprint data" relates to any representation of information about the fingerprint of a living individual and includes the image of and numerical codes derived from a fingerprint.

Collection of fingerprints has long been associated with the investigation of crime. Lowered costs and easy-to-use technologies have recently brought fingerprint scanners into widespread use for other purposes such as recording attendance and access to specific facilities. Given the uniqueness and the immutability of fingerprint data, the growing popularity of fingerprint scanners has raised privacy concerns as to the gravity of the harm that may be caused to the individuals 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 fingerprint data collection.

This guidance note deals with the following questions:

1. Why are fingerprint data personal data?
2. Whether or not fingerprint data should be collected?
3. What are the principal requirements under the Ordinance on data collection?
4. What is a privacy impact assessment and what needs to be considered in conducting the assessment?
5. What should be considered in ensuring that the individuals have free and informed choice and can make a conscious decision on whether or not to supply the fingerprint data?
6. What should be addressed after having decided to collect fingerprint data?

Why are fingerprint data personal data?

The term "personal data" under the Ordinance means any data (i) relating directly or indirectly to a living individual; (ii) from which it is reasonably practicable for the identity of the individual to be directly or indirectly ascertained; and (iii) in a form in which access to or processing of the data is reasonably practicable.

There is no doubt that fingerprints are unique biometric data belonging to an individual, but views vary as to how practical it is to identify an individual based on a fingerprint image, or on data which represent features of a fingerprint.

A lay person may not be able to ascertain the identity of an individual by looking at the individual's fingerprint image. Even more so, where only unique numerical codes are generated from the characteristics of a fingerprint, one would not normally be able to tell from the codes the identity of the person whom the codes represent. For this reason, one might think that fingerprint data are not personal data. However, this view would not be correct if one can, by linking the fingerprint image or the codes (however derived and fragmented) with, say, another database, identify a particular individual. In such a case, the fingerprint image or the codes (as the case may be), when combined with other identifying data, would be considered personal data under the Ordinance.

Whether or not fingerprint data should be collected?

Following the Court decision in *Eastweek Publisher Limited & Another v. Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83, the Privacy Commissioner for Personal Data ("the Privacy Commissioner") has taken the general view that where there is no collection of personal data at all, the matter would fall outside the jurisdiction of the Ordinance.

In some cases, even where fingerprint data are involved, there may not have been collection of personal data. For instance, an employer may wish to install a fingerprint recognition system which converts certain features of the fingerprint of an employee into unique numerical codes and only stores the latter in a smart card held by the employee. Whenever the employee presents the smart card and his fingerprint, the system verifies the identity of the employee by comparing and matching the numerical codes stored in the smart card with the fingerprint features presented by the employee. The employer does not hold or have access to a copy of the employee's fingerprint data except at the time of the comparison. Since the employer in such a case has not collected the employee's fingerprint data, the fingerprint recognition system would not be regulated by the Ordinance.

Requirements on collection of fingerprint data

Data Protection Principle ("DPP") 1(1) of the Ordinance generally requires that personal data shall not be collected unless they are collected for a lawful purpose directly related to the function or activity of the data user, the collection of the data is necessary for or directly related to that purpose, and that the data collected shall be adequate but not excessive.

A data user should ensure that the collection of fingerprint data is for a lawful purpose related directly 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.

Privacy Impact Assessment

Given the sensitive nature of fingerprint data, data users who are considering collection of fingerprint data must first consider, in compliance with DPP1(1), whether such collection is necessary at all. To this end, they are encouraged to conduct a privacy impact assessment.

Privacy impact assessment ("PIA") is a systemic process that evaluates a proposal in terms of its impact upon personal data privacy. The objective of the PIA is to avoid or minimize adverse impact.

There is no hard and fast rule in determining whether collection of fingerprint data is "necessary and not excessive". The situations and justification of different data users vary widely. Below are some indicators to assist data users in conducting the PIA.

Purpose of collecting fingerprint data

Data users should answer at least the following questions to determine whether collection of fingerprint data is necessary:-

- ◇ What is the need or purpose served by collecting fingerprint data?
- ◇ If there is already a system in place intended to serve the need or achieve the purpose, what is wrong with the existing system?
- ◇ Can the inadequacy or problem with the existing system be remedied? If so, why not arrange such a remedy?
- ◇ Is there an alternative method or system that can be used to achieve the purpose without collecting fingerprint data? If so, why not use the alternative?

Answering these questions enables data users not only to assess whether collection of fingerprint data is necessary or not, it also helps them to explain why collection is necessary in the event of any legal challenge arising under the Ordinance. It is therefore important that the data users document their justification(s).

Purpose and justification for collecting fingerprint data vary in different situations. While the Privacy Commissioner will consider them on a case-by-case basis, some purposes are common and it would be useful to discuss them here for general guidance.

- ◇ Recording attendance: Usually, attendance of staff or students may be recorded by signing in personally or with the use of access cards held by the staff or students. Data users should have good reasons for collecting their fingerprint data instead of or in addition to such measures.

- ◇ Security: While collection of fingerprint data may be justified by security reasons, e.g. to ensure that only authorized persons are permitted to enter restricted areas or to gain access to confidential information, use of fingerprint data is not necessarily a better choice. Access to restricted areas or data may be protected by passwords given to authorized persons. Installation of surveillance cameras monitoring restricted areas or computer terminal may strengthen the security.

The above purposes (attendance and security) may often be achieved by means that are less privacy intrusive and more economical than installing a system to collect and process fingerprint data.

Consider whose fingerprint data are intended to be collected

If the fingerprint data of a large number of individuals are to be collected, the potential damage caused by data breaches would be more serious. Stronger justification is thus required for collecting fingerprint data.

Where, for instance, the purpose of collection is to ensure that only authorized persons can enter an area or gain access to a database, only the fingerprint data of those authorized persons instead of the larger population of both authorized and unauthorized individuals should be collected.

Children of school age or individuals who are incapable of managing their own affairs are vulnerable and require stronger protection of their data privacy. Collection of fingerprint data from these groups, if challenged, will be critically examined by the Privacy Commissioner.

Consider the extent of the data to be collected

In ordinary circumstances, it should not be necessary for data users to collect fingerprint data of all fingers of an individual.

Even if only a number of reference points of a finger would be used to generate a numerical code, the number of fingerprint reference points should be kept to a minimum (e.g. the number of reference points a data user needs in managing a population of 30 should be less than that needed by a data user managing 1,000 individuals.) In any case, the numerical codes derived from a fingerprint should be stored in such a form from which it is technically infeasible or difficult to convert back to the original fingerprint image.

Continuous and widespread use of fingerprint scanners, e.g. installation of fingerprint scanners in all accessible areas including washrooms, should be avoided.

Free and informed choice to permit conscious decision by individuals when they provide fingerprint data

Individuals should be provided with free and informed choice and given a full explanation of the personal data privacy impact of the collection of their fingerprint data.

Each individual is free to decide on whether or not and how his/her fingerprint data should be collected or processed by the data user. If the individual permits his/her personal data to be collected and managed in a particular way, this choice has to be respected and the Privacy Commissioner will not interfere unless the individual's decision-making is called into question, e.g. it was not an informed choice of the individual, the choice was not made voluntarily, or he/she was under undue pressure in consenting to the collection and processing of his/her personal data. It is recommended that the individuals' consent should be recorded in writing to minimize room for dispute.

A data user should as far as practicable provide each individual with the free choice of a less privacy-intrusive alternative to the collection of his or her fingerprint data, for example, the option of using a smart card or an electronic access permit, etc. The data user should adopt all practicable measures to protect the individuals' personal data privacy and reduce the ensuing adverse privacy impact. Evidence of such measures having been taken will be viewed favourably by the Privacy Commissioner should a complaint against the data user be brought before him. Inconvenience to the data user is generally not an acceptable reason for denying such an option to an individual.

For consent to be voluntarily and expressly given, the Privacy Commissioner regards it as critical that (i) the individual possesses the requisite mental capacity to understand the adverse impact on personal data privacy; and (ii) there be no undue influence on the individual when consent is sought.

For children of school age, it is objectionable from the perspective of personal data protection that they be exposed to acts or practices that depreciate privacy; they may as a result become less aware of the data privacy risks inherent in certain acts or practices that may have an adverse impact upon them later in life.

It is common for employees to complain that they were put under pressure by their employers to provide or to consent to the disclosure of their personal data to the employers. Data users who wish to collect employees' fingerprint data must ensure that their employees are given a free and informed choice on whether to supply the data. Even in special cases where collection of employees' fingerprint data is "necessary and not excessive," collection must be by means that is fair in the circumstances. Therefore, employees who are unwilling or unable to supply their fingerprint data should not be penalised.

In other situations where there appears to be a disparity in bargaining powers between the data user and the data subject, 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 should make every effort to dispel any reasonable suspicion of undue influence.

Matters to be attended to after having decided to collect the fingerprint data

Having been satisfied that the collection of fingerprint data is necessary and not excessive, data users should be mindful that the manner of collection and subsequent handling of the data must also comply with other requirements under the Ordinance. Protection of personal data collected is an ongoing legal obligation of the data users.

Duty to inform the data subjects on or before collection

In order to comply with DPP1(3), data users should explicitly inform each individual whose fingerprint data are to be collected:

- Whether provision of the fingerprint data is voluntary or obligatory;
- Where provision of the fingerprint data is obligatory, what the consequences would be for the data subject who fails to provide the data;
- The purpose(s) for which the fingerprint data are to be used;
- Who may have access to the fingerprint data, and under what circumstances may access be gained;
- If the fingerprint data may be transferred to other persons, the classes of persons to whom the data may be transferred in the circumstances that the transfer will be made;
- Whether the fingerprint data could be relied upon to take adverse actions against him/ her; and
- His/her rights to request for access to or correction of the fingerprint data, and how the request should be made (name, post and contact particulars of the person who is authorized to handle the requests).

Establish strong controls for access to, use and transfer of fingerprint data

Fingerprint data should be accessed only on a need-to-know basis. The more people who may have access to the fingerprint data, the more serious the impact on the relevant individual's data privacy.

Data users should not use (including disclosure) an individual's fingerprint data for any purpose that is not related to the purpose for which they were originally collected, unless they have the individual's explicit and voluntary consent to such use, or if such use is exempted from the provisions of the Ordinance. Data users who fail to comply with this requirement may contravene DPP3.

Written policy and clear guidance should be devised to ensure the proper use of the fingerprint data collected, and to prevent unnecessary linkage between the fingerprint database with other IT systems or database that may result in the transfer or change of use of the fingerprint data.

In ordinary circumstances, fingerprint data should not be transferred to any third party. If they are transferred, data users should have strong justification for doing so. Generally speaking, that could be done in limited circumstances, e.g. for the detection of crime.

Retention of fingerprint data

Data users should regularly and frequently purge fingerprint data which are no longer required for the purpose for which they were collected. Otherwise, data users may be in contravention of DPP2(2) and section 26 of the Ordinance.

The longer the retention period of the fingerprint data, the more serious the impact on the relevant individual's data privacy in the event of a data breach. Where, for instance, an employee's fingerprint data have been collected to control access to the employer's premises or computer system, the fingerprint data should be deleted as soon as the employment is terminated.

Ensure data accuracy

Data users are required under DPP2(1) to take all reasonably practicable steps to ensure that the personal data collected are accurate.

If the fingerprint data collected can be used to take adverse action against the individual, accuracy of the data is of particular importance to the individual. For example, where an employee supplies fingerprint data each working day to verify attendance, but due to inaccuracy of the data collected, the employee's attendance at work is not properly recorded, and as a result the data user-employer deducts his salary or terminates his employment.

To ensure that the fingerprint data kept are accurate, data users must ascertain and be satisfied that the false acceptance rate and false rejection rate of the fingerprint recognition system are within a reasonable standard, having regard to the size of the population monitored by the system. Data users should also give the individual reasonable opportunity to explain before deciding whether to take any adverse action against the individual.

Data security

DPP4 requires that all reasonably practicable steps shall be taken to ensure that personal data held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to, among other things, the kind of data and the harm that could result if any of those things should occur. Given the sensitivity of fingerprint data, it is important for data users to guard against compromise and theft of the fingerprint database and that effective security measures should be implemented as are reasonably practicable in the particular circumstances. Examples of some security measures to be considered are:

- ◇ The IT system which is used to store and process the fingerprint data should be carefully evaluated and regularly examined to ensure that sufficiently effective privacy-protective measures are employed;
- ◇ Encrypting the fingerprint data;
- ◇ The database access is restricted to authorized persons on a need-to-know basis and is protected by strong passwords (e.g. combination of letters, numbers and symbols);
- ◇ Access to the database is restricted to a small number of designated terminals only ;
- ◇ Each access is recorded in a log record; and
- ◇ Use of CCTV to monitor the terminal.

Duty to make the privacy policy generally available

Data users should devise privacy policies and procedures setting out clearly the rules and practices that are to be followed in collecting, holding, processing and using fingerprint data. They should draw to the specific attention of the individuals who may be affected by such policies and procedures and make them available for review in compliance with DPP5.

Staff training

It is recommended good practice that regular privacy compliance assessments and reviews be conducted by the data user to verify that the acts done and practices engaged are in compliance with the Ordinance. Proper training, guidance and supervision have to be given to the staff responsible for the collection and management of the fingerprint data. Staff who fail to properly carry out their duties in the handling of fingerprint data should be subject to appropriate disciplinary actions.

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
Email: enquiry@pcpd.org.hk

05/12