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 and Use of Biometric Data

INTRODUCTION

This guidance note is intended to assist data users[1], who wish to collect biometric data, to comply with the Personal Data (Privacy) Ordinance (the "**Ordinance**"). This should be read **BEFORE** data users decide on whether or not biometric data is to be collected, and if collected, be regularly referred to.

Biometric data includes the physiological data[2] with which individuals are born with and behavioural data[3] which is characteristics developed by an individual after birth. Biometric data is therefore data directly related to an individual. While it may not be reasonably practicable for a lay person to ascertain the identity of an individual by merely looking at the individual's fingerprint images or their numeric representations[4], when the biometric data is linked with personal data in another database, a particular individual (also called "data subject" under the Ordinance) can be identified. For the purpose of this guidance note and for the reason above, biometric data is therefore considered to be personal data under the Ordinance[5]. As such, all those who collect and/or use biometric data are data users under the Ordinance.

This guidance note addresses the following topics:

1. **Need for caution to handle sensitive biometric data**
2. **Justifications for collecting and using biometric data**
3. **Risk minimisation techniques in biometric data collection**
4. **The need for a privacy impact assessment**
5. **Free and informed choice to allow collection of one's biometric data**
6. **Privacy requirements for dealing with the biometric data collected**

---

1 Defined under the Personal Data (Privacy) Ordinance as a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data.

2 For examples, DNA samples, fingerprints, palm veins, hand geometry, iris, retina and facial images. Most physiological data cannot be changed.

3 For example, handwriting pattern, typing rhythm, gait and voice pattern. The behavioural data are prone to changes by the individual concerned either consciously or subconsciously.

4 Numeric representations may refer to information describing types and locations of major features of a fingerprint (such as ridge ending, diversion, merger, etc) in relation to each other.

5 Under the Ordinance, "personal data" 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.

1. NEED FOR CAUTION TO HANDLE SENSITIVE BIOMETRIC DATA

Biometric data could be sensitive data as it often contains an individual's intimate information relating to health, mental condition or racial origin[6], and it is often used for identification in criminal investigation[7] because of the uniqueness of the data. Any wrongful disclosure of biometric data could lead to unintended/unauthorised re-identification[8] of individuals, impersonation[9], or even discrimination due to unauthorised disclosure of intimate details of the individuals[10], which all entails grave consequences.

The appropriateness of the collection of biometric data and the precautions to be taken to protect such data collected vary with the level of sensitivity of the biometric data concerned. Data user must consider the sensitive nature of the data concerned, which depends on a number of factors as tabulated below, using an individual's DNA, facial images, palm shape and handwriting pattern as examples:

		DNA	*Facial images*	*Palm shape*	*Handwriting pattern*
1	*Uniqueness*[11]	High	Medium	Low	Low
2	*Any likely changes with time*[11]	No	Yes	Yes	Yes
3	*Multiple purposes of usage*[12]	Yes	No	No	No
4	*Capable to be collected covertly*[13]	Yes	Yes	No	Unlikely
5	*Impact to individual when leaked/ revealed*	Grave[14]	Possibly some	Not so grave[15]	Possibly some[16]

[6] DNA is known to reveal the congenital conditions of an individual, together with gender and ethnic original, and increasingly believed to uncover mental health conditions and the inclination on personality. Retina images have been accepted as being able to tell the health condition of individuals. Some also believe that iris images can indicate individual's health and personality.

[7] Fingerprints, DNA, facial images and handwriting have long been used by law enforcement agencies in criminal investigations for the purpose of identification.

[8] Re-identification may happen when biometric data is leaked with or without other information. For example, if facial images of patients of a drug rehabilitation centre are leaked, it may either directly identify individuals who are famous or arouse interests in identifying the individuals.

[9] For example, if the fingerprint templates are leaked, fake fingers with sufficient details can be produced which may be used to impersonate the owner of the template for gaining access to areas protected by fingerprint recognition system.

[10] If DNA sequence or characteristics are leaked, it may lead to the assumption that the individual concerned has a higher probability of certain health or mental issues (but the individual has not been clinically diagnosed as such) and have services or job opportunities denied.

[11] The combination of uniqueness and whether the biometric data can change over time, or be changed by the data subject, has a great implication in personal data privacy. For biometric data that is unique and impossible to change, such as DNA, any wrongful disclosure will mean that the data subjects can never be disassociated with the leaked data that is potentially accessible by many others.

[12] Multiple purposes of usage often refer to whether the biometric data can be used for purposes other than identification. For example, DNA and retina images could reveal other characteristics, such as physical and mental health conditions, that may otherwise be hidden from public eyes.

[13] Whether biometric data can be capable of collected covertly will suggest whether the data subjects are likely to be aware of the collection and decide on whether to allow for the collection.

[14] The leaking of DNA information for data subject is of grave concerns because the data subject cannot change his own DNA to reduce/eliminate the risk of re-identification. More importantly, other usually hidden characteristics of the data subject will be made known as a result.

[15] The impact of leaking palm shapes of data subjects usually is considered low. Not only palm shapes may be similar to one another and may change over time, the subsequent collection of palm shape for comparison will usually require the data subject to consciously present his palm for measurement.

[16] The impact of leaking of handwriting pattern of data subjects may depend on a number of factors. Usually data subject can deliberately change the pattern to avoid detection and he should usually be aware of any such collection. However, malicious parties may use handwriting pattern analysis to gain knowledge in order to mimic the data subject's signatures.

Keeping of biometric data in its original format may pose greater privacy risk than in their template form[17] because the templates usually contain less details and offer little secondary use when compared with the original image[18]. Data users should therefore, as soon as possible, derive biometric data templates from the original biometric samples/images for storage and subsequent use, and discard the original samples/images safely afterwards. The templates derived from biometric samples/images should be stored in such a form from which it is technically infeasible or difficult to convert back to the original graphical image.

Data user therefore needs to be aware of the sensitivity of the data concerned before deciding what data to collect and in what format they are to be kept. In this regard, the cost and the availability of biometric data readers and scanners should not be the prime concern of the data user.

2. JUSTIFICATIONS FOR COLLECTING AND USING BIOMETRIC DATA

Biometric data may be collected and used for various purposes. For example, in a bio-hazardous laboratory where access must be restricted to trained professionals, retina or iris recognition systems may be used for access control that does not involve any physical contact with the biometric scanner. Another example could be the use of palm-geometry recognition systems for access control and attendance recording by construction-site workers who have attained the necessary skills/safety certificates. In some cases, facial recognition or typing rhythm analyser may be deployed to continuously verify the identities of users of sensitive computer systems after the initial log on. Whether or not a particular type of biometric data could be collected depends on the purpose of their collection and the ways such data are collected.

A data user should ensure that the collection of biometric data is for a lawful purpose related directly to its function and activity[19]. Examples of lawful purpose in this regard include the collection of DNA by law enforcement agencies for investigation of crime, the facial images by immigration department for the immigration control, or the fingerprint by employer for control of access to high security and restricted areas by authorised personnel.

The collection of biometric data must be "necessary and not excessive" for achieving such purpose[20] of investigation of crime, the immigration control, or control of access to restricted areas, etc. Hence, relevant data user has to consider whether it is feasible to collect less sensitive biometric data to achieve the same purpose without compromising effectiveness.

The privacy concerns vary in nature and to different extent, depending on the type of biometric data to be collected and the purpose of such collection. Currently, the fingerprint data and facial images are the most common biometric data collected and used for the purposes of identification and verification, and data user should understand the different privacy concerns in collecting the biometric data for these two purposes.

Identification involves the presenting of a live biometric sample and then asking the system to search and find a match from a database

[17] Templates are numeric information describing relevant features in the biometric data. For example, positions of ridges in fingerprints, and distance between facial features such as eyes, nose and mouth in facial images.

[18] For example, the leakage of fingerprint images may allow higher chance of re-identification, impersonation, and other usages than the leakage of their templates. The leakage of facial images instead of facial templates may reveal the gender and ethnic origin of the data subject.

[19] Data Protection Principle ("DPP") 1(1) of the Ordinance requires that personal data shall not be collected unless it is collected for a lawful purpose directly related to the function or activity of the data user.

[20] DPP1(2) and (3) of the Ordinance requires that 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.

holding templates of many individuals. Because of the possible similarities in the various templates in the database, more reference points are usually needed in the template and from the sample in order to find a match in the database with certainty. For example, in the case of a facial recognition attendance system used in a company of 1,000 people, employee arriving in the office needs to present his faces to a camera, the system then needs to capture features of that employee and compare them with 1,000 templates in the database until only one person is confidently identified. In order to do this, both the features captured and the features stored in templates will have to be quite detailed so that no one else would be mistaken as the person arriving.

Verification, on the other hand, requires fewer reference points from the sample when compared with the identification process. Verification involves the presenting of a live biometric sample and then asking the system to verify whether or not it belongs to a specified person. In this process, the system merely needs to retrieve the template of the claimed individual from the database and confirms that it is the same or similar to the live sample. For a similar example, the employee arriving at work, apart from showing his face to the camera, also enters his staff number to tell the system who he is. In this case, the system only needs to capture fewer details of the face, retrieves the template of the declared employee, and confirm if they match. The system does not need to be overly concerned if there are other similar templates in the database, and how similar those templates are, when carrying out the comparison. As such, the level of details required to perform the verification will be less than the level of details required to identify the employee without knowing firstly who he is.

Very often, commercial organisations collect biometric data just for confirming the identities of individuals and as such they should choose verification biometric systems that operate in the way described above to minimise the number of biometric features to be collected.

3. RISK MINIMISATION TECHNIQUES IN BIOMETRIC DATA COLLECTION

(i) Use of smartcards in storing biometric data/templates

For the purpose of security or access controls, an employer may wish to install a verification system which converts certain biometric data of an employee, say, fingerprints, into templates and have them stored in a smartcard to be given the employee. Whenever the employee presents the smartcard and his fingerprint together to the system, the system can verify the template in the smartcard with the fingerprint presented by the employee and confirm whether or not the fingerprint belongs or is similar to that held in the smartcard. Provided that the employer does not hold or have access to a copy of the employee's fingerprint data except at the time of the comparison (as opposed to the employer centrally storing all the fingerprint templates together with other identifying particulars), the risks and harms associated with misuse and unauthorised disclosure of the fingerprint templates could be reduced. The risk in biometric data collection by a verification system that stores the template in a smartcard to be retained by the data subject will be minimised by a combination of the following measures:

1. The biometric data is not used for purposes other than verification;

2. The biometric data is not kept or stored by the employer anywhere else or by any other means;

3. The biometric data is encrypted and stored only in the employee's smartcard; and

4. No other personal data is stored in the smartcard electronically or printed physically on the card face which can identify to whom the biometric data belongs.

As a recommended best practice, the number of features captured in the template should be proportionate to the number of data subjects the system needs to differentiate. For example, the chance of similar fingerprints in a 10,000 people system will be higher than a system with only 50 people. The latter system therefore does not need to collect as many fingerprint minutiae as the former one for it to work properly. Moreover, the comparison of the templates with the live fingerprints should be carried out in an integrated unit of smartcard reader and fingerprint scanner (so that both the template and the fingerprint image do not need to be transferred to a backend system for processing).

In practice, the smartcard would contain certain identifier of the holder so that a backend system may record the access event for further use (e.g. to maintain attendance record or security log for individuals). So long as any such identifier stored or printed on the smartcard does not reveal the identity of the holder to a third party and there is a genuine need for such a fingerprint verification system, the Privacy Commissioner for Personal Data (the "**Commissioner**") considers the use of fingerprint data to be acceptable in the circumstances.

(ii) Biometric encryption

The use of biometric encryption can also reduce the personal data privacy risk associated with the collection and use of biometric data. Biometric encryption is not about encrypting biometric data but is about an encryption technique that uses biometric data as the encryption key (the secret) for the encryption. The detailed explanation of biometric encryption is beyond the scope of this guidance. Suffice it to note that as no collected biometric data (or its template) is ever stored in the system, the risk associated with misuse and unauthorised disclosure would therefore be small.

4. THE NEED FOR A PRIVACY IMPACT ASSESSMENT ("PIA")

There is no hard and fast rule in determining whether collection of biometric data is "necessary and not excessive". Given the wide range of sensitivity of biometric data, data users who intend to collect biometric data must first consider whether such collection is necessary at all[21]. To this end, they are encouraged to conduct a PIA, which is a systemic process that evaluates a proposal in terms of its impact upon personal data privacy. Engaging a PIA could help to avoid or minimise the adverse impact to the individuals concerned.

Below are some indicators to assist data users in conducting the PIA.

(i) The need for collecting biometric data

Data users should consider the following matters in order to determine whether collection of biometric data is necessary:

- What is the need for the collection of biometric data?
- If there is already a non-biometric system in place to serve the need and if it is not working adequately, can the inadequacy be remedied? If so, remedying the existing system is preferred to resorting to collection of biometric data.
- If there is an alternative system that can be used to serve the same purpose as collecting biometric data, the alternative should be considered by evaluating its privacy intrusiveness.
- Less sensitive and/or less amount of biometric data should be collected to achieve the same purpose in order to minimise the privacy intrusiveness to the individuals concerned.

[21] DPP1(1).

The above considerations would also help the data users justify the need for the collection of biometric data in the event of any legal challenge arising under the Ordinance.

Purpose and justification for collecting biometric data vary according to different situations. While the 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: Attendance of staff or students is usually recorded by signing in personally or with the use of an access card held by the staff or students. Data users must have overriding reasons to justify the collection of biometric data, especially the more sensitive biometric data, instead of or in addition to such usual measures.

- Security control: While collection of biometric data may be justified by security reasons, e.g. to ensure that only authorised persons are permitted to enter restricted areas or to gain access to confidential information, the use of biometric data is not necessarily a better choice. Access to restricted areas or data may also be protected by passwords and access cards given to authorised persons. Installation of surveillance cameras monitoring restricted areas/computer terminal with regular checks may further strengthen security.

Data users need to remember that the purposes of attendance recording and security control may often be achieved by other less privacy-intrusive methods, particularly when sufficient penalty for non-compliance of those methods is introduced.

Continuous and indiscriminative use of biometric scanners, e.g. installation of fingerprint scanners in all accessible areas including toilets, should be avoided as it would very likely be unjustified.

(ii) Whose biometric data should and could be collected

Strong justification is required if the biometric data of a large number of individuals are to be collected, as the potential damage caused by data breaches would be very serious.

Hence, where the collection of biometric data is to ensure only authorised entry, only the biometric data of those authorised persons should be collected.

Children of school age or individuals who are less capable of managing their own affairs are vulnerable and require stronger protection of their data privacy. Collection of biometric data from these groups, if challenged, will be critically examined by the Commissioner. In any event, it is objectionable for children of school age to be exposed to acts or practices that depreciate privacy, as 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.

(iii) The extent of the data to be collected

It is unnecessary for data users to collect extensive or complete biometric data of an individual, so long as the data collected are sufficient for their purposes. For example, in the case of fingerprint data collection, it is probably unnecessary to involve more than two fingers for an individual.

Even if only a subset of the overall biometric characteristics is used to generate a template, the number of reference points should be kept to a

minimum depending on circumstance. For example, the number of reference points a data user needs from a fingerprint to differentiate an individual from a population of 30 should be less than those needed for a population of 1,000 individuals.

5. FREE AND INFORMED CHOICE TO ALLOW COLLECTION OF ONE'S BIOMETRIC DATA

Data subjects should be provided with free and informed choice to allow the collection of their biometric data, together with a full explanation of the personal data privacy impact of the collection of such data.

Data users should inform each data subject, on or before his biometric data is to be collected[22]:

- Whether provision of the biometric data is voluntary or obligatory;
- Where provision of the biometric data is obligatory, what the consequences would be for the data subject who fails to provide the data;
- The purpose(s) for which the biometric data is to be used;
- Who may have access to the biometric data, and under what circumstances may access be gained;
- If the biometric data may be transferred to other persons, the classes of persons to whom the data may be transferred;
- Whether the biometric data could be relied upon to take adverse actions against the individual; and
- The individual's right to request access to or correction of the biometric data, and how the request should be made (name, post and contact particulars of the person who is authorised to handle the requests).

Data users who wish to collect employees' biometric data must ensure that their employees are given a free and informed choice on the supply of the data. Assuming the collection of employees' biometric data is "necessary and not excessive," such collection must be by means that is fair in the circumstances, and collection of biometric data from employees who fear to be penalised if they are unwilling or unable to do so may not be fair collection. Accordingly, the collection of biometric data covertly would require very strong justification. Furthermore, if there is inherent disparity in the 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 biometric data and be given the option to choose between giving or withholding the data. The data user should make every effort to dispel any reasonable suspicion of undue pressure imposed on the data subject.

If the data subject is given a choice to choose and does choose to allow his biometric data to be collected or processed, such choice will be respected. As such, the Commissioner will not interfere unless that the choice is not voluntary or is made under undue pressure. An individual's consent, if any, should be recorded in writing to avoid future 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 biometric data, e.g., the option of using a smartcard on its own with CCTV monitoring as an alternative to a fingerprint-based attendance system. The data user should adopt all practicable measures to protect the privacy of individuals' personal data and minimise any adverse privacy impact on the individual. Evidence of such measures having been taken will be viewed favourably by the 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 alternative to an individual.

[22] DPP1(3).

For consent to be voluntarily and expressly given, the 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 is no undue influence on the individual when the consent is sought.

6. PRIVACY REQUIREMENTS FOR DEALING WITH THE BIOMETRIC DATA COLLECTED

(i) Establish strong controls for access to, use and transfer of biometric data

Data users should not use (including disclose to a third party) an individual's biometric data for any purpose that is not related to the purpose for which it was 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[23].

Protection of personal data collected is the legal obligation of the data users throughout the life cycle of such data. The more people who have access to the biometric data, the more likely that the data will be used by unauthorised person and for an unauthorised purpose. Biometric data should therefore be allowed access only on a need-to-know basis.

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

(ii) Retention of biometric data

Data users should regularly and frequently purge biometric data which is no longer required for the purpose for which it is collected[24]. Hence, if an employee's biometric data has been collected to control access to the employer's premises or computer systems, such data should be deleted as soon as the employment is terminated.

Retaining personal data for a period beyond what is necessary would not only contravene the Ordinance, but also burden the data user in safeguarding data security and assuming unnecessary risk of a data breach.

For the purpose of research or statistics, data users who want to keep personal data collected for longer than is required may apply anonymisation to the personal data collected so that it can no longer be used to identify individuals, and therefore is not regulated under the Ordinance. Data users should, however, consider seriously the implication of possible privacy impact of de-identified biometric data and whether it is really possible to anonymise biometric. For example, DNA samples or sequences, even when they are not associated with any names, may still reveal such information as race, physical or mental disability, family relationship with one another etc. that may allow individuals to be re-identified under certain circumstances.

(iii) Ensure data accuracy

Data users are required to take all reasonably practicable steps to ensure that the personal data held is accurate[25].

---

[23] DPP3.
[24] DDP2(2) and section 26 of the Ordinance.
[25] DPP2(1).

As the biometric data collected can be used to take adverse action against the individual, accuracy of the data is of particular importance to the individual. Where an employee supplies biometric data on each working day to prove work attendance, any inaccuracy of the data collected may result in salary deduction or even termination of employment.

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

(iv) Secondary use

Data users are required not to use personal data collected for a new purpose without the express consent of the data subject[26].

Some biometric data, such as DNA and retina images, may contain rich information about an individual in terms of physical health or even mental conditions. Data users collecting such data for one purpose must ensure that it is not being used for another unrelated purpose without obtaining express consent from data subject. For example, DNA samples collected or DNA tests carried out originally for an annual body check-up as part of the medical benefit offered by the employer should not be used by the employer to determine the long-term employability of the employee in terms of health insurance liability without the employee's consent.

(v) Data security

All reasonably practicable steps shall be taken to ensure that personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to the kind of data and the harm that could result if any of those things should occur[27]. Given the sensitivity of biometric data, it is important that data users guard against any risk of compromising and thieving of the biometric database and that effective security measures are implemented as are reasonably practicable in the particular circumstances. Examples of worthy security measures are:

- The IT system which is used to store and process the biometric data should be carefully and regularly evaluated to ensure that sufficiently effective security and privacy-protective measures are in place;
- Encrypting the biometric data while it is being stored or transmitted; and
- Data access is restricted to authorised persons on a need-to-know basis and is protected by strong passwords (e.g. combination of letters, numbers and/or symbols) while all such accesses are recorded/logged.

---

[26] DPP3(1).
[27] DPP4(1).
[28] DPP5.

(vi) 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 biometric data, and make them known to all parties concerned, such as employees, contractors and/or customers. Data users should draw the specific attention of the individuals affected to such policies and procedures, and make them publicly available for review[28].

(vii) Staff training

Regular privacy compliance assessments and reviews should be conducted by the data users to ensure 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 biometric data. Employees who fail to properly carry out their duties in the handling of biometric data should be subject to appropriate disciplinary action.

(viii) Use of contractor

If contractors are engaged in the handling of personal data, data users must adopt contractual or other means to prevent personal data transferred to the contractor from being kept longer than necessary and from unauthorised or accidental access, processing, erasure, loss or use[29].

Data users should also note that they may be held liable for any personal data leakage resulted from a security or programming failure on the parts of the contractor, regardless whether such contractor is engaged in the handling of personal data held by the data user.

It is, therefore, in the best interest of data users who engage contractors to observe recommendations given in the *Outsourcing the Processing of Personal Data to Data Processors Information Leaflet*[30] published by the Commissioner, in addition to any other relevant and applicable considerations in relation to security and proper programming practice.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address: 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

[29] DPP2(3) and DPP4(2).
[30] Available at www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/dataprocessors_e.pdf.