BAKER & MCKENZIE

Client Alert

July 2015

Privacy Commissioner Cautions Against Excessive Collection and Use of Biometric Data

Comprehensive guidance on the collection and use of biometric data, such as DNA, fingerprint and facial recognition data, was released by the Office of the Privacy Commissioner of Personal Data ("**PCPD**") on 20 July 2015.

The Guidance on Collection and Use of Biometric Data ("**Guidance**") was issued in response to increasing use of such data by organisations in Hong Kong, and replaces previous guidance issued in 2012 on the collection of fingerprint data. The Guidance was released the day before publication of the PCPD's *Investigation Report: Collection of Fingerprint Data by Queenix (Asia) Limited ("**Queenix**")* ("**Investigation Report**"), in which the Privacy Commissioner served an Enforcement Notice on Queenix for excessive collection of fingerprint data.

In the Investigation Report the PCPD found on the facts that it was not absolutely necessary for Queenix to collect employee fingerprint data for the purposes of security and monitoring staff attendance. The PCPD observed Queenix should have considered the readily available alternatives, such as the use of stronger door locks / chain locks, which did not involve collection of personal data.

Why is the Guidance and Investigation Report relevant to you?

The Investigation Report makes it clear that the PCPD considers the collection of biometric data to be a serious issue and unnecessary or excessive collection of such data will not be tolerated. Both the Guidance and the Investigation Report stress the importance of carrying out a Privacy Impact Assessment ("**PIA**") before deciding to collect biometric data. In particular, clients should:

- have strong justification for collecting biometric data;
- ensure that free and informed consent is obtained prior to collection;
- adopt risk minimisation techniques and implement strong controls to protect the data once collected; and
- where possible, use less privacy intrusive alternatives than collecting biometric data.

The Guidance clarifies the PCPD's position with respect to biometric data and what it considers to be acceptable use and practice of such data. The PCPD's recommendations are summarised below.

Hong Kong

14th Floor, Hutchison House
10 Harcourt Road
Central, Hong Kong

Tel: +852 2846 1888
Fax: +852 2845 0476

Beijing

Suite 3401, China World Office 2
China World Trade Centre
1 Jianguomenwai Dajie
Beijing 100004, PRC

Tel: +86 10 6535 3800
Fax: +86 10 6505 2309

Shanghai

Unit 1601, Jin Mao Tower
88 Century Avenue, Pudong
Shanghai 200121, PRC

Tel: +86 21 6105 8558
Fax: +86 21 5047 0020

What is biometric data?

There are two types: ***Physiological Data*** and ***Behavioural Data.***

	Characteristics	Examples
Physiological Data	Born with the data. Doesn't change.	DNA samples, fingerprints, palm veins, hand geometry, iris, retina, facial images.
Behavioural Data	Developed after birth. Prone to changes, consciously or unconsciously.	Handwriting patterns, typing rhythm, gait and voice patterns.

While it may not be reasonably practical for a lay person to ascertain the identity of an individual from such data alone, **when biometric data is linked with personal data in another database, an individual/data subject can be identified**. Therefore this data is considered "personal data".

Should organisations collect biometric data?

The appropriateness of collection varies with the level of sensitivity of the biometric data concerned. The PCPD encourages data users to consider the sensitive nature of the data concerned, i.e.:

	DNA	Facial images	Palm shape	Handwriting Pattern
1. Uniqueness	High	Medium	Low	Low
2. Any likely changes with time?	No	Yes	Yes	Yes
3. Multiple purposes of usage	Yes	No	No	No
4. Capable of being collected covertly	Yes	Yes	No	Unlikely
5. Impact to individual when leaked/revealed?	Grave. A person cannot change their DNA	Possibly some	Not so grave	Possibly some

Conduct a Privacy Impact Assessment

To determine whether collection is necessary and not excessive, the PCPD recommends conducting a PIA, which documents consideration of the following:

(a) **What is the *need* for collecting biometric data.** Is there is a working system already in place, and does it really need to be upgraded? If

an organisation considers that biometric data is required, is there a less intrusive verification system available? The Guidance gives the following examples:

✘ **Using biometric data to record attendance:** unlikely to satisfy the need and required "overriding reasons to justify the collection of biometric data".

? **Using biometric data for security controls:** biometric data collection may not always be the most appropriate choice. Security can be improved by other less privacy-intrusive methods, such as through a combination of CCTV and passwords. The Investigation Report suggested that stronger door locks/chain locks were more effective for ensuring security than a fingerprint lock.

(b) **Whose biometric data should and could be collected.** Strong justification is required if collecting the biometric data of a large number of individuals due to the potential risk of data breaches. Collection of biometric data from children and other vulnerable members of society is strongly discouraged.

(c) **The extent of data to be collected.** It is unnecessary to collect extensive or complete biometric data. For example, in the case of fingerprint data, only data from two fingers would be sufficient.

Considerations when collecting personal data

- **If data is collected, keep it in "template" form.** A template is numeric information which describes relevant features of the biometric data. Templates pose a lower privacy risk because they contain fewer details and offer little secondary use compared to an original image. Data users should, as soon as possible, derive biometric data templates from original biometric data samples for storage and subsequent use, and discard the original samples/ images safely afterwards. The templates should be stored in such a way so that it is technically infeasible or difficult to convert back to the original image.
- **Data collected should be for a lawful purpose related directly to its function and activity.** Examples include a collection of: DNA by law enforcement agencies for investigation of a crime; facial images by the Immigration Department for immigration control; and fingerprints by employers for control/restriction of access to high security locations by authorised personnel.
- **Must be *necessary* and not excessive.** In the event an organisation *does* deem it appropriate to collect such personal data, the PCPD encourages organisations to consider whether it is feasible to collect less sensitive biometric data to achieve the same purpose without compromising on effectiveness.

In the Guidance, the PCPD gives the example of ***identification data*** versus ***verification data*****.** Identifying an individual using facial recognition data, for example, requires the collection and storage of much more information

and running that individual's data against a large database sample, rather than mere identification which only requires a few reference points.

Risk Minimisation: Examples of acceptable uses of biometric data collection where there is a genuine need

The PCPD gives two examples of biometric data collection which reduce the risks associated with disclosure: the use of ***smartcards*** for storing biometric data and ***biometric encryption***.

Smartcards for security access which store fingerprint data into templates, and are then used in conjunction with a verification system, would reduce the risk of collection of biometric data (so long as the employer does not hold, or have access to, the fingerprint data apart from at time of comparison), as data is encrypted and nothing on the smartcard would reveal the identity of the holder to a third party.

Collecting consent to use of biometric data

Data subjects should be provided with a **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.

The PCPD offers guidance on the type of information to be provided:

- 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).

In the case of employees who fear being penalised if they are unwilling or unable to consent to biometric data collection, this will not be considered "fair" collection.

In addition, a data user should, as far as practicable, provide each individual with a free choice of a less privacy- intrusive alternative to the collection of his biometric data e.g. using a smartcard with CCTV monitoring as an alternative to fingerprint based attendance system. In the Investigation Report, the PCPD states that informed consent could only be made if Queenix's employees had the choice to opt for other alternatives (which they did not).

www.bakermckenzie.com

To find out more about how our Privacy and Data Protection Group can add value to your business, please contact:

Anna Gamvros
+852 2846 2137
anna.gamvros@bakermckenzie.com

Susan Kendall
+852 2846 2411
susan.kendall@bakermckenzie.com

Paolo Sbuttoni
+852 2846 1521
paolo.sbuttoni@bakermckenzie.com

Requirements for the handling of biometric data

Finally, the Guidance sets out the requirements for the handling of personal data.

1. **Establish strong controls for access to, use and transfer of biometric data.** Data users should not use or disclose biometric data for any purpose other than the purpose of collection without data subject consent. Written policy and clear guidance should be devised to ensure proper use and prevent unnecessary linkage between biometric databases with other systems, transfer or change of the data.
2. **Retention of biometric data.** Data users should regularly and frequently purge biometric data no longer required for the purpose for which it is collected, e.g. as soon as an employee's contract is terminated. For data that is de-identified for research or statistics, consider whether it is really possible to anonymise the data.
3. **Ensure data accuracy.** Data users are required to take all reasonably practicable steps to ensure data is accurate. Data users must ascertain and accept that false acceptable rates are within reasonable limits.
4. **Secondary use**. Data users may not use personal data for a new purpose except with consent.
5. **Data security**. All reasonably practicable steps should be taken to ensure the biometric data is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to the kind of data and harm that could result. Examples of worthy security measures include encryption and data access restricted to a "need to know" basis and strong password protection.
6. **Make policies available**. Data users should devise policies and procedures setting out clearly the rules and practices in collection, holding, processing and use of biometric data and make them available to data subjects.
7. **Staff training**. Regular compliance assessments and reviews, as well as proper training, guidance and supervision, should be taken.
8. **Use of contractors**. If contractors are engaged, data users must adopt contractual or other means to prevent the contractor keeping the data longer than necessary and protection from unauthorised or accidental access, processing, erasure, loss or use.