**Overview**

The *Guidance Note on Collection and Use of Biometric Data* (Guidance), published on 20 July 2015, sets out comprehensive advice to organisations considering implementing increasingly cheap and available biometric technologies. There would appear to be a rebuttable presumption that all biometric data will be considered to be personal data even if a lay person cannot immediately identify the individual. It is also apparent that the Office of the Privacy Commissioner for Personal Data (PCPD) views biometric data to be highly “sensitive” personal data and (even though not distinguished in the *Personal Data (Privacy) Ordinance (Cap 486)* (PDPO)) expects it to be treated in accordance with strict controls. The key message is that organisations should not blindly implement, for example, fingerprint recognition devices without assessing the privacy risks and justifications, considering less privacy-intrusive measures, or offering individuals a free and informed choice and appropriate controls. Overall, and unlike other guidance notes, the Guidance should really be seen not just as best practice but minimum compliance standards for organisations handling biometric data.

**Background: “sensitive data”**

The protection of biometric data is an issue that the PCPD has advocated for several years. The PDPO is unusual in not distinguishing sensitive personal data. Despite strong support from the PCPD, and draft proposals in the public consultation document, to include additional protections for biometric data and more generally sensitive personal data, these were not taken up when the PDPO was amended in 2012. By publishing the Guidance, the PCPD is returning to this topic and taking the opportunity to promote the (strict) standards it expects organisations to meet when handling what it describes as “sensitive data”.

The Guidance also follows recent enforcement action against a company who used a fingerprint recognition device for security and staff monitoring purposes in breach of the PDPO. Although the PCPD has investigated similar issues in the past, the PCPD describes this latest case as a “vivid example of preferring the convenience and affordability of such
devices to the neglect of the underlying privacy concerns”.

The Guidance replaces the PCPD’s previous guidance on the collection of fingerprint data, and updates and extends it to other forms of biometric data, such as DNA and facial images.

**Biometric data: personal data**

The Guidance describes biometric data as including both:

- physiological data with which individuals are born, and so generally cannot be changed by the individual, such as DNA samples, fingerprints, IRIS scans and facial images, and
- behavioural data developed since birth, such as handwriting and voice patterns, which may consciously or sub-consciously be changed by the individual.

The Guidance would appear to introduce a rebuttable presumption that all biometric data – whether stored as full images or as numerical codes or other representations based only on some features of the biometric data - will be considered by the PCPD to be personal data even if a lay person cannot immediately identify the individual. In effect, it would appear that it will be for a data user to demonstrate that it has no access to any other personal identification particulars (for example, in another database) of the relevant individuals in order to persuade the PCPD that the biometric data is effectively anonymised such that they are not data users of the biometric data. However, this may be difficult in practice given that the Guidance states that: “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”.

**Caution and strict controls**

1. **Assess the sensitivity of the biometric data**

The Guidance emphasises the general need for caution when handling biometric data, but advises that the data user’s approach should vary depending on the sensitivity and format of the biometric data in question. The Guidance emphasises that other considerations, such as the cost and availability of biometric data readers, should not be an organisation’s prime concern.

In terms of assessing sensitivity, relevant factors include: uniqueness of the data; likelihood of the data changing over time; whether the data could be used for multiple purposes; possibility of covert collection; and impact of a data leak. The Guidance indicates that DNA data is likely to have the highest sensitivity, with handwriting patterns likely to be considered at the opposite end of the risk spectrum.

Biometric data should at the earliest opportunity be converted from its original image into a template (e.g., a numeric representation or equivalent), and the template should be "stored in a form from which it is technically infeasible or difficult to convert back to the original graphical image”.

2. **Assess whether the collection of biometric data is necessary and justified**

An organisation must ensure that its proposed collection and use of biometric data is fair, lawful and necessary under the first Data Protection Principle (DPP). In particular:

- the collection of the biometric data must be for a lawful purpose related to the organisation’s function and activity. Examples cited in the Guidance include collection of facial images by immigration authorities for immigration
control; and collection of fingerprints by employers to control access to high security/restricted areas, and
- the collection must be “necessary and not excessive” for achieving this purpose.

Organisations are advised to conduct and document a Privacy Impact Assessment (PIA). Organisations are advised to
balance the need for biometric data collection against the possibility of using alternative non-biometric or less intrusive
biometric systems or collecting less sensitive biometric data.

If the need for collecting biometric data is established and justifiable, detailed consideration should be given as part
of the PIA to whose biometric data should and could be collected, and the extent of the data needed. In the PCPD’s view,
strong justification would be needed to collect extensive or complete biometric data; to collect biometric data from a
large number of individuals, or from children and other vulnerable individuals; or for covert collection. The Guidance
further advises that indiscriminate and continuous use of biometric scanners, such as fingerprint access to areas such
as bathrooms or pantries, is unlikely to be justifiable.

3. Ensure individuals are given a free and informed choice

Data subjects must be given a free and informed choice to allow their biometric data to be collected, and in practice
must be able to demonstrate that to the PCPD if a complaint were made.

In practice this means that, in addition to the usual information required to be notified in a personal information collection
statement (PICS) under DPP1(3), a PICS concerning biometric data must also fully explain the personal data privacy
impact of the collection of their biometric data, including informing individuals of whether the biometric data could be
used to take adverse actions against them. In addition:

- To ensure fair collection and avoid the inference of undue influence on an individual, especially where there is an
  inherent disparity of bargaining power between the collecting organisation and the individual, such as an employer-
  employee relationship, organisations should take steps to ensure individuals are given the option of giving or
  withholding their biometric data without fear of being penalised.
- As far as practicable, a less privacy-intrusive option should be offered as an alternative to the collection of
  biometric data. The PCPD will not generally consider inconvenience to be an acceptable reason for not offering
  such an alternative.
- Businesses must ensure that an individual has the requisite mental capacity to understand the potentially adverse
  privacy risks of the collection.

4. Adopting risk minimisation techniques

Organisations are urged to adopt measures to minimise the privacy impact to individuals when handling their personal
data, for example: using biometric encryption; or storing encrypted template biometric data in a smartcard (without other
identifying data) held by the individual rather than in a central system.

5. Comply with the Data Protection Principles

Organisations are also reminded to comply with the remaining DPPs when handling biometric data, in particular data
users must:

- DPP2(1): take all reasonably practicable steps to ensure the accuracy of the biometric data held in light of the
  potential harm. Possible safeguards include: identifying false acceptance/rejection rates of a proposed biometric
  system; and allowing individuals to explain an irregularity before taking action against them
• **DPP2(2):** implement retention policies and procedures for biometric data for the organisation and its contractors, including regular and frequent purges of biometric data that is no longer required. Guidance is given on anonymising biometric data to enable further research or statistical use but, as noted above, this may be difficult in practice.
• **DPP3:** obtain explicit and voluntary consent from an individual to any secondary use of their biometric data.
• **DPP4:** implement effective security measures appropriate to the biometric data processing in question and potential harm. This should include technological measures (such as updating IT security, and implementing access controls, system separation and encryption) as well as operational measures (such as restricting physical access only to those on a need to know basis) and contractual measures (particularly if third party contractors may need access to the data), and
• **DPP5:** implement and publicise clear privacy policies and procedures in relation to biometric data, and require staff to - and train them on how to - comply with them.

### Conclusion: minimum compliance standards

The Guidance, although not legally binding, gives a very clear message to organisations that the PCPD expects organisations to exercise “extreme caution” when collecting, using and retaining biometric data. Unlike other guidance notes, the Guidance should really be seen not just as best practice but minimum compliance standards. Therefore, organisations are strongly advised to assess and document their reasoning when implementing biometric data technologies as to why it is necessary and proportionate, why less privacy-intrusive alternatives are not available, and the controls implemented to minimise the privacy risks. Otherwise it is likely that they may find it difficult to justify the scheme to the Privacy Commissioner if a complaint is made.

Although the examples in the Guidance are largely concerned with the use of biometric data by employers for identification and verification purposes, those collecting and using biometric data for other purposes – such as medical research, life sciences and connected healthcare businesses – are also strongly advised to take note of the PCPD’s advice.

The Guidance is available on the PCPD’s website: click [here](#).

---

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document.