Biometrics in the workplace.

The following guidance has been prepared as an aid to those employers seeking to use a biometric system in the workplace. The document is intended to encourage employers to consider the need for a system and then to assess the privacy impact of different systems. The document is not intended to promote any particular system, but is intended to make employers aware of their responsibilities under the Data Protection Acts 1988 & 2003. It is the use of a system by an employer that may be a data protection concern, not necessarily the production or sale of a system. All situations must be judged on a case-by-case basis.

1. Different types of Biometric systems

All biometric systems operate on the basis of the automatic identification or authentication/verification of a person. What differs between systems is the nature of the biometric and the type of storage.

1.1 Information used to generate biometric data

Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, outline of a hand, an ear shape, voice pattern, DNA, and body odour. Biometric data might also be created from behavioural data such as hand writing or keystroke analysis. Generally, a digitised template is produced from the biometric data. This template is then compared with one produced when an employee presents at a reader.

1.2 Types of biometric data.

There are three principal types of biometric data

- Raw Images, consisting of recognisable data such as an image of a face or a fingerprint, etc.
- Encrypted images, consisting of data that can be used to generate an image.
- Encrypted partial data, consisting of partial data from an image, which is encrypted and cannot be used to recreate the complete original image.

1.3 Types of Biometrics systems

There are two principal types of systems

- Identification systems, which confirm the identity of an individual;
- Authentication / verification systems, which confirm that a biometric derived from a person who presents at a reader matches another biometric, typically stored on a card and presented simultaneously.

1.4 Storage of biometric data.

There are two principal methods of storing biometric data/templates

- Central databases store the templates on a central system which is then searched each time a person presents at a reader.
- A card is used to store a template. A template is generated when a person presents at a reader, and this template is compared with the template on the card.

2. Data Protection issues concerning biometrics.

2.1 Proportionality

Section 2(1)(c)(iii) states that data

"shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed."

The key word here is "excessive". Is there a need for a particular system? What is wrong with current systems or less invasive alternatives? As employees have fundamental Human Rights which are protected by the Data Protection Acts, an employer must conduct some assessment of the need for a system and evaluation of the different types of system before introduction.

Determining what is excessive requires a case-by-case analysis. Some factors which may be taken into account include:

- **Environment.** The nature of the workplace may require high levels of security. Areas containing sensitive information, high value goods or potentially dangerous material may warrant a higher level of security than would areas with low value goods or areas with complete public access.
- **Purpose**. Can the intended purpose be achieved in a less intrusive way? A system used to control access for security purposes might be more legitimate than a system used by the same employer purely for time management purposes.
- **Efficiency.** Ease of administration may necessitate the introduction of a system where other less invasive systems have failed, or proved to be prohibitively expensive to run.
- **Reliability**. If a employer suffers as a result of untrustworthy staff, impersonating each other for various reasons, then a system may be justified as long as other less invasive ones have been assessed and reasonably rejected.

3. Fair obtaining and processing.

Section 2(1)(a) of the Acts require that

"The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly".

In order to demonstrate compliance with this provision, at least one of the provisions of Section 2A of the Acts must be met. These include

- Employee consent,
- Where the performance is necessary for the performance of a contract to which the data subject is parity,
- For compliance with a legal obligation to which the employer is subject,
- Where the processing is necessary for the purposes of the legitimate interests pursued by the employer or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Consent is not generally a satisfactory legitimiser in an employment context, as it can be argued that consent is not freely given. However, if an employer offers a biometric as an option, then consent may be seen to be freely given.

Whilst the "legitimate interest" provision may seem appealing, it requires that a balance be struck. What is acceptable in one case may not be in another and an employer seeking to rely upon this provision must take into account the potential effect upon employee privacy rights.

3.1 Fair obtaining of sensitive data.

If a biometric identifies sensitive data (such as data relating to an employee's health), at least one provision of section 2B of the Acts must be met in addition to those mentioned above. These provisions include

- The explicit consent of employees.
- Where the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the employer in connection with employment.
- Where the processing is necessary for the purposes of establishing, exercising or defending legal rights.

As before, consent is difficult to rely upon in an employment context.

Any legal obligation to be aware of the presence of employees need not, in itself, require a biometric system to satisfy. A similar case would apply to employers who seek to justify a system as necessary to defend their own rights. The key word with both these provisions is "necessary".

4. Transparency

Section 2D of the Acts require that an employer provide at least the following information to employees when processing their data:

- The identity of the employer.
- The purpose in processing data.
- Any third party to whom the biometric data will given.

Identity is generally obvious and disclosure will typically only be an issue if another company administers, maintains or manages the system. But disclosure would include sending data to a parent company.

It is essential that employees are aware of the purpose for which the biometrics data will be processed. This means that an employer must carefully think through any purpose or potential purpose. Is the system solely for access control? Will it be used for time management? What are the consequences for the employee concerned if there is an identified abuse of the system? Under what circumstances will management access logs created by the system?

Transparency is even more important where the biometric system does not require the knowledge or active participation of an employee. A facial recognition system, for instance, may capture and compare images without that person's knowledge.

5. Accuracy

Section 2(1)(b) of the Acts require that data shall be

"Accurate and complete and, where necessary, kept up to date".

Any biometric system must accurately identify the persons whose data are processed by the system. If changes in physical or physiological characteristics may result in a template becoming outdated, some procedure must be put in place to ensure that the data are kept up to date.

6. Security

The requirement, under section 2(1)(d), that an employer has appropriate security measures in place to prevent the unauthorised access to, or the unauthorised alteration, disclosure or destruction of data would appear to promote the use of technological solutions such as biometrics.

However, in deciding upon what constitutes an appropriate security measure, Section 2C details four factors that should be taken into account:

- The availability of technology.
- The cost of implementing such technology.
- The nature of the data being protected.
- The harm that might result through the unlawful processing of such data.

This nature of the data and the harm caused through unlawful processing must be carefully considered. For example, patient medical records should expect to be held in a more secure environment than would a fast food company's customer database.

7. Privacy Impact Assessment.

The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is used. A case-by-case judgement is required. With that in mind, the Commissioner encourages employers to take the above guidance into consideration before introducing any biometric system.

Before an employer installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. An

employer who properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against an employer by the Commissioner, or may expose an employer to a claim for damages from an employee. Data protection responsibility and liability rests with the employer, not with the person who has supplied the system (except where that person also acts as a data processor on behalf of the employer).

Some of the points that might be included in a Privacy Impact Assessment are:

- Do I have a time management and/or access control system in place?
- Why do I feel I need to replace it?
- What problems are there with the system?
- Are these problems a result of poor administration of the system or an inherent design problem?
- Have I examined a number of types of system that are available?
- Will the non-biometric systems perform the required tasks adequately?
- Do I need a biometric system?
- If so, why kind do I need?
- Do I need a system that identifies employees as opposed to a verification system?
- Do I need a central database?
- If so, what is wrong with a system that does not use a central database?
- What is the biometric system required to achieve for me?
- Is it for time management purposes and/or for access control purposes?
- How accurate shall the data be?
- What procedures are used to ensure accuracy of data?
- Will the data require updating?
- How will the information on it be secured?
- Who shall have access to the data or to logs?
- Why, when and how shall such access be permitted?
- What constitutes an abuse of the system by an employee?
- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring employees to participate?
- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- How shall I inform employees about the system?
- What information about the system need I provide to employees?
- Would I be happy if I was an employee asked to use such a system?