The use of biometric devices at the workplace

Biometrics is the science and technology of uniquely identifying human subjects by means of measuring and analysing one or more intrinsic physical or behavioural traits. These human body characteristics may include fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements.

Biometric systems include applications making use of biometric technologies and which allow the automatic identification, verification or authentication of a natural person. The increase in the deployment of biometric systems at workplaces, mainly for attendance and access control purposes, has raised privacy concerns especially at a European level and has been the subject of laborious discussions.

In principle, the processing of personal data involving the use of a biometric system is considered by privacy experts to be only justified in places demanding a high level of security and strict identification procedures. Generally, the use of biometrics solely for the purposes of attendance and salary computation is considered to be excessive and therefore unreasonable, particularly if the employer may accomplish the same objectives by resorting to less intrusive methods, for example electronic tags. Deploying these systems for the sake of keeping up with technology and merely for the purpose of convenience is not deemed to be consistent with the privacy agenda.

Prior to implementing a biometric system, employers are advised to carry out a proper privacy impact assessment in order to ensure that the use of biometrics is essentially necessary. The principles of finality and proportionality, key terminology in the data protection dictionary, should be factored in the assessment so as to ascertain that the introduction of such system is indispensable.

Since the use of biometric systems involves processing of personal data, the operation should be notified to the Data Protection Commissioner. In these cases, being a process which may involve particular risks to the privacy of individuals and which requires a case-by-case evaluation by the Commissioner, a notification for prior checking should be submitted.

The implementation of similar systems should occur in a transparent manner and therefore appropriate information should always be provided to employees. Where employees are unionised, there should be prior and proper consultation with the respective union.

Where the introduction of biometric systems is deemed necessary, employers should opt for that system which provides a high level of comfort in terms of the privacy requirements. This is possible in view of the technological progress achieved in this field. These systems include those which do not physically record and process the actual image of the biometric feature, such as the fingerprint. During the enrolment phase, the data is immediately converted into a template containing a unique binary code which represents the characteristics or measurements of the biometric feature. This binary code is normally encrypted and kept in a separate storage space, for instance, in the memory of the biometric device. In this way the biometric data is segregated from other personal information conventionally stored in a back-end database and kept for administrative purposes.

For instance, every time the person makes use of the biometric device to enter or exit the work premises, the system will convert the fingerprint data to a binary code and match the code with the one previously stored during the enrolment phase to authenticate the individual. A unique reference number, such as a pin code or index number, which is uniquely assigned to every person, is usually used to link the template data with the other details stored in the back-end database. This matching process will enable the identification of the individual without actually processing his or her fingerprint.
The employer must ensure that a fall-back procedure is always in place for those individuals who, for a valid reason, are not eligible for enrolment under the biometric system.

Employers are advised to adopt privacy-friendly systems, where the storage of data containing biometric elements is retained on the chip or on the card itself. This practice ensures that the data is retained by the individual and the authentication process is carried out by means of a one-to-one match. This approach is consonant with the practice adopted by the European Data Protection Supervisor.

Where the employer engages the services of another organisation for the management of the biometric system, the relationship must be governed by means of a written agreement which will bind the managing organisation to solely act upon the instructions of the employer and implement all the required security measures to protect the personal data against any unlawful form of processing.