A complaint was lodged on 9th August 2013 at the Data Protection Office under section 11 of the Data Protection Act(DPA) against Respondent by Complainant with regard to her dismissal as she refused to provide her fingerprint for the recording of attendance.

My office opened an inquiry and informed Respondent ,in writing, of the steps to follow in compliance with the DPA before processing Complainant's fingerprint.

Whilst this office has no jurisdiction to entertain issues outside data protection and will not assess whether the dismissal was justified or not, the issue of dismissal is directly linked to the intended processing without consent of personal information, i.e, fingerprints which are used to identify employees.

The Data Protection Commissioner has decided as follows:-

Recalling my decision of 17.7.2013 against another company currently under appeal at the ICT Tribunal and based upon ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 3/2012 on developments in biometric technologies which represents the applicable doctrine at page 3, first para., where it was stated as follows:-

"*Biometric technologies that once needed significant financial or computational resources have become dramatically cheaper and faster. The use of fingerprint readers is now commonplace. (...) Biometric technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition many of them allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through*

the growing deployment of these technologies. Every individual is likely to be enrolled in one or several biometric systems.

At page 6, para.4,:-

"Accuracy: When biometric systems are used it is difficult to produce 100% error-free results. This may be due to differences in the environment at data acquisition (lighting, temperature, etc.) and differences in the equipment used (cameras, scanning devices, etc.).

At page 8, paras.1 & 2,:-

Proportionality

The use of biometrics raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. As biometric data may only be used if adequate, relevant and not excessive, it implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way.

In analysing the proportionality of a proposed biometric system a prior consideration is whether the system is necessary to meet the identified need, i.e. is essential for satisfying that need rather than being the most convenient or cost effective. A second factor to take into consideration is whether the system is likely to be effective in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used. A third aspect to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate. The fourth aspect in assessing the adequacy of a biometric system is to consider whether a less privacy intrusive means could achieve the desired end 2. (...) 2 For example, smart cards or other methods that do not collect or centralize biometric information for authentication purposes.

At page 20-21 last para.,:-

"There are data protection concerns associated with the use of fingerprints that can be briefly described as follows:

Accuracy: Even though fingerprints eventually present a high accuracy rate, this can be challenged due to limitations related to the information -low quality of the data or non-consistent acquisition process – or representation - features selected or quality of the extraction algorithms –issues. This can lead to false rejection or false matches.

Impact: The irreversibility of the process can reduce the possibility of the individual of exercising their rights or to reverse decisions adopted based on a false identification.

The reliance on the accuracy of fingerprinting can make possible mistakes harder to rectify, leading to far reaching consequences for individuals. This needs to be taken into account when the proportionality of the processing in relation to the specific decision to be taken based on the fingerprints is assessed. It should be also mentioned that lack of security measures can lead to identity theft that can have a strong impact for the individual.

Linkability: fingerprints provide potential for misuse as the data can be linked with other databases. This possibility of linking up to other databases can lead to uses non compatible with the original purposes. There are some techniques, like convertible biometrics or biometric encryption that can be used to reduce the risk.

Processing of sensitive data: According to some studies, fingerprint images can reveal ethnical information of the individual.

Further purposes or purposes of processing: Central storage of data, especially on large databases, implies risks associated with data security, linkability and function creep. This allows, in absence of safeguards, the use of the fingerprints for purposes different than those that initially justified the processing.

Consent & Transparency: Consent is a core issue in the use of fingerprints for uses other than in law enforcement. Fingerprints can be easily copied from latent prints and even photographs without the individual's knowledge. Other issues concerning consent are those related to (...) the validity of consent for providing fingerprints in a labour context.

Revocability: fingerprint data are very stable with time and should be considered irrevocable. A fingerprint template may be revoked under certain conditions.

Anti-spoofing protection: fingerprints can be easily collected because of the multiple tracks of fingerprints an individual leaves behind. Moreover, false fingerprints can be used with many systems and sensors, especially when such systems do not include specific anti-spoofing protection. The success of an attack depends largely on the type of sensor (optical, capacitive, etc.) and the material used by the attacker.

At page 12, para. 2:-

Processing of biometric data can be necessary for the performance of a contract to which the data subject is party or can be necessary in order to take steps at the request of the data subject prior to entering into a contract. It has however to be noted that this applies in general only when pure biometric services are provided. This legal basis cannot be used to legitimate a secondary service that consists in enrolling a person into a biometric system. If such a service can be separated from the main service, the contract for the main service cannot legitimate the processing of biometric data. Personal data are not goods that can be asked for in exchange of a service, therefore contracts that foresee that or contracts that offer a service only under the condition that someone consents to the processing of his biometric data for another service cannot serve as legal basis for that processing"

- it is clear from the paragraph above that the performance of the main contract of employment cannot be used as a legal ground to justify the collection of fingerprints in the absence of valid consent, especially in an employment context as referred above where the imbalance between the powers of the employer and the employee is obvious. Forcing the service of biometric data collection on the employee which is a separate requirement from the performance of the contract of employment cannot be deemed justified in the absence of valid consent. It is also clear from the above paragraph that even though a contract of employment stipulates clearly that the processing of fingerprints is compulsory for all employees to perform the duties under the contract, this is not justified. A contract of employment cannot be stretched to such an extent as to justify the necessity of fingerprints for attendance purposes in a democratic society.

In S. AND MARPER v. THE UNITED KINGDOM ECHR GRAND CHAMBER 4 December 2008:- *it was held that that the indefinite retention of fingerprints by the police under the UK Police and Criminal Evidence Act (PACE) was done in violation of Article 8 of the European Convention on Human Rights:-*

At para. 66. The Court notes that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III, and Y.F. v. Turkey, no. 24209/94, § 33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person's physical and social identity (see Mikulić v. Croatia, no. 53176/99, § 53, ECHR 2002-I). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other

authorities, Bensaid v. the United Kingdom, no. 44599/98, § 47, ECHR 2001-I with further references, and Peck v. the United Kingdom, no. 44647/98, § 57, ECHR 2003-I). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see, mutatis mutandis, Burghartz v. Switzerland, 22 February 1994, § 24, Series A no. 280-B, and Ünal Tekeli v. Turkey, no. 29865/96, § 42, ECHR 2004-X). Information about the person's health is an important element of private life (see Z v. Finland, 25 February 1997, § 71, Reports of Judgments and Decisions 1997-I). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see, in particular, Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects, in addition, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz, cited above, opinion of the Commission, p. 37, § 47, and Friedl v. Austria, 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). The concept of private life moreover includes elements relating to a person's right to their image (see Sciacca v. Italy, no. 50774/99, § 29, ECHR 2005-I).

67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see Amann v. Switzerland [GC], no. 27798/95, § 69, ECHR 2000-II). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the

nature of the records, the way in which these records are used and processed and the results that may be obtained (see, mutatis mutandis, Friedl, cited above, §§ 49-51, and Peck, cited above, § 59).

68. The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. (...)

85. The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.

101. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient".

103:-"The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention (see, mutatis mutandis, Z v. Finland…). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention and the

Preamble …). The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention) (…)"

For the sake of clarity, I have decided to reproduce the relevant parts of the opinion and the case above verbatim such that there is no misinterpretation of the reasoning applied.

The *Marper* case confirms the protection of personal data as part of the fundamental human right to privacy and the term "privacy" is also present in article 22 of our civil code and the DPA is the law protecting this fundamental human right. This case illustrates the importance of respecting human rights' principles whilst processing fingerprints by the police, inter alia, the state. Therefore private employers cannot enjoy a lesser duty or privilege towards fingerprint processing of employees in the name of monitoring attendance and claim that this interference with the fundamental right to privacy is reasonably justifiable in our democratic society as interpreted in *Marper* or possibly found to be justified for the execution of the essence of a contract of employment which concerns the performance of essential duties and functions. The test as shown above is a stringent one.

In view of the fact that there are three main risks associated with the use of fingerprints namely identity fraud, purpose diversion and data breach occurrence, the random use of fingerprints cannot be allowed and prosecution is advised against Respondent for breach of sections 24 or 25 and 61 of the DPA based upon the evidence before me which establish beyond reasonable doubt that Complainant was justified in not providing her consent to Respondent for the processing of her personal information which was also the reason for her dismissal. Fingerprints may be classified as personal data and/or sensitive

personal data in compliance with section 2 of the DPA depending on the information they might generate on the person identified.

The matter will be referred to the Police under section 20 of the DPA subject to the same issue currently under appeal being thrashed out before the ICT Tribunal and if required subsequently by the Supreme Court.

Mrs Drudeisha Madhub

Data Protection Commissioner

Data Protection Office

Prime Minister's Office

4th floor, Emmanuel Anquetil Building, Port Louis

16.05.14.