澳 門 特 別 行 政 區 政 府
Governo da Região Administrativa Especial de Macau
個 人 資 料 保 護 辦 公 室
Gabinete para a Protecção de Dados Pessoais

Unofficial Translation

On using facial identification attendance control systems

7 September 2009

(Note: This document is for public reference; it contains excerpts from the Office's written responses to enquiries about using facial identification attendance control systems.)

Regarding the issue of using facial identification attendance control systems raised in several enquires, this Office holds the following opinions:

First, it should be clarified that, while the law does not prohibit employer institutions from using biometric attendance devices for attendance control purposes, the use of the said equipment involves processing of personal data; therefore, the use is subject to the provisions of the *Personal Data Protection Act*. Employers must handle employees' personal data in compliance with the law for their data processing to be legal. They should observe the principle of good faith, of respecting personal data privacy, of refraining from data processing for purposes other than that for which the data are collected, of keeping personal data no longer than their purposes require, of security and confidentiality of data, etc.

This Office has prepared and made available to the public a guide entitled *Issues Relating to Using Fingerprint / Hand Geometry Devices to Check on Work Attendanc*, and has answered citizens' enquires about the use of various biometric devices. These documents are available for download at www.gpdp.gov.mo.

Judging by the characteristics of various devices and the nature of the biometric data involved, this Office holds that fingerprint or hand-geometry attendance devices are of a type that intrudes relatively less on the rights and interests of the persons whose data are concerned. In contrast, while facial data collected with facial identification attendance control systems may be used in passive data collection, facial data tend to lend themselves to uses unknown to the data subject. Therefore, facial identification devices have greater potential impact on people. In addition,

facial data tend to be more indicative of such data as gender and race, within which the racial or ethnic origin is sensitive data. Therefore, personal data processing involving facial data affects people's rights and interests and privacy to a greater extent.

In general, the legality of an employer using biometric identification attendance devices to collect and process employees' data depends on one of the following three reasons:

1. The unambiguous consent of the employees;
2. The definitive provisions of an employment contract (refer to Item (1) of Article 6 of the *Personal Data Protection Act*);
3. In certain special circumstance. the ability of employers to prove that their legal rights and interests have a priority over the rights, freedom and guarantees of the employees (refer to Item (5) of Article 6 of the *Personal Data Protection Act*).

Under the circumstances listed in the above order, as the data subject, the employees involved have decreasing control over their personal data, with increasing intrusion on employee privacy.

Take the circumstance in which the employers claim data processing legitimacy because of "employees' explicit consent". The employees have the maximum autonomy in that they can at anytime withdraw whatever consent they have given. Once the employees disagree or withdraw their consent, the employers will have no legality whatsoever in processing the employees' data, and will have to turn to other reasonable means of attendance control. Under the third circumstance, however, the employees in general are in no position to effectively oppose the processing of their data, unless they are able to offer substantial and indisputable argument or proof that their individual rights, interests, freedom and guarantee take the precedence of that of the employer.

According to the principle of proportionality, employers must have legitimate reasons to adopt a data collecting approach that is more intruding on their employees' privacy; failing that requirement, employers should opt for approaches that would affect employee privacy to a lesser extent.

This Office thinks that where facial data are used only for attendance purposes, breach of the principle of proportionality is likely to happen. However, it is not necessarily. For example, it is legitimate for an institution to adopt the use facial identification attendance control systems because its employees "unambiguously consent to it". The employees may choose to agree, they may as well disagree. If they

disagree, and the employer institution can provide other appropriate attendance devices, then it is still proportionate. Take a health-care institution for another example. While it is legitimate for the institution to use biometric attendance devices on account of "express provisions in the employment contracts", it is nonetheless reasonable if it takes the nature of its operations into account and decides to avoid using fingerprint /hand-geometry devices, in despite of the fact that these devices are less intruding on personal privacy and rights, in order to prevent their potentially negative health ramifications. That is also proportionate.

Therefore, when deciding whether to use facial identification attendance control systems, an employer institution should at least consider the following requirements:

1. Legitimacy: the criteria for making data processing legitimate;
2. Proportionality: Whether it is possible to adopt a processing approach that is less intruding on the privacy and rights of the data subject.

In view of the fact that facial identification attendance control systems affect privacy, rights and interests of the data subject to a relatively greater extent, the Office holds that, where personal data processing does not rely on "employees' unambiguous consent" for its legitimacy, the employers involved must have substantial reasons to claim that their rights and interests or the collective rights and interests outweigh that of the employees. Where data processing relies on "employees' unambiguous consent" for its legitimacy, the employer institution concerned must ensure that employees may choose to disagree freely, as well as withdraw their consent at any time; the employer must also offer other reasonable means of attendance control for the employees to choose from.