



DATA PROTECTION REQUIREMENTS FOR ATTENDANCE VERIFICATION SYSTEMS (AVSs)

INTRODUCTION

It is within the legitimate interest of any employer to implement an AVS for the better control and management of the employees. Government departments are endeavouring to introduce AVSs in all its places of work, a corporate initiative driven by the Management and Personnel Office, OPM. The intention of implementing an AVS is for government departments to depart from traditional manual systems such as that of signing an attendance sheet, guidance for which has already been given in the Data Protection HR Corporate Procedures (section 2.13). There may also be other mechanical devices which may also have to be replaced with electronic devices.

The aim of these guidelines which have been discussed also with the Commissioner for Data Protection is to highlight the data protection implications which need to be taken into consideration prior to any decision being taken, and to provide data protection safeguards in the implementation of such systems.

TYPES OF AVS

These systems may be either mechanical or electronic. Normally AVSs are classified into two categories, namely those referred to as Conventional Recognition Devices (CRD), and other more sophisticated type termed as Biometric Recognition Devices (BRD). The difference between the two types is:

- a) The CRD processes normal conventional binary data, and they are regarded as less privacy intrusive systems. Such devices may include electronic tags, swipe cards, punch clocks and others.
- b) The BRD processes biometric data to measure physical, physiological or behavioural characteristics of an individual. These devices would automatically identify biometric features including hand geometry or palm, fingerprint, iris and retina, face recognition and/or others.

DATA PROTECTION IMPLICATIONS

AVSs may be used for security purposes, recording attendance, salary computation and audit trails. The Data Protection Act (DPA) applies to AVSs in the same manner as it applies to any other operation of processing personal data. The implications are the same and in general it is expected that:

1. There are criteria for processing (see article 9 of DPA). Processing operations by AVSs fall under article 9(f) as it is considered that an employer has a legitimate interest to introduce systems for time and attendance, as well as to monitor efficiency at the place of work.
2. All requirements for processing are adhered to (article 7). In particular the following have to be strictly observed:
 - a. Proportionality – is viewed in relation with the purpose for processing. Personal data is required for a specific purpose and has to be adequate, relevant and not excessive for such purpose.
 - b. Fair obtaining and lawful processing – implies that the data subject is to be aware of such processing and that it is done fairly, only for the purpose for which data is collected.
 - c. Transparency – is achieved if sufficient information is given to the data subject, namely the purpose for processing, recipients of data, and any third parties to whom data are disclosed.

- d. Accuracy – entails having procedures in place to ensure that data are kept up to date if changes occur. Procedures need to be in place across all departments to cater for such requirement.
 - e. Retention – consists of procedures to delete all data in the event that an employee is no longer part of the organisation in question.
3. There should be appropriate technical and organisational security measures against unlawful use and accidental destruction or loss in line with article 26. Such safeguards are required for the secure storage and access of personal data stored in an AVS. As is the case with other critical systems, logical and physical controls, including business continuity plans, should address this area.
 4. The data subject can also exercise the right of access and can also request the data controller to rectify, block or erase any AVS data which is not processed in accordance with the DPA (vide articles 21 and 22).
 5. Where a processor is contracted to maintain an AVS, and hence may process personal data held in the system, the data protection clauses have to be included in the written agreement as stated in articles 25 and 26 of the DPA.

WAY FORWARD

Taking the above implications into consideration, the following way forward is being suggested

a) Data Controller

It is of utmost importance to determine at the outset who is the data controller. In cases where an AVS is to be implemented in one building which houses one department, it is very clear that the data controller will be the Head of Department. Government departments may be faced with a dilemma of who is data controller when a building contains more than one department/ministry, or if it is decided that one system is to be implemented for the whole ministry, incorporating all departments. Therefore in these circumstances, the data controller may vary depending on the way the ministry/departments are organised. This situation may prompt a two-way approach:

- i) Each department situated in the building may have an independent AVS for its own use. This scenario leads to the Head of Department/Ministry as the data controller.
- ii) The ministry, normally through the Chief Information Officer (CIO) or the Director for Corporate Services (DCS), implements an AVS for all departments under the ministry. This scenario is more of a centralised type of processing aiming to achieve economies of scale and exercise control across all organisations within the ministry. The data controller in this case will be either the Permanent Secretary delegating the responsibility to the CIO or the DCS, or else jointly if each head of department or his representative will have access to the data regarding his/her employees. If access is not possible directly through the system, each head of department may be provided with the necessary report concerning his/her employees only.

b) Purpose

As the processing criteria of an AVS concerns the legitimate interests of the employer, and article 9(f) of the DPA states clearly that: *“Personal data may be processed ifprocessing is necessary for a purpose that concerns a legitimate interest of the data controller.....except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy”*, it is critical to establish the finality of such processing operation, to determine the purpose for processing and the proportionality of what type of processing operation is required. This means that an employer must carefully think through any purpose or potential purpose, whether it is required just for attendance verification or for other purposes as well, including security and audit trail. In general, Data Protection Authorities regard the use of biometrics solely for attendance and payroll purposes as unreasonable, especially if the same objectives may be accomplished by less intrusive means, as in general it is viewed that biometrics can have

consequences in terms of the individual's fundamental rights and freedoms, including the right to privacy.

c) Type of Device

Data Protection Authorities often view the use of a BRD type of AVS by an employer as a privacy concern. The implementation of biometric systems at the place of work presents a number of risks of data protection breaches which need to be addressed. The finality and the purpose for processing are therefore of utmost importance to consider the proportionality to be applied to justify what type of device is to be used. The top level technical specification to be issued by MITA is to be consulted prior to issuing a tender for any type of AVS.

CRD

Assuming that the AVS is to be used solely for attendance and payroll purposes, the CRD is the preferred option. A CRD does not process biometric data and hence they are regarded as less intrusive to private life. The data generated in a CRD is similar to any other conventional computer system which processes binary data, and the safeguards required should be to the same level of other computer systems. In terms of processing personal data in a CRD type of AVS, interfacing with other systems will be smoother as there is no need to convert biometric data to binary code and then map to other identification details for further processing.

BRD

Where a device is required for security purposes, and access control and monitoring are required at a number of entrance points to certain sensitive locations within the building, or if secure identification is needed in order to prevent fraudulent acts, then the use of a BRD may be justified. Where the security requirement is not so clear, it is suggested that a business case be presented to the Commissioner for Data Protection (DPC) to seek approval prior to issuing the tender document. The Data Protection Unit at OPM may be asked to assist the department concerned in the discussions with the DPC, involving the Data Protection Officer as well.

Assuming that a BRD is justified, the following needs to be taken into account:

- i) The type of biometric system to be used should be one which involves less privacy risk by not processing the actual image of the biometric feature. Biometric images should not be stored but converted into templates and it would be extremely difficult to generate a usable image ("reverse engineered") from the template. Systems which allow the recording and storage of actual biometric features are unacceptable.
- ii) The preferred type is where the storage of data containing biometric elements are retained in a card held exclusively by the user for matching purposes. Biometric systems related to physical characteristics which do not leave traces (e.g. outline of the palm) are also preferred to those systems having a possibility to leave traces (e.g. fingerprint).
- iii) At enrolment stage, the biometric image should be converted into a template containing a unique binary code representing the unique characteristics of the biometric feature, which is to be encrypted and stored separately, normally in the device itself, from other identification data. The unique reference number is used to link with the other personal details stored in the back-end database which is normally situated either in a server or PC to be used solely for this system. Every time the individual is presented at the BRD, the biometric feature will be converted to the binary code and it is matched with the template code captured at enrolment stage. All steps should be taken to avoid the use of biometric data as a universal user ID.
- iv) Biometric data and the templates created thereafter should not be used for any other purpose than that specified to the data subject, and it should be confined only to that processing operation where the device is situated in the ministry/department concerned.
- v) Biometric applications should be self contained systems and should not interface with other biometric recognition applications. This means that the templates created would be unique for that application and cannot be used by other systems. The biometric application should, however, be capable of generating an output transaction file containing just the unique reference number and

the other necessary details (e.g. time in; time out; location; etc); to be further processed in other applications such as HR and payroll systems.

- vi) Changes in physical and physiological characteristics may result in a template becoming outdated. In this regard, a procedure must be put in place whereby the reliability of stored templates must be regularly checked and a periodic enrolment is suggested to ensure that the template built on biometric data is kept updated. The supplier of the BRD may be consulted in this regard.
- vii) There should be an alternative procedure to cater for those cases where individuals are not in a position to use biometric systems.

d) Engaging a Processor

Where a processor is going to be engaged to maintain the application and the device in question, a contract in writing should be in place containing data protection clauses in line with the Policy regarding Processors engaged by Ministries/Government Departments and the specimen clauses therein (http://intra.gov.mt/downloadfile.asp?file=d_xi_contractual_clauses.pdf&site=1)

e) Informing the Data Subject

As provided by the DPA, the employees, being the data subjects, should be given all the information regarding the processing of their personal data, including who is the data controller, whether biometric data are being processed or not, the purposes for processing, how data are being collected and used, who has access to such data, and knowledge of the logic involved in any automatic processing of personal data. The data subject should also be informed of the right of access and rectification if required.

f) Security

Role Based Access Control mechanism should be implemented to control all access rights and privileges, depending on the roles required by the users in question. There should be an audit trail indicating how the data are being accessed. Separate and more restrictive access control mechanisms should be implemented in case of biometric data. In this regard a full blown audit mechanism should be implemented even for biometric data and templates. Other organisational security measures should take place such as installing a CCTV camera near the devices, again, informing the data subjects accordingly. It is very important that the templates binary code is encrypted and all biometric data are deleted when no longer required, as indicated under retention requirements at point (h) below. Business contingency plans should also cater for business continuity in case of default. All other security standards in accordance with GMICT policies (http://mitts.gov.mt/PortalPublic/ICT-HTML/GMICT_Policy_Index.html), such as password policies, etc, are to be implemented.

g) Notification and Prior Checking

All processing operations in relation to an AVS should be notified to the DPC. Where there are biometric data involved, an application should be submitted to the DPC for prior checking in accordance with article 34 of the DPA. The DPC will carry out an evaluation to check whether there are particular risks of improper interference with the rights and freedoms of the data subjects.

In cases where ministries/departments have already implemented an AVS, it is important that the notification to the DPC be updated. Furthermore, should the device process biometric data, (including palm readers), the DPC should be asked to carry out an assessment even though the system is already implemented.

h) Retention

Data should not be kept longer than necessary. A retention period should be determined, depending on the purpose of processing tied with the type of data being processed. The following scenarios need to be taken into account:

- i) In cases where the AVS is a CRD, recording only time and attendance of employees, the data may be kept for two years in line with the procedure for attendance sheets (section 2.13 in the Data Protection HR Corporate Procedures).
- ii) Where the purpose of the AVS is also for security and monitoring purposes and it is a CRD type, the security related data may be held for a longer period as required for security purposes, however deleting it after an extended period and if no security threats occur during that period.
- iii) In both different purposes above and where the AVS is a BRD type, all biometric data and the template code appertaining to the employee in question, with the exception of the template unique reference number, should be deleted within a month following the termination of the employee's employment with the data controller. All other data together with the template unique reference number may be held on the same lines as above.

A retention policy for AVS data should therefore be drafted in this regard, including also deletion of biometric templates where there are changes to biometric features as mentioned in c (vi) above. The National Archives Act is also to be taken into consideration in the process for approval for such retention policies, involving also the National Archivist.

CONCLUSION

This document has been discussed with MPO and approved by the DPC. It is not intended to be looked at in isolation. On the contrary, public officers should also consult the policy document to be issued by MPO as well as the technical specifications to be issued by MITA on the same subject. Other guidelines which may be issued by the DPC should also be consulted. The Data Protection Unit at OPM may be contacted for further guidance, should data protection assistance be required in the implementation of an AVS in a ministry/department, involving the Data Protection Officer in the process.

9 September 2009