Unofficial Translation

Principles Concerning the Protection of Personal Data in the Workplace: Guidelines for Employee Monitoring *

The Office for Personal Data Protection, September 2007

In accordance with, and for the purpose of effectively implementing, Law No. 8/2005, hereafter referred to as Personal Data Protection Law, these Guidelines have been formulated to protect personal data, and to help employers make corresponding policies on the monitoring of their employees after careful considerations so that breach of the law is avoided.

These Guidelines apply to institutions of the public sector and private sector, (hereafter referred to as Institutions) in the context of employers monitoring their employees' activities.

1. The Acts of Monitoring as Acts of Processing Personal Data

Generally, monitoring employees by the employer may involve telephone monitoring, Email monitoring, Internet monitoring, and video monitoring.

The act of employers monitoring their employees includes collecting and processing personal data.

In accordance with Article Four of the Personal Data Protection Law, "personal data" refers to any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (i.e. the data subject). The "identifiable person" refers to one who can be identified, directly or indirectly, in particular by reference to an indication number, or to one or more factors specific to his physical, biological, mental, economic, cultural or social identity, *such as name, sex, date of birth, age, marital status, address, telephone number, fax number, Email address, workplace, occupation/position, income, elector's number, bank accounts, photographs, voice and image, etc.*

"Telephone monitoring" refers to the monitoring and recording of the contents such as telephone numbers, telephone conversations and messages that the employee receives and sends through the telecommunication facilities provided by the employer. This includes the collecting and recording of the employee's voice, and others.

"Email monitoring" refers to the monitoring and recording of the Email items that the employee receives and sends through the facilities provided by the employer. This includes the collecting of the Email addresses that the employee uses for sending and receiving messages, and others.

"Internet monitoring" refers to the monitoring and recording of the web-browsing activities that the employee is engaged in through the facilities provided by the employer. This includes the collecting of the web-browsing records of the employee and the data that the employee has sent and received, and others.

"Video/CCTV (closed-circuit TV) monitoring" refers to the monitoring and recording of the web-browsing activities that the employee is engaged in through the facilities provided by the employer. This includes the collecting and recording of the images of the employee and of others.

The "processing of personal data" refers to any operation or set of operations which is performed upon personal data, by automatic means or otherwise, such as the collecting, recording, arranging, storing, adapting or altering, retrieving, consulting and using, disclosure by way of transmission, dissemination, alignment or combination/inter-connection, blocking, erasure, destruction or otherwise.

Article Three of the Personal Data Protection Law stipulates that this Law "applies to the processing of personal data by automatic means, wholly or partly, and to the processing of personal data by non-automatic means, which forms part of manual filing system." Therefore, the above monitoring activities are regulated by the Personal Data Protection Law.

2. Assessment by the Employer Prior to Decision on Employee Monitoring

Monitoring activities, such as telephone monitoring, Email monitoring, Internet monitoring and video/CCTV monitoring, involve collecting personal data of the employee, therefore the employer, prior to deciding whether to embark on employee monitoring, should evaluate the need and give careful and comprehensive considerations, particularly to the following points:

(1) The purpose of collecting the data and whether it is legitimate;
(2) Whether the practice of monitoring is necessary for achieving the purpose, and whether alternatives to monitoring are available, which will minimize involvement in the processing of personal data;
(3) Whether the monitoring practice, scope and timing is appropriate and justified;
(4) What data should be included for the collection and whether they are essential for attaining the expected goals;
(5) Whether the monitoring will safeguard the interest of the employer, the interest of the employee and the interest of the client;
(6) What harmful results brought about by inappropriate handling of the data collected; and
(7) How to formulate the rules for protecting personal data and the Personal Data Collection Statement.

3. Principles to be Observed Relating to Employee Monitoring

As monitoring is an act falling within the scope of personal data collection, the employer carrying out employee monitoring should abide by the Personal Data Protection Law, handle personal data in transparent and legal ways with due respect to personal privacy, fundamental rights and freedom as bestowed by law and observe the principle of good-will (See Article Two and Item 1 (1) of Article Five of the Personal Data Protection Law). The violation of the principles listed here may constitute administrative infringement, or even criminal acts. The employers may also need to compensate the victim.

(1) The Principle of Legality and Legitimacy

The principle of legality and legitimacy covers three aspects: the legitimacy of purpose, the legitimacy of methods and the legitimacy of scope.

A. The legitimacy of purpose

Generally speaking, the purpose of the employer collecting the personal data of the employee and monitoring the employee's behaviour in the workplace is to meet the operative need of the institution and safeguard the interests of the employer. It is legal and legitimate for the employer to conduct employee monitoring within the scope of business and accountability to guarantee the operation and general interests of the institution.
The major factors that the employer should bear in mind when conducting employee monitoring are:

- Whether they are measures necessary for the protection of the employee's safety;
- Whether there exist major risks of property loss or damage;
- Whether there are strong security demands necessitated by the nature of the institution;
- Whether there exist risks of employees' revealing/disclosing confidential information or secrets to other institutions or individuals;
- Whether there are employees engaging themselves in private activities during work-hours thus affecting their work efficiency;
- Whether there are improper uses of the computer facilities thus affecting the whole system of the institution;
- Whether the employee provides good service to the client and how to protect the tripartite interests: the interests of the institution, the interests of the employee and the interests of the client, in case the client lodges a complaint; and
- How to minimize the negative effects of employee monitoring on the relationship of cooperation and mutual trust between the employer and the employee.

B. The legitimacy of methods

To carry out employee monitoring legally and legitimately, the methods adopted must be those necessitated by the purpose. They must be open and accessible to the employee and the monitoring must not be conducted by secret means. The retention period of the data collected should be justified by the purpose. The retention period recommended is three months, not exceeding six months even in exceptional cases.

C. The legitimacy of scope

The areas/scope for the monitoring is limited to the employee's work-related activities and precludes activities related to the employee's private life. Acts falling outside this scope may constitute an intrusion of the right to privacy, and therefore a violation of Article Three of The Basic Law of the Macao Special Administrative Region (which states: … Macao residents shall enjoy the right to personal reputation and the privacy of their private and family life.) *For example, monitoring devices such as video/CCTV cameras must not be installed in the employee's rest-place or change-room and the Email messages that the employee sends to his/her family during non-office hours should not be monitored.*

(2) The Principle of Appropriateness

Here the principle of appropriateness mainly refers to appropriate and minimum intrusion.

A. No action of personal data collecting should be taken if alternatives are available to achieve the same purpose, i.e., if personal data collection is not absolutely necessary. *For example, in order to prevent computer viruses, the employer can install virus checking devices or filter software, and at the same time issue clear guidelines for the employee not to visit or browse certain webs, without resorting to collecting the data of the Internet webs that the employee has visited or browsed.*

B. Employee monitoring should only be targeted at and carried out in high-risk businesses and high-risk areas for the purpose of protecting the employer's legitimate interests and preventing potential risks. No personal data collecting should take place if the employee is not in possession of the institution's classified or confidential information or if the possession doesn't constitute a risk. Email messages labeled "Personal/Private" should not be monitored; no video monitoring should take place in non-high risk areas. *For example, video/CCTV cameras are installed only in places in which there are confidential or sensitive information, files, materials and systems.*

C. The monitoring hours should be kept to the minimum. No employee monitoring should take place during non-office hours.

D. The degree/extent of monitoring should be necessitated by the purpose to be achieved and collection and processing of personal data should be kept to the minimum. *For example, only the Email addresses by which the employee sends and receives messages and only the telephone numbers by which the employee sends and receives calls are recorded; the contents are not monitored unless absolutely necessary.* The contents of telephones, Emails and videos are reviewed and examined only when absolutely necessary. *For example, when a complaint is received from a client, it is necessary to check the contents of telephone recordings and Email messages.* However, when this is being done, it is best that the employee concerned should be present, unless he is involved in a disciplinary, administrative or criminal infringement under investigation.

(3) The Principle of Safeguarding the Rights of the Employee Concerned

Employee monitoring in the workplace must be open (by transparent means) to guarantee the exercise of relevant rights by the employee concerned. In accordance with the Personal Data Protection Law, the employee concerned/data subject has the right to information, the right of access and the right to object. (Articles Ten to Twelve, the Personal Data Protection Law)

A. The right to information

When personal data collecting takes place, the institution concerned should inform the employee concerned of the following:

- The identity of the entity responsible for processing personal data, and the identity of the representative of the entity if there is one;
- The purpose for processing the personal data, *such as ensuring the safety of business secrets of the institution, guaranteeing service quality, guarding the safety of high-value materials, etc.*
- The category of the data receiver or receiver;
  Whether the data will be passed on to other institutions for information or for handling in the process of monitoring, the employee concerned should be informed if a processor is involved.
  In general, the data is already recorded in the system of the institution concerned and it is not necessary for a third party to process it. However, the employer should assign certain personnel to conduct the monitoring and processing the relevant data. At the same time the employer should make it known to the employee that the data may be submitted to competent authorities, investigators and the judiciary for purposes of criminal or disciplinary investigations.
- Replies, obligatory or voluntary, from the employee concerned, as well as the consequences if the employee concerned does not reply.

This applies to the situation when questioning and answering are involved in an investigation for data collecting.

- Under necessary circumstances, in order to ensure accurate data processing, the employee concerned has the right of access, consult and make rectifications and is informed of the conditions and terms for exercising these rights. (See B. The right of access given below.)

B. The right of access

The employee, being the data-subject, has the right of access. The employee can consult his/her personal data freely without restriction and the employer should provide him/her with relevant information within a reasonable period of time. The employee can obtain the following items:

- Confirming whether the data concerning the employee has been processed, the purposes of the processing, the categories of the data processed, and the recipient or categories of recipient;
- Clear communication of the data undergoing processing and the source of the data;
- Knowledge of the reason why the relevant data has been automatically processed;
- The rectification, erasure or blocking of data the processing of which does not comply with the Personal Data Protection Law, in particular, because of the incomplete or inaccurate nature of the data;
- Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with that stated above, unless this proves impossible.

C. The right to object

Save where otherwise provided by law, the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, and where there is a justified objection the processing instigated by the controller may no longer involve the data.

4. Personal Data Collection Statement on Employee Monitoring: Points for Attention

Prior to conducting employee monitoring, the employer must formulate clear Personal Data Collection Statements, which clearly state and explain the following:

(1) The purpose of employee monitoring. *For example, whether the telephone recording is only for the purpose of ensuring service quality or also used for the purpose of appraising staff performance, whether video monitoring is for*

security purposes or the data recorded is used for the purpose of monitoring staff attendance.

(2) The categories of the personal data to be collected for monitoring.

(3) The uses of the personal data collected for monitoring, which should not be deviated from the purpose of monitoring.

(4) The criteria for using the personal data collected for monitoring: *For example, it should be stated clearly in the statement on Email monitoring that only the uses of private Emails are logged. If necessary, it should also include the conditions under which the contents of private Emails are monitored. It should be stated clearly in the statement on video monitoring whether the taped data is checked regularly or only when the need arises.*

(5) Authorized personnel with access to the data processed from monitoring: *For example, the personnel operating and monitoring the video & recording facilities; the personnel with the right of access to the relevant data.*

(6) Generally, the duration of the data processed for monitoring should not exceed six months, unless the law or contract terms stipulate a longer duration or the relevant records have become evidence of disciplinary, administrative or criminal infringement.

(7) The employee's right to information, right of access and to rectify data, and right to object should be clearly stated, and so should the regulations on the reasonable fees charged for the employee to exercise the right of access and consult data. The fees charged are on a case-by-case basis but the employee concerned should be informed of the fees before exercising this right.

(8) The formulation of "house rules" regarding employees using the institution's facilities for private or personal use. The house rules mainly include:

A. If the employer allows his/her employees to use the Institution's Email address, telephones and Internet/web facilities for personal or private use, what time they are allowed to use them and whether there are other restrictions. *For example, they should indicate contents or categories that cannot be transmitted by Emails; employees are requested to label their private Emails; activities that employees are not allowed to be engaged in when they are using the Internet; and the webs that they are not allowed to browse, etc.*

B. The venues or places where video facilities are installed and time when video monitoring takes place.

C. The ways in which the relevant data is retained and destroyed.

5. Other Points for Attention

(1) After a decision is made to carry out employee monitoring, the employer should communicate with the employee about the content of Personal Data Collection Statement so that the employee will understand and cooperate.

(2) The employer should ensure through various channels that the employee is informed of the content of the Personal Data Collection Statement and make timely reviews and revisions.

(3) Measures for retaining the collected data should be adopted to ensure that the data will not be deleted, reduced, revised, accessed by unauthorized persons or used for other purposes, lost or damaged due to improper keeping.

(4) Personnel authorized to monitor and process the data should undergone training in professional ethics and operational skills so as to ensure that they observe all the regulations relating to the purpose, uses and methods of use as stated in the statement.

(5) Once the employee monitoring takes place, all the persons using the relevant facilities, entering and leaving the relevant venues should be informed of the monitoring and the purpose of monitoring. *For example, the caller should be informed of the monitoring once he is put through; notices should be put up prominent positions in video-monitored venues and a note should be attached to an Email.*

(6) If a processor is needed to assist in conducting monitoring, it is necessary to select one who can ensure organizational and technical security and provide sufficient measures for security and confidentiality and is bound by the contract and the Guidelines.

(7) Most of employee monitoring involves automatic processing of personal data. The employer should notify the Office for Personal Data Protection in accordance with Article Twenty-two of the Personal Data Protection Law. The notification should include the content in Article Twenty-three of this law. If the processing of the data involves inter-connection/combination of personal data, application for permission should be made to the Office for Personal Data Protection. (See Article Nine and Article Twenty-two of the Personal Data Protection Law.)

(8) Even if it is stated in the contract that the employee is not allowed to handle private matters by using the institution's facilities, this does not mean that the employer can carry out employee monitoring at will. The employer must observe the Personal Data Protection Law and these Guidelines when conducting employee monitoring.

(9) The Office for Personal Data Protection recommend that well-equipped employers designate specialized personnel to be responsible for handling inquiries and requests in the area of "processing personal data" so as to

guarantee the interests of the employer, the interests of the employee and the interests of the client.

* The Office for Personal Data Protection will make appropriate adjustments or revisions to these guiding principles according to actual circumstances.

Appendices:

1. Sample: Personal Data Collection Statement on Telephone Monitoring
2. Sample: Personal Data Collection Statement on Video Monitoring
3. Sample: Personal Data Collection Statement on Video Monitoring

Personal Data Collection Statement on Telephone Monitoring
(Sample)

This Statement sets out the XXX's (hereafter referred to as Institution) policy regarding telephone monitoring within this Institution.

1. Regulations concerning employees using the Institution's telephone facilities

Owing to the needs of operation, telephone-monitoring facilities are installed within this Institution.

Employees are permitted to use the Institution's telephone facilities for personal and private purposes provided that this will not affect the operation and functioning of the Institution, damage its interests or violate any laws.

When using the Institution's telephone facilities, the employees are not permitted to perform the following acts:

- Disclosing confidential and sensitive information of the Institution;
- Engaging, in the name of the Institution, in activities outside the functions of the Institution;
- Performing illegal acts.

2. **The purpose of telephone monitoring**

The Institution monitors its employees using the telephone facilities that it provides, with the following aims and objectives:

- To ensure the quality of its service;
- To appraise the performance of its employees; and
- To guarantee the legitimate interests of the Institution.

3. The personal data collected from telephone monitoring

By using relevant technology in its central telephone monitoring system, the Institution collects the following information:

- The telephone numbers of incoming/outgoing calls received/made by the employees, dates, beginning and ending time, and recordings of contents.

4. **The use of personal data collected from telephone monitoring**

- For the purpose mentioned above, the Institution can access/consult all the data collected, including listening to the recordings of telephone calls.

5. Authorized personnel with access to the data processed from monitoring

Only directors and authorized staff members of the Institution have access to the data mentioned above. They all have the obligation to observe the rules set in this Statement and the principle of confidentiality.

In case of a disciplinary investigation, the relevant data may be passed on to the personnel responsible for disciplinary investigations.

In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be passed on to police authorities, judicial authorities or other competent institutions.

6. Duration of the Data Retention

Generally, the retention period of the above data is six months. In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be retained until after it is passed on to authorities or institutions stated above, or one month after the verdict of the trial, or even longer upon the request of those authorities or institutions.

7. Consequences of Violation

The person violating this Statement is liable to punishments, including the possibility of dismissal.

8. The Rights of the Employee

In accordance with the law, the employee has the right to information, the right of access and the right to object. When exercising the right of access, the employee should apply in writing to the directorship of the Institution and pay a reasonable fee for it.

Declaration of the Office for Personal Data Protection
This sample is for reference only. Institutions should formulate their own “Personal Data Collection Statement” in accordance with their own specific needs and circumstances.

Personal Data Collection Statement on Email & Internet Monitoring

(Sample)

This Statement sets out the XXX's (hereafter referred to as Institution) policy regarding its employees' use of the Institution's facilities to send and receive Emails and browse the Internet.

1. **Regulations concerning employees sending & receiving Emails and browsing the Internet**

To meet the needs of operation, the Institution provides some of its employees with Email and Internet facilities to facilitate their work.

The Institution permits its employees to use the above facilities for personal and private purposes under the following conditions:

- Pre-condition: This will not affect the operation and functioning of the Institution, damage its interests or violate any laws.
- Time of use: In general, employees should use the above facilities for personal and private matters during break/recess.

When employees use Email facilities for personal and private purposes, they should label their private Emails as "private". They are not permitted to perform the following acts when using Emails:

- Transmitting and disseminating indecent, obscene, defamatory, insulting and other unlawful or criminal messages or materials;
- Disclosing the Institution's confidential or sensitive information;
- Carrying out, in the name of the Institution, activities outside the functions of the Institution;
- Engaging in illegal activities.

When employees visit or browse the Internet for private and personal purposes, they are not permitted to perform the following acts:

- Browsing indecent or obscene websites or web-pages;
- Downloading or installing software without the Institution's permission;
- Uploading for disseminating the Institution's secrets or sensitive information;
- Uploading for disseminating indecent, obscene, defamatory, insulting and other unlawful or criminal messages or materials;
- Engaging in illegal activities.

2. **The purpose of Email & Internet-use monitoring**

The Institution monitors its employees using the Email & Internet facilities that it provides, with the following aims and objectives:

- To ensure the quality of its service;
- To appraise the performance of its employees; and

- To guarantee information security.

3. The personal data collected from Email & Internet-use monitoring

For monitoring purposes, the Institution collects, by means of computer software and relevant technology, the following information and has the data saved/stored in its servers:

- The Email addresses of senders and recipients of incoming/outgoing Emails received/sent by the employees, as well as dates, time, subjects and contents;
- The time that the employees browse the Internet, the web-pages and data sent and received by the employees.

4. **The use of personal data collected from Email & Internet monitoring**

- In order to guarantee the quality of service and appraise the performance of its employees, the Institution can access/consult at any time the contents of employees' Email messages that are not marked or labeled as "Private". In the case of security checks, disciplinary investigations or criminal investigations, or in other cases as required by law, the Institution can also access/consult the contents of employees' Email messages that are marked or labeled as "Private".
- In order to appraise the performance of its employees, the Institution can access/consult at any time the time that the employees use the Internet and the web-pages browsed by them. In the case of information security checks, disciplinary investigations or criminal investigations, or in other cases as required by law, the Institution can also access/consult the data sent and received by the employees.

5. Authorized personnel with access to the data processed from monitoring

- Personnel managing the Institution's Email & Internet facilities are authorized to access the relevant logs stored in the Institution's servers, but not the contents of Emails or the data sent and received by the employees. Only the directors of the Institution and staff members assigned by the directors can access/consult all the logs and contents. These staff members have the obligation to observe all the rules set in this Statement and confidentiality.
- In case of a disciplinary investigation, the relevant data may be passed on the personnel responsible for disciplinary investigations.
- In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be passed on to police authorities, judicial authorities or other competent institutions.

6. Duration of the Data Retention

Generally, the retention period of the above data is six months. In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be retained until after it is passed on to authorities or institutions stated above, or one month after the verdict of the trial, or even longer upon the request of those authorities or institutions.

7. Consequences of Violation

The person violating this Statement is liable to punishments, including the possibility of dismissal.

8. The Rights of the Employees

In accordance with the law, the employee has the right to information, the right of access and the right to object. When exercising the right of access, the employee should apply in writing to the directorship of the Institution and pay a reasonable fee for it.

Declaration of the Office for Personal Data Protection
This sample is for reference only. Institutions should formulate their own “Personal Data Collection Statement” in accordance with their own specific needs and circumstances.

Personal Data Collection Statement on Video Monitoring
(Sample)

This Statement sets out the XXX's (hereafter referred to as Institution) policy regarding video monitoring within this Institution.

1. Video monitoring

Owing to the need of operation, video-monitoring facilities are installed within this Institution.

Venues/premises equipped with video-monitoring facilities include: public reception areas (simultaneous recording), entrances and exits of offices and storerooms, and corridors. All the video-monitoring facilities are in 24-hour automatically working mode.

2. The purpose of video monitoring

The Institution conducts video monitoring, with the following aims and objectives:

- To protect the Institution's assets/properties and other legitimate interests;
- To protect the employee's safety and their other legitimate rights;
- To ensure the quality of service (restricted to public reception areas);
- To appraise the performance of its employees (restricted to public reception areas, entrances and exits of offices, including the check-in/check-out areas in which employees record their attendances).

3. The personal data collected from video monitoring

For monitoring purpose, the Institution adopts video monitoring facilities and relevant technology to automatically record all the images in front of the camera lens (parts of voices/sounds simultaneously recorded) and corresponding dates and time.

4. The use of personal data collected from video monitoring

For the purpose mentioned above, the Institution can access/consult all the data collected, including recordings and images.

5. Authorized personnel with access to the data processed from monitoring

Personnel responsible for security monitoring are authorized to observe the immediate records, but they are not permitted to access past records. Only the directors and designated personnel of the Institution can access all the above data, including past records. They all have the obligation to observe the rules set in this Statement and confidentiality.

In case of a disciplinary investigation, the relevant data may be passed on to the personnel responsible for disciplinary investigations.

In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be passed on to police authorities, judicial authorities or other competent institutions.

6. Duration of the Data Retention

Generally, the retention period of the above data is six months. In case of a criminal investigation, and when it is mandatory as required by law, the relevant data may be retained until after it is passed on to authorities or institutions stated above, or one month after the verdict of the trial, or even longer upon the request of those authorities or institutions.

7. **Consequences of Violation**

The person violating this Statement is liable to punishments, including the possibility of dismissal.

8. The Rights of the Employee

In accordance with the law, the employee has the right to information, the right of access and the right to object. When exercising the right of access, the employee should apply in writing to the directorship of the Institution and pay a reasonable fee for it.