G.N. 2206

GUIDELINES PURSUANT TO SECTION 8(5) OF THE PERSONAL DATA (PRIVACY) ORDINANCE

Pursuant to section 8(5) of the Personal Data (Privacy) Ordinance, notice is hereby given that the Privacy Commissioner for Personal Data has prepared a revised version of the *Privacy Guidelines: Monitoring and Personal Data Privacy at Work*. The revised version of the Guidelines as set out below takes effect on 22 April 2016 and henceforth supersedes the previous version of the Guidelines, which was published by notice in the *Gazette* on 17 December 2004.

Privacy Guidelines: Monitoring and Personal Data Privacy at Work

PART I – General

1.1 Introduction

1.1.1 These Guidelines ("these Guidelines") have been issued by the Privacy Commissioner for Personal Data ("the Commissioner") in the exercise of the powers conferred on him by Part 2 of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Ordinance"). Section 8(5) of the Ordinance empowers the Commissioner to prepare and publish guidelines for the guidance of data users and data subjects indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under the Ordinance.

1.1.2 Where employee monitoring is undertaken resulting in the collection of personal data of employees, the employer shall ensure that such act or practice complies with the Data Protection Principles ("DPPs") of the Ordinance. The Guidelines are issued in the context of personal data management and are indicative of the manner in which the Commissioner offers guidance to employers on the application of the provisions of the Ordinance as they relate to the activity of employee monitoring.

1.2 Purpose of these Guidelines

1.2.1 The purpose of these Guidelines is to provide guidance to employers on the steps they can take in assessing whether employee monitoring is appropriate for their business, and where it is deemed appropriate, how they can develop privacy compliant practices in the management of personal data obtained from employee monitoring.

1.2.2 These Guidelines offer a practical solution in terms of balancing the legitimate business interests of employers and the personal data privacy rights of employees. They are not definitive statements of law. On the contrary, they constitute an approach that should be seen to be illustrative of best practices while at the same time acknowledging that there will always be certain exceptions to the rule. In promulgating these Guidelines, the Commissioner is endeavouring to establish recommended standards of personal data management in the context of employee monitoring.

1.3 Application of these Guidelines

1.3.1 The Ordinance is enacted to protect the privacy of individuals in relation to personal data. For information to qualify as "personal data" within the definition given in the Ordinance, the information must be represented in a recorded form relating directly or indirectly to a living individual and from which it is practicable to ascertain directly or indirectly the identity of the individual. Otherwise it falls outside the ambit of the Ordinance.

1.3.2 Accordingly, these Guidelines apply to employee monitoring activities whereby personal data of employees is collected[1] in recorded form. They do not apply to activities where no personal data of employees is collected.

1.3.3 Because of the diverse needs of employers operating in different business sectors it would be unwieldy to try to address all the personal data privacy issues arising in every conceivable situation in which employee monitoring is undertaken. What these Guidelines seek to do is to offer practical guidance on the steps that should be taken by employers when they monitor employees using the following means:

---

[1] According to the judgement given by Ribeiro, JA in the Court of Appeal case of *Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data [2000] 2HKLRD83,* there is no collection of personal data unless the collecting party is thereby compiling information about an individual whom he has identified or intends or seeks to identify and that his identity is an important item of information. Where there is no collection of personal data, the DPPs are not engaged.

- **Telephone Monitoring：** Monitoring and recording telephone calls and voice mails made or received by employees on telecommunications equipment, including mobile phones, made available by the employer.

- **Email Monitoring：** Monitoring and recording employees' use of email sent and received on equipment made available to them by the employer.

- **Internet Monitoring：** Monitoring and recording employees' web browsing activities using equipment made available to them by the employer.

- **Video Monitoring：** Monitoring and recording employees' work activities and behaviours by the use of video recording or closed circuit TV systems ("CCTV"), or similar equipment.

1.3.4 It may be difficult, in some situations, to ascertain whether a monitoring activity would amount to "collection" of personal data and hence fall within the scope of these Guidelines. The following examples illustrate situations in which "collection" of employees' personal data may not have occurred; nonetheless it would be prudent for the employer to observe the good practices contained in these Guidelines.

Examples:

(a) The real time viewing of images of employees displayed on a monitor that is an integral part of a CCTV system installed by the employer when the recording function has not been activated.

(b) The incidental capturing of the image of an employee who happens to walk across the tracking path of a CCTV camera that is installed for general security purposes.

(c) Telephone conversations that take place between an employee and a customer in which the conversation is recorded by an audio device for the sole purpose of keeping customer transaction records.

Explanatory notes:

In example (a), the recording function of the CCTV system has not been activated and consequently no personal data is capable of being collected.

However, the CCTV system may be readily switched from non-recording to recording mode such that the personal data of employees can be readily collected on videotape. This being the case, it would be prudent for employers to observe the good practices contained in these Guidelines.

In example (b), if the CCTV camera is located or positioned such that it does not focus on the activities of any particular employee or group of employees, there is no collection of personal data involved in the activity concerned despite the fact that there might be a glimpse of the employee's image recorded by the camera. However, if the employer has reasonable cause to retrieve from the tape a record of activities of employees, for example, a suspicion of wrongdoing or breach of in-house policies, such act of record retrieval by the employer may amount to "collection" of personal data.

In example (c), a conversation recorded between an employee and a customer amounts to information relating to the transaction conducted by the customer. It does not amount to an act whereby the employer is compiling information about the employee. However, the situation may change when the customer lodges a complaint against the employee for improper handling of his instructions. In which case, and in the course of investigating the complaint, the employer may resort to retrieving tape records (and thereby collecting data) relating to the way in which the employee has handled the transaction.

1.3.5 These Guidelines also apply, although in a limited manner, to covert monitoring activities carried out by employers of domestic helpers. A typical example is the use of hidden pinhole cameras by householders to monitor the activities of domestic helpers working at home. They often justify the use of these cameras on the grounds of protecting the safety of children or detecting child abuse. This type of monitoring can be highly privacy intrusive due to its secretive nature.

1.3.6 As distinct from a more conventional workplace such as an office, the type of monitoring mentioned in paragraph 1.3.5 occurs at the employer's home, for example, the lounge area, which also happens to be the workplace of the domestic helper.

1.3.7 The application of these Guidelines does not necessarily prohibit monitoring activities carried out in the domestic household. The central issues to be addressed concern the necessity, reasonableness and openness of the video monitoring activities intended to be undertaken by employers of domestic helpers.

1.3.8 An information leaflet, entitled "Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers" is issued specifically for domestic employers highlighting certain essential aspects of these Guidelines that are particularly relevant to employers of domestic helpers.

1.4 Using these Guidelines

1.4.1 These Guidelines provide a reasonably comprehensive guide to employers and offer a better understanding to employees of the application of the provisions of the Ordinance to employee monitoring. There is no intention on the part of the Commissioner to determine whether employee monitoring should, or should not, be resorted to in the process of effectively managing the assets, resources and affairs of the employer. That decision rests with the employer although it is one that may warrant consultation with employees.

1.4.2 The Commissioner strongly encourages employers who undertake, or may undertake, monitoring of their employees to comply with these Guidelines. Employers may either adopt the Guidelines as written or use them as a model that may be adapted to suit specific operational needs or circumstances.

1.4.3 The substance of the Guidelines is contained in Part II and Part III of this document. They are briefly outlined below.

- **Part II – Evaluating the Need for Employee Monitoring and its Impact upon Personal Data Privacy**

  The good practice recommendations under this heading of the Guidelines are designed to assist employers in assessing the appropriateness of introducing employee monitoring in the workplace and its impact on personal data privacy. In essence they draw upon the concept of fair collection of personal data under the relevant requirements of DPP1(2) of the Ordinance.[2]

- **Part III – Managing Personal Data Obtained from Employee Monitoring**

  This part of the Guidelines offers employers good practice guidance in the management of personal data obtained from employee monitoring. It draws attention to DPP5 requiring employers to be entirely open about the employee monitoring policies they adopt[3]. It also deals with restrictions placed upon the use of employee

---

[2] DPP1(2) provides that personal data shall be collected by means which are lawful and fair in the circumstances of the case.

[3] DPP5 requires that all practical steps shall be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data; be informed of the kind of personal data held and the main purposes for which such personal data is, or is to be, used.

monitoring records, their management and compliance with security, right of access, and retention requirements.

The statements contained in these Guidelines are not intended nor shall they be construed to be definitive statements of law. Nothing herein shall prejudice the exercise of the powers and functions of the Commissioner under the Ordinance. For the avoidance of doubt, these Guidelines do not affect the application of the common law duty of confidence that may arise in relation to employee monitoring.

PART II

Evaluating the Need for Employee Monitoring & Its Impact upon Personal Data Privacy

2.1 Introduction

2.1.1 This part of the Guidelines offers employers an assessment process that should be given consideration prior to any final decision being taken as to whether employee monitoring is appropriate to their needs. Where that is held to be the case, employers must address their legal obligations, under the provisions of the Ordinance, in relation to the collection of employees' personal data using monitoring devices.

2.1.2 Prior to embarking upon employee monitoring, employers are recommended to conduct due diligence by undertaking a systematic assessment process conveniently referred to as the **3As – Assessment, Alternatives and Accountability**. The purpose of such an assessment is to assist employers in determining whether employee monitoring is the best of a range of options given the risks and activities the employer seeks to manage.

2.1.3 The 3As process consists of a simple yet practical framework against which employers, and interested employees, may reflect upon the impact of conducting employee monitoring in circumstances that would involve the collection of the personal data of employees. The three components of the process are as follows.

- **Assessment** of the risks that employee monitoring seeks to manage and the benefits to be derived from applying it to those risks, having regard to the purpose(s) that relate to the business functions or activities of the employer.

- **Alternatives** to employee monitoring and a consideration of the range of options open to the employer that may be equally cost effective and practical in their application, yet less privacy intrusive.

- **Accountability** of the employer in those circumstances in which employee monitoring results in the collection of personal data of employees. It is the responsibility of the employer to implement privacy compliant data management practices in the handling of personal data obtained from employee monitoring.

2.2 Assessing the Appropriateness of Employee Monitoring

2.2.1 Employers are recommended to begin any consideration of employee monitoring by establishing the purpose(s) that employee monitoring seeks to fulfil. This can be determined by assessing the risks that employee monitoring seeks to manage and the benefits to be derived from applying it to those risks.

2.2.2 In assessing the risks that are to be managed, employers should not only identify the risks but also justify, in a realistic manner, the existence and extent of those risks. Mere perception of risk unconnected with the nature of the business would not be sufficient to justify employee monitoring.

2.2.3 Employers may consider circumstances in which employee monitoring may also serve to protect the interests of clients and customers. Depending on the nature of the business, benefits to third parties such as ensuring prompt dispute resolution or controlling service quality to customers may be taken into account when assessing benefits to be derived from monitoring.

2.2.4 Although employers have many legitimate reasons for monitoring employees it is incumbent upon them to satisfy themselves, and possibly their employees, that the reasons are well founded and that the monitoring is related to and align with their business needs. For example:

(a) to manage workplace productivity, service quality control or enforcement of company policies;

Example:

The amount of time spent on web-browsing activities by employees may be monitored to prevent company resources from being substantially

used for private purposes that may adversely impact upon the productivity of the organization.

Example:

Telephone records (both call list and content) may be collected for the purpose of monitoring service delivery e.g. to ensure the quality and consistency of telephone service to customers after employees have received on-the-job training in telephone service excellence.

(b) to protect the safety of employees, business assets, intellectual property or other proprietary rights;

Example:

The contents of email sent using communications equipment supplied by the employer may be monitored for the purpose of ensuring the integrity and security of confidential business information, e.g. to prevent insider trading or the leakage of company trade secrets.

(c) to prevent vicarious liability where the employer assumes legal responsibility for the actions and behaviour of employees;

Example:

The logging of websites visited by employees may be designed to detect activities that are prohibited when accessing the Internet such as downloading copyright protected materials without the licence of the copyright owner. Infringement of copyright laws is an act for which the employer may be held liable.

(d) to comply with statutory or regulatory obligations that provide, or give reasonable cause, for the preventive monitoring of employees.

Example:

CCTV cameras may be used to create a video record of employees entrusted with the handling of hazardous goods or equipment, e.g. radioactive or other toxic chemicals, to ensure compliance with health and safety regulations in the workplace.

2.2.5 Having established the purpose(s) of monitoring employees, employers should assess the likely adverse impact that monitoring may have on the personal data privacy of employees. In the process, it would be good practice for employers to consult, and take into consideration, the views expressed by employees in determining the parameters to a reasonable expectation of privacy at work.

Explanatory notes:

In the vast majority of cases, employee monitoring is conducted out of an operational need to protect the business interests of employers. Some employers may hesitate in communicating their intention to conduct monitoring on the basis that it may cause friction between employees and management. Where this reaction can be predicted, employers could limit any negative impact by involving employees in the process. A consultative approach would most likely be conducive to building mutual trust between employers and employees.

2.2.6 When assessing the adverse impact of monitoring, employers may consider its potential intrusiveness upon an employee's privacy by addressing the following questions.

(a) To what extent will personal data relating to the private life of an employee be monitored?

Example:

If monitoring of employee's email content is considered, the concern is whether the message being monitored is work related or purely private in nature. Emails that are clearly unrelated to employees' performance at work, e.g. the content of a personal email sent by an employee to his spouse during a lunch break, will likely be characterised as incurring a greater sense of intrusiveness.

(b) What categories of personal data will be collected in the process of monitoring? Will the personal data privacy of third parties be affected?

Example:

In telephone monitoring, the logging of telephone numbers of parties called by an employee in the form of a call list would be less intrusive than a more intensive logging system that records the contents of the conversation between the parties. In the latter case, the record of the conversation may have collected the personal data of a third party, e.g. a friend that the employee has called.

(c) What harm may be inflicted upon employees as a result of any improper management of their personal data contained in monitoring records?

Example:

The harm that could result in the event of a mis-management of monitoring records may depend on the sensitivity of data collected. A

taped conversation between an employee and his family doctor about the employee's health may be characterised differently than one recorded between the employee and a friend about a vacation plan.

(d) To what extent will the mutual trust essential for good employee relations be affected by the introduction of employee monitoring?

Example:

Overly intrusive monitoring measures can cause employees stress or erode trust within an organization. Employers are more likely to gain acceptance from employees if they take measures that ensure employees are guaranteed the areas, means of communication and periods of the day in which they can be sure they will not be monitored.

2.2.7 Having conducted the assessments as recommended in paragraph 2.2.1 (establishing purposes) and paragraph 2.2.5 (assessing adverse impact), employers should determine whether the undertaking of employee monitoring can be justified as "reasonable" and "fair" in the circumstances.

Explanatory notes:

An employer has a right to direct his employees' work activities and for that reason the employer has a right to reasonably monitor such activities. In exercising employee monitoring, employers should seek to strike a balance between the pervasiveness of monitoring and the magnitude of the employers' risk that the monitoring aims to reduce. The issue therefore is deciding what constitutes an acceptable level of monitoring.

2.2.8 In evaluating whether an employee monitoring measure may amount to a reasonable and fair practice, employers should take into account the following benchmark standards or other comparable standards:

- that the monitoring of employees serves a legitimate purpose that relates to the function and activity of the employer;
- that the monitoring measures are necessary to meet that purpose and are confined to the employee's work;
- that the personal data collected in the course of monitoring is kept to the minimum necessary to protect the interests of the employer or to effectively address those risks inherent in the lawful activities of the employer;
- that the monitoring is carried out by the least intrusive means and with the least harm to the privacy interests of employees.

2.2.9 As a matter of good practice in the management of personal data, employers are encouraged to document the evaluation process they have undertaken and share it with their employees. Such a gesture indicates the transparency of the process and informs employees of the rationale behind employee monitoring, what they may expect and the in-house rules that have to be followed.

2.3 Alternatives to Employee Monitoring

2.3.1 Employers should note that there are realistic alternatives to employee monitoring. Before committing to employee monitoring, employers are strongly encouraged to give careful consideration to alternatives that may be equally cost-effective and practical in their application, yet less privacy intrusive.

Examples:

(a) To detect computer viruses that may accompany any inbound email attachment, an employer may consider the installation of appropriate automatic virus checking software. This would enable the employer to detect suspect messages without having to resort to opening and reading the contents of all inbound emails addressed to employees.

(b) To prevent unauthorised access to websites containing salacious material, or downloading other unacceptable content from the Internet, an employer may consider the installation of filter software. This may achieve the same effect yet be considerably less intrusive than the employer logging all websites visited by employees.

2.3.2 Employers should examine whether there are pragmatic alternatives to the measures that may be resorted to when engaging in employee monitoring. In considering this issue, employers may reflect upon the following questions that serve to place reasonable limits on monitoring.

(a) Can monitoring be confined to areas of high risk?

Example:

Where CCTV is adopted as a means of protecting business assets, an employer should consider whether the monitoring can be restricted to selected areas instead of monitoring all areas, e.g. areas of operation that contain secret data, sensitive documents or high value items.

(b) Can monitoring be restricted to certain personnel or certain times of the day rather than conducted on a universal or perpetual basis?

Example:

Where appropriate, monitoring should be targeted and applied on a limited duration basis. Where seriously improper conduct is reasonably suspected to be or have been committed, monitoring might take place for the purposes of confirming the suspicion and for gathering of evidence. Unless the employer fails to narrow down the scope of suspected targets through limited or selective monitoring, it should not indiscriminately subject all employees to monitoring. Once the suspect is identified or evidence is gathered, the monitoring should cease.

(c) Would selective or random checking, rather than continuous monitoring, be effective and sufficient for the employer's purpose?

Example:

Continuous CCTV monitoring may be considered in areas where the safety of persons or protection of property is paramount, such as in correctional institutions, and where the risks cannot be adequately addressed by undertaking selective checks on a random basis. An example of telephone monitoring would be where an employer is obliged, under regulatory requirements, to carry out preventive monitoring on employees, e.g. fund managers and investment advisers whose business conduct is governed by the Code of Conduct issued by the Securities and Futures Commission.

(d) Can communications monitoring be restricted to the log records of communications rather than the contents of communications?

Example:

In general, employers are not precluded from monitoring employees' communications if they are business related. Very often, the log record of email communications would be sufficient if the monitoring serves to trace the time spent by employees on email usage unless there are compelling circumstances that warrant access to the contents of emails, e.g. when it is necessary to verify a possible violation of company rules on email usage.

2.3.3 As a general rule, employee monitoring should be conducted in an overt manner. Owing to its highly intrusive nature, covert monitoring should not be used unless it is justified by the existence of relevant special circumstances. In this respect, employers should take into account the following factors:

- there is reasonable suspicion to believe that an unlawful activity is about to be committed, is being committed or has been committed;

- the need to resort to covert monitoring to detect or to collect evidence of that unlawful activity is absolutely necessary given the circumstances;

- the use of overt monitoring would likely prejudice the detection or the successful gathering of evidence of that unlawful activity;

- covert monitoring can be limited in scope so that it targets only those areas in which an unlawful activity is likely to take place and it is undertaken on a limited duration basis only.

Example:

Where an employer has reasonable cause to suspect that unlawful activities are taking place in the workplace, e.g. theft of company confidential data by employees, it may not be feasible, using overt monitoring or other reasonable measures, for the employer to obtain conclusive evidence that would identify the parties concerned. In such circumstances, and as a last resort, the employer may consider covert monitoring for the express purpose of identifying those parties, and for no other purpose. Having identified any culprit(s), the covert monitoring should be immediately curtailed.

2.3.4 As a matter of principle, covert monitoring that makes use of video recording devices such as pinhole cameras that target at locations where employees have a reasonable expectation of privacy should be avoided. This applies to places such as toilets and changing rooms.

2.4 Accountability of the Employer

2.4.1 Employers who have decided to monitor employees at work should accept responsibility and be accountable for the proper conduct and operation of their monitoring activities. Specifically, they have a duty to ensure that:

(a) a privacy policy pertaining to employee monitoring is developed and brought to the notice of employees before the monitoring is introduced; and

(b) privacy compliant measures are developed to protect the personal data of employees that may be collected in the course of monitoring.

2.4.2 It is important for employers, as data users, to recognise that they are liable under the provisions of the Ordinance for the proper management of personal data collected while conducting employee monitoring. That legal obligation extends to the acts and practices undertaken by a third party where the third party is engaged as an agent acting with authority on behalf of the employer.

2.4.3 In addition, an employer is also liable for all acts or practices engaged in by those employees charged with the responsibility of handling personal data collected in the course of conducting employee monitoring.

Example:

Where managers or supervisors, in the course of their employment, are charged with the authority of carrying out employee monitoring that entails the collection of personal data, the employer should take measures to ensure that those staff have received training in the statutory requirements under the Ordinance and the procedures of managing personal data obtained from monitoring records.

Example:

If it is the intention of the employer not to monitor the email or web-browsing activities of its employees, but given the built-in recording features of the software and the ease and likelihood that such act may be committed by other staff for which the employer may be held liable, it is prudent for the employer to make clear its intention to those staff who are charged with the responsibility of administering such software or communication devices.

2.4.4 Apart from the liability mentioned in paragraphs 2.4.2 and 2.4.3, employers should be aware that their employee monitoring practices may be subject to investigation by the Commissioner in an alleged breach of the Ordinance if such practices involve the collection of personal data. In any investigation by the Commissioner, employers may be called upon to explain and prove, among other things, that:

- the monitoring is only carried out to the extent necessary to deal with the legitimate business purposes of the employer;
- personal data collected in the course of monitoring is kept to an absolute minimum and by means that are fair in the circumstances;
- a written privacy policy on employee monitoring has been implemented and practicable steps have been taken to communicate that policy to employees.

PART III

Managing Personal Data Obtained from Employee Monitoring

3.1 Introduction

3.1.1 This part of the Guidelines seeks to offer practical advice to employers on the development of employee monitoring policies and related personal data management practices. The coverage offered is not intended to be exhaustive, however, it is indicative of what the Commissioner would expect responsible employers to give careful consideration to when formulating monitoring policies and data management practices that are compliant with the requirements under the Ordinance.

3.1.2 In designing monitoring policies and data management procedures employers are encouraged to adopt a systematic process conveniently referred to as the **3Cs – Clarity, Communication and Control,** or some similar approach, that gives comparable coverage to the personal data privacy issues raised by employee monitoring. The three components of the process are as follows.

- **Clarity** in the development and implementation of employee monitoring policies that clearly specify the purpose(s) served by employee monitoring, the circumstances under which monitoring may take place and the purpose(s) for which personal data obtained from monitoring records may be used.

- **Communication** with employees to inform them of the nature of, and reasons for, the monitoring of their activities at work prior to undertaking employee monitoring.

- **Control** over the holding, processing and use of monitoring records to safeguard the protection of employees' personal data contained in them.

3.1.3 The 3Cs process is intended to illustrate a practical approach towards good personal data management. As with the 3As, employers are encouraged to make reference to the advice contained in these Guidelines to develop alternative guidance that could more effectively address sector-specific requirements.

3.2 Clarity in the Formulation of Employee Monitoring Policies

3.2.1 It is of paramount importance that employers adopt a transparent approach to the formulation and dissemination of employee monitoring policies and practices. An effective means of achieving transparency would be for employers to implement a comprehensive written privacy policy that governs personal data management practices relating to employee monitoring, i.e. an Employee Monitoring Policy[4].

3.2.2 An Employee Monitoring Policy should explicitly refer to the following matters:

- the business purpose(s) that employee monitoring seeks to fulfil;
- the circumstances under which monitoring may take place and the manner in which monitoring may be conducted;
- the kinds of personal data that may be collected in the course of monitoring;
- the purpose(s) for which the personal data collected in monitoring records may be used.

Explanatory notes:

A clearly articulated Employee Monitoring Policy would provide employees with a better understanding of the scope of monitoring activities undertaken by an employer. From the employer's perspective, a clear policy addressing monitoring activities would have the effect of making known the employer's intention regarding those activities that the employer seeks to restrict.

Where there are already in place general privacy policies which an employer has adopted, it is good time for the employer to review and consider improvements to these policies having regard to the good practices recommended in these Guidelines. In situations where different monitoring policies and practices were adopted, an employer may find it appropriate to consolidate these policies or to appoint a designated personnel to co-ordinate and implement these policies in the interest of efficient management.

Examples:

(a) It may be necessary for an employer, or particular employees, to comply with industry-specific statutory or regulatory provisions, e.g. a

---

4 A sample Privacy Policy Statement on Email Monitoring is provided in Appendix I.

professional code of conduct. Compliance with such a code may warrant the installation of monitoring equipment to ensure that employees fulfil their obligations. In these circumstances, the employer should document those requirements in the Employee Monitoring Policy as a stated purpose that warrants the collection of the personal data of employees by monitoring.

(b) The logging of email usage is normally carried out by network software on mail servers. Email logs may record the email addresses of senders, recipients of mail messages and the time of transmission. Network administrators access these logs for the purpose of routine maintenance and management of the network. The contents of emails are not normally logged but are stored on mail servers or saved in staff's email boxes. Where, under exceptional circumstances, access to and viewing of the contents of email is deemed necessary, employers should state clearly in the privacy policy the nature of the exceptional circumstances and those authorised to view the contents of email.

(c) Personal data obtained from employee monitoring should be used for purposes consistent with, or directly related to, the purposes for which the monitoring was introduced. Where the monitoring of the contents of telephone calls by tele-marketing staff is not only used for the purpose of enhancing the delivery of quality service to customers but serve other purposes as well, such as for assessing and appraising the performance of these staff, the good practice is for the employer to specify clearly all the intended purposes of use of the personal data so collected.

3.2.3 Employers who use video recording equipment to monitor the activities and behaviours of employees at work are recommended to include in the Employee Monitoring Policy information relating to the operation of the equipment. Such a disclosure offers clarity in terms of those activities to which the monitoring is directed and serves to inform employees of the measures taken to protect the recorded information. However, in deciding how to go about making such disclosure (or the extent of the information contained in the disclosure), the employer may have regard to the purpose given rise to the need to conduct video monitoring. Where, for example, the purpose is to collect evidence of wrongdoing based on reasonable suspicion, an employer may take into consideration whether disclosure would prejudice such purpose of collection.

Example:

An effective CCTV monitoring policy may include, in addition to matters described in paragraph 3.2.2, the following information:

- *those personnel authorised to operate the equipment;*

- *the criteria for accessing monitoring records, e.g. whether all recordings are viewed routinely or only when an incident is reported?*

- *the retention period of the recorded information, e.g. how long is the recorded information retained if no incident is reported?*

- *the security measures that apply to the storage, release and disposal of recorded information, e.g. a log record is kept to indicate when the information is released, under what authority and if it will be returned or destroyed after use.*

- *where the situation and the need for monitoring allow, it is recommended to include in the policy the areas in which the monitoring is located and the times when monitoring will be in effect.*

3.2.4 Employers who seek to monitor employees' activities relating to the use of work-related communication facilities are recommended to include in the Employee Monitoring Policy a clear statement regarding the conditions of use of such facilities ("house rules"). Declaring the "house rules" will enable employees to be informed of the consequences of their actions and, once informed, respond with appropriate behaviours.

Explanatory notes:

Communications monitoring is frequently undertaken by employers to ensure employees' compliance with corporate standards of conduct and house rules. Although the scope of house rules applied by employers to their employees may vary, as a matter of good practice the following aspects relating to the use of communications equipment should be considered:

- *an unambiguous statement informing employees whether personal use of communications equipment is, or is not, permitted;*

- *where personal use is permitted, the conditions that govern the use of communications equipment for private purposes;*

- *whether the employer reserves the right to access the contents of communications sent or received by employees other than the traffic or time logs recorded by communications equipment;*

- *the procedures and sanctions to be applied in those circumstances in which an employee is found to be in breach of the conditions of use.*

Examples:

(a) An effective email monitoring policy may include further information that addresses the following matters:

- *the types of contents that are prohibited in email usage, e.g. sending defamatory statements about other employees, sending company information that is confidential, etc.*

- *where appropriate, instructions for employees to label email messages as "Personal and Private" in the header field so that messages of a personal nature can be clearly distinguished from work-related messages;*

- *any specific procedures that apply to the distribution of incoming or outgoing emails and the erasure of email messages held on mail servers.*

(b) An effective Internet monitoring policy may include further information that addresses the following matters:

- *an electronic trace of every access to the Internet may be held on servers because server software routinely records the website addresses (i.e. URLs) of sites visited, the date, time and the duration of the visits;*

- *the types of activities that are prohibited when accessing the Internet, e.g. downloading materials that are subject to copyright protection, accessing sites containing pornographic contents, etc.*

- *where employers permit employees to use the Internet for personal purposes unrelated to work, e.g. online shopping or e-banking, they should inform employees to exercise good judgment when selecting the sites they visit and refer them to the types of sites that are held to be unacceptable.*

3.2.5 It would be good practice for employers to consult employees in the process of developing an Employee Monitoring Policy. The consultation provides an opportunity for employees to clarify any potential misunderstanding of the issues so that there is no prospect of any unpleasant surprise when the policy is put into force.

Example:

When developing an employee monitoring policy that allows for sanctions to be imposed on those employees in breach of the "house rules" relating to email usage, an employer may consult employees on the procedures designed to audit compliance with the house rules. In the process, employers may explain the steps to be taken e.g. whether a warning will be given before any disciplinary action is considered.

3.3 Communicating the Privacy Policy to Employees

3.3.1 Having developed an Employee Monitoring Policy, employers should take practicable steps to ensure employees to be notified of the policy. This could be done in a number of ways, for example:

- incorporate the policy into personnel training or orientation programmes;
- publish the policy in the employee handbook or manual;
- post the policy on notice boards;
- include the policy as part of an employment agreement;
- link the policy to a network login screen that requires affirmative acknowledgement before being allowed access to the network.

3.3.2 It would be good practice for employers to review their Employee Monitoring Policy on a regular basis to ensure that it is up-to-date and remains relevant to the needs of the employer. Employees should be immediately informed of any revisions the employer may make to any policies and practices that may impact upon the personal data privacy of the individual.

3.3.3 It would be good practice for employers to make known their monitoring practices to persons whose activities may be captured by monitoring equipment that is primarily used to observe employee actions and behaviours.

Examples:

(a) Where CCTV monitoring is in operation in locations accessible to the general public, employers should give notification by using clearly written signage prominently displayed in the proximity of CCTV cameras, or any other monitoring equipment, informing them that it is, or may be, in operation. A message along the following lines may be considered: "This area is under video monitoring for the purposes of ensuring your security and safety when visiting our premises".

(b) Where telephone monitoring is used to record conversations between employees and members of the public, it would be good practice for employers to activate a pre-recorded telephone message that informs incoming callers that the ensuing telephone conversation may be recorded and the purpose(s) to which the recording may be put. This would not apply if the employer has reason to believe that the calling party is likely to be aware of the taping of telephone conversations, e.g. such a condition has been included in a service agreement between the employer and the caller.

(c) *In the case of email monitoring, a warning notice alerting both senders and recipients of email may be inserted in all messages thereby notifying the parties of the existence of the monitoring system.*

3.4 Control over the Holding, Processing and Use of Monitoring Records

3.4.1 Unless employers obtain the prescribed consent of an employee, or unless there is an applicable exemption provided for under the Ordinance, an employee's personal data collected in monitoring records may only be used for the purposes stated in the employer's Employee Monitoring Policy, or for a directly related purpose.

Examples:

(a) *A "directly-related" purpose of a CCTV tape recording of a group of employees participating in a presentation skills training workshop would be to use the tape recording of that exercise for inducting new recruits or controlling service quality delivery.*

(b) *An exemption that may be of direct relevance would be where the personal data is used for the purposes of the preclusion or remedying of seriously improper conduct. In the context of employee monitoring, any act or conduct of the employee that would amount to valid grounds for summary dismissal could be indicative of "seriously improper conduct."*

3.4.2 Employers should note that information collected using monitoring equipment may be misleading, misinterpreted or deliberately falsified. It may also be inaccurate due to equipment or software malfunction. It would be prudent for employers to exercise care before using the information contained in monitoring records for the purpose of taking adverse action against an employee.

Examples:

(a) *An employer may resort to Internet monitoring to ensure that employees comply with house rules on web browsing. However, it should be remembered that different proprietary search engines generate different search results. Links to websites may, unintentionally, result in the employee visiting a prohibited site due to unclear hypertext links or misleading banner advertising.*

(b) *There are situations in which an employer may rely upon monitoring records as the basis for disciplining employees for infringing corporate policies or house rules e.g. "improper" email usage or web browsing "misconduct". If an employer wishes to use these records as a*

ground for dismissing an employee, the employer may consider allowing the employee access to the monitoring records and the opportunity to respond to any allegations made.

3.4.3 Personal data contained in monitoring records should not be kept any longer than is necessary for fulfilling the stipulated purpose, including any directly related purpose, for which the records are to be used. It would be good practice for an employer to specify the retention periods of monitoring records, taking into account the nature of the information and the purpose for which the personal data was collected.

Example:

Recorded information contained on CCTV tape records should be routinely erased according to a pre-determined schedule, say 7 days. Although different circumstances may necessitate different retention periods, a shorter period should also be considered, e.g. if viewing of the recorded information reveals no incidents or no incident is reported after a certain period.

3.4.4 Generally, retention periods of not more than six months are preferred. While recognising that longer retention periods may be appropriate in certain circumstances, it is prudent for employers to consider any exceptions on a case-by-case basis. For example, an employer may be obliged to retain monitoring records for a longer period under the following circumstances:

- where there is a legal or contractual obligation on the part of the employer to retain the records for a specified period;
- where the recorded information reveals an incident of wrongdoing or seriously improper conduct by an employee and the employer uses the information to make a decision that directly affects the employee;
- where the recorded information are required as evidence in legal or disciplinary proceedings.

3.4.5 Employers should implement security and access control measures to safeguard the protection of personal data collected in monitoring records against unauthorised and accidental access, or wrongful use.

Examples:

(a) CCTV tape records or other storage formats that are used should be securely locked in a storage facility located in a controlled access area. When old storage formats are disposed of, they should be destroyed by irreversible, secure means and not deposited in unattended public disposal facilities.

(b) *Access to personal data collected from employee monitoring should be restricted to authorised personnel and only for a notified purpose. For example, view information contained in monitoring records only when there is a need to do so, either because an incident has been reported or is suspected to have occurred. Where practicable, logs should be kept that record all instances of access to, and use of, the monitoring records.*

3.4.6 Employers have a responsibility to ensure that those personnel responsible for managing employee monitoring possess the requisite integrity, prudence and competence and are aware of any audit requirements that may be imposed on their activities.

Example:

Where IT staff are deployed to administer communications or CCTV monitoring, it is important that the persons entrusted with this responsibility exercise due diligence in the application of the employer's monitoring policies. Those personnel should be subject to periodic appraisal checks to ensure their activities are compliant with those aspects of the employer's policies relating to the management of personal data.

3.4.7 Employers should ensure that employees are able to exercise their right to access their own personal data collected in the course of employee monitoring, subject to the provisions of the Ordinance.

Explanatory notes:

An employee who is the subject of monitoring has a right to request access to his personal data derived from monitoring records under section 18 of the Ordinance. Unless exempted or prohibited from doing so under the Ordinance, an employer is required to provide a copy no later than 40 days after receiving a data access request from the employee. In the event of an employer being unable to provide the copy within the 40-day limit, the employer must communicate that fact and the reasons in writing to the employee concerned before the expiry of that period and must provide the copy as soon as practicable thereafter.

The Ordinance provides for a data user to impose a fee (which shall not be excessive) for complying with a data access request. It would be good practice for an employer to notify the employee of the charge imposed prior to compliance with the request. This is particularly important where, in order to comply with the data access request, the employer is obliged to undertake substantial editing work in order to delete third parties' personal data that may be contained on the same record as that of the requestor.

Examples:

(a) *A recorded telephone conversation between an employee and a customer in phone-banking transactions may contain personal data relating to the employee and the customer. When a data access request is made by the employee for a copy of the taped conversation, it may be impracticable for his employer not to disclose that part of the taped conversation that relates to the customer unless the customer has consented to such disclosure. In this circumstance, the employer may consider preparing a written transcript from the tape record having edited out the identifying particulars of the customer. A copy of the edited transcript may then be provided to the employee at a reasonable fee to cover the expense incurred.*

(b) *Electronic log records such as the traffic and time logs of email usage or Internet access are usually activated by network server software. Printing programmes that produce readable printed formats of these records are common features of the software. Where editing of any third party's data is required for the purpose of complying with a data access request concerning such log records, it can be made in the usual manner on the printed copy of the logs.*

(c) *An employee may request access under the Ordinance for his personal data held in a video tape, for example, a tape that recorded his attendance or behaviour at work. Technical assistance may be required in duplicating and editing the tape requested for and the employer may impose a fee for complying with the data access request, taking into account the costs involved which are directly related to and necessary for such compliance. The parties are therefore encouraged to seek for other practical solutions, for example, instead of asking for a copy of the tape, the parties may agree to the viewing of the relevant footage that contains the requested personal data. In the absence of any amicable solution, an employer shall ensure that in complying with the data access request, the identifying particulars of other data subjects (unless their consent is obtained) contained in the tape are edited out.*

Appendix I
A Sample Privacy Policy Statement on Email Monitoring

ABC Ltd - Email Usage Monitoring Policy

This statement sets out the company's policy regarding email facilities provided to employees of ABC Ltd.

Conditions of use of email facilities

ABC Ltd provides email facilities to employees primarily for facilitating the business of the company. However, the company is prepared to permit reasonable and responsible use of email facilities for non-business or personal purposes on the express understanding that such usage will not be detrimental to the best interests of the company or the responsibilities of the individual member of staff. The following email usages are not permitted:

- transmitting messages for personal commercial purposes;
- sending defamatory, indecent messages or other unlawful materials;
- disseminating sensitive or confidential information and trade secrets of ABC Ltd;
- knowingly causing interference with or disruption to the company's network resources, e.g. by sending unsolicited bulk mails or data that function in a malicious manner;
- performing any unlawful activities that may render the company liable for the acts done.

Purpose of monitoring email usage

ABC Ltd uses automated software to keep and monitor logs of email usage for the following purposes:

- to facilitate the efficient provision of service to customers;
- to maintain a stable email service environment for communications;
- to provide information for management to ensure the proper utilization of company's resources.

Circumstances under which monitoring may take place

ABC Ltd reserves the right to log all out-going and in-coming emails. The email log contains the email addresses of the sender or recipient, the date, time, and message header information. Copies of emails are also stored in network mail servers. The company reserves the right to access the contents of all business-related emails held in staff's mailboxes, at any time, during periods when staff are absent from work. This is necessary for the company to carry on its business affairs and in order to avoid any disruption of service to customers. Random checks will be conducted to ensure the conditions of use of email facilities are observed.

Purpose for which monitoring records may be used

The logs and recorded information of emails will be used for ensuring compliance with the purposes for which this policy seeks to fulfil. ABC Ltd reserves the right to access contents of email copies where it is necessary in order for it to respond to any legal processes or to investigate any suspected breach of this policy. Subject to aforesaid, all logs and copies of emails stored in the network mail servers will be routinely erased within one month. Authorisation to access the logs of emails is restricted to the Network Administrator. Access to contents of emails requires a higher level of authorisation.

Violation of this policy may result in disciplinary action including termination of employment.

All enquiries shall be directed to the Administration Manager who is the responsible officer for carrying out this policy.

Appendix II – Data Protection Principles

1 Principle 1 - Purpose and Manner of Collection of Personal Data

(1) Personal data shall not be collected unless -
(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
(b) subject to paragraph *(c),* the collection of the data is necessary for or directly related to that purpose; and
(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are -
(a) lawful; and
(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that -
(a) he is explicitly or implicitly informed, on or before collecting the data, of -
(i) whether it is obligatory or voluntary for him to supply the data; and
(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
(b) he is explicitly informed -
(i) on or before collecting the data, of -
(A) the purpose (in general or specific terms) for which the data is to be used; and
(B) the classes of persons to whom the data may be transferred; and
(ii) on or before first use of the data for the purpose for which it was collected, of -
(A) his rights to request access to and to request the correction of the data; and
(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

2 Principle 2 - Accuracy and Duration of Retention of Personal Data

(1) All practicable steps shall be taken to ensure that -
(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;
(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used -
(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise, or
(ii) the data is erased;
(c) where it is practicable in all the circumstances of the case to know that -
(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and
(ii) that data was inaccurate at the time of such disclosure.

that the third party -

(A) is informed that the data is inaccurate; and
(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3) -
data processor means a person who -
(a) processes personal data on behalf of another person; and
(b) does not process the data for any of the person's own purposes.

3 Principle 3 – Use of Personal Data

(1) Personal data shall not, without the prescribed consent of the data subject be used for a new purpose.–

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—
(a) the data subject is -
(i) a minor;
(ii) incapable of managing his or her own affairs; or
(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136);
(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and
(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section –
new purpose, in relation to the use of personal data, means any purpose other than -
(a) the purpose for which the data was to be used at the time of the collection of the data; or
(b) a purpose directly related to the purpose referred to in paragraph (a).

4 Principle 4 - Security of Personal Data

(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to -

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2) -
data processor has the same meaning given by subsection (4) of data protection principle 2.

5 Principle 5 - Information to be Generally Available

All practicable steps shall be taken to ensure that a person can -
(a) ascertain a data user's policies and practices in relation to personal data
(b) be informed of the kind of personal data held by a data user;
(c) be informed of the main purposes for which personal data held by a data user is or is to be used.

6 Principle 6 - Access to Personal Data

A data subject shall be entitled to -
(a) ascertain whether a data user holds personal data of which he is the data subject;
(b) request access to personal data -
(i) within a reasonable time;
(ii) at a fee, if any, that is not excessive;
(iii) in a reasonable manner; and
(iv) in a form that is intelligible;
(c) be given reasons if a request referred to in paragraph *(b)* is refused;
(d) object to a refusal referred to in paragraph *(c);*
(e) request the correction of personal data;
(f) be given reasons if a request referred to in paragraph *(e)* is refused; and
(g) object to a refusal referred to in paragraph *(f)*.

22 *April 2016*
Stephen Kai-yi WONG
Privacy Commissioner for Personal Data