

Personal Data (Privacy) Ordinance

**A Draft Code of Practice on
Monitoring and Personal Data
Privacy at Work**

Consultation Document

**Deadline for Submission of Comments
7 June 2002**



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

This consultation document is issued by the Office of the Privacy Commissioner for Personal Data for the purpose of public consultation in accordance with section 12(9) of the Personal Data (Privacy) Ordinance (Cap.486)

If you wish to make a submission in response to this document, please do so in writing in Chinese or English to the following address:

The Office of the Privacy Commissioner for Personal Data
Unit 2001, 20th Floor, Office Tower
Convention Plaza
1 Harbour Road
Wan Chai
HONG KONG

Tel: 2827 2827 Fax: 2877 7026 E-mail: pco@pco.org.hk

Submissions should be made on or before 7th June 2002

Please mark your submission: **Draft Code of Practice on Monitoring and Personal Data Privacy at Work**. If the submission is made by E-mail, please type **Draft Code of Practice on Monitoring at Work** in the subject field.

The PCO would like, either in discussion with others or any subsequent report, whether privately or publicly, to be able to attribute comments submitted in response to the consultation document. Any wish to remain anonymous in relation to all or part of a response will be respected, but if no such wish is indicated, it will be assumed that the party making the response may be named.

Any personal data provided with a submission will only be used for the purpose of carrying out this public consultation exercise, including the preparation of a final version of the code and any explanatory document or commentary in relation to it.

You have rights of access and correction with respect to your personal data. If you wish to exercise these rights with respect to personal data held by us, please contact the Administration and Finance Manager of the Office of the Privacy Commissioner for Personal Data at the above address.

*Office of the Privacy Commissioner for Personal Data
March 2002*

Table of Contents

Part I CONSULTATION PAPER

1	INTRODUCTION.....	4
2	THE ORDINANCE AND CODES OF PRACTICE	4
3	THE ORDINANCE AND EMPLOYEE MONITORING	5
4	THE DRAFT CODE OF PRACTICE	8

Part II DRAFT CODE OF PRACTICE ON EMPLOYEE MONITORING

	INTRODUCTION.....	15
	INTERPRETATION.....	17
	USING THIS CODE	18
1	FAIR EMPLOYEE MONITORING PRINCIPLES.....	19
	1.1 Introduction.....	19
	1.2 Principles Applicable to Employee Monitoring.....	19
2	FAIR EMPLOYEE MONITORING PRACTICES.....	21
	2.1 The Collection of Monitoring Records.....	21
	2.2 The Notification of Monitoring Practices.....	26
	2.3 The Handling of Monitoring Records.....	31

PART I – CONSULTATION DOCUMENT

1 Introduction

- 1.1 The Personal Data (Privacy) Ordinance (“the PD(P)O”) provides for comprehensive control of the collection, holding, processing and use of personal data, including personal data used for employment related activities. The purpose of this document is to consult with interested parties, and the public in general, on a draft Code of Practice (“the Code”) that seeks to give practical guidance to the application of the requirements of the Ordinance to employee monitoring involving personal data. The draft Code is set out in full in Part II of this document. Some key issues raised by the content of the draft Code, on which views are sought, are described in paragraphs 4.5 (Key Provisions) and 4.6 (Issues for Consultation) of this Part.

2 The Ordinance and Codes of Practice

- 2.1 The Privacy Commissioner for Personal Data (“the Privacy Commissioner”) is responsible under the Ordinance for promoting, monitoring and supervising compliance with its provisions.
- 2.2 The Privacy Commissioner may, for the purpose of providing practical guidance in respect of any of the requirements of the PD(P)O, approve and issue codes of practice (section 12(1) refers). Before approving a code of practice, the Privacy Commissioner is required to consult such representative bodies of data users to which the code will apply and other interested persons as he thinks fit (section 12(9) refers).
- 2.3 A contravention of a code of practice approved by the Privacy Commissioner does not of itself constitute a breach of the PD(P)O. However, such a contravention may be used as evidence against the person concerned in proceedings before a magistrate, court, or the Administrative Appeals Board (section 13(2) refers), as well as in any case before the Privacy Commissioner.

3 The Ordinance and Employee Monitoring

- 3.1 In 2000 the Office of the Privacy Commissioner for Personal Data (“the PCO”) commissioned the Social Sciences Research Centre of Hong Kong University to commission a survey of data users. In a sample of 485 respondent organisations, 64% had installed at least one of five types of employee monitoring facilities. The survey findings also revealed that only 18% of the 310 data users that operated any of the types of surveillance facilities had a written policy on employee monitoring. 35% of respondents did not even know whether such a policy existed. In the view of the PCO this is not a desirable situation given the provisions of the Ordinance and, more specifically, the provisions of Data Protection Principle 1 pertaining to the collection of personal data.
- 3.2 The PCO acknowledge that there are a range of justifiable grounds for some level of monitoring of some employees at certain times. The questions that need to be addressed by the Code are how much, which employees, and when? Only by providing answers to those questions can there be a balance between the rights of the employer and the personal data privacy rights of the employee established under the provisions of the PD(P)O. Those rights relate to the collection, accuracy, use, storage, security, access to, and correction of, personal data. The Code enshrines those rights and offers pragmatic guidelines and best practices associated with the application of the provisions of the Ordinance to employee monitoring.
- 3.3 The Code is of particular relevance to the employer and employee relationship because the technologies involved in employee monitoring may be used to collect, process, store or retrieve information that may contain personal data. An example of this technology would be E-mail monitoring software that may record details of outbound and inbound messages sent from, or to, an E-mail account provided by the employer for work-related purposes. In the absence of the employer prohibiting the use of E-mail facilities for personal use, there is a distinct possibility that it may be used for such purposes. Where that is the case both the employer and employee stand to benefit from the existence of a clear policy on E-mail and other facilities and networks that are subject to employee monitoring. The fundamental argument here is that clarity and transparency around employee monitoring practices are of benefit to both parties. The alternative is no employee monitoring policy and an assumed understanding between the parties. In both instances there is the prospect of ambiguity and in such circumstances employees run

the risk of an unpleasant surprise. The Code seeks to offer clarity to employers, employees and third parties e.g. clients visiting the employers premises, by providing a framework that will be of benefit to the drafting of an in-house policy on employee monitoring.

- 3.4 In seeking to strike a balance between the interests of the employer and the personal data privacy provisions of the PD(P)O, and related Data Protection Principles (please refer to Appendix I), the PCO is mindful of the need to apply two principles to the fairness of employee monitoring practices.

3.4.1 **The Principle of Proportionality**

An important tenet contained in the PD(P)O is that of proportionality. Employees are entitled to be treated with respect and dignity by their employer, and this includes an expectation of respect for their personal privacy, especially those behaviours, movements and communications which are clearly unrelated to the performance of their work.

Any intrusion on an employee's privacy should be in proportion to the benefits derived from monitoring by a reasonable employer, which, in turn, should be related to the risks monitoring is intended to reduce. The risks that an employer may take into account in justifying a certain level of monitoring include:

- Financial loss e.g. mis-appropriation of funds or fraud
- Damage to reputation and goodwill
- Unauthorised disclosure of confidential information, including loss of trade secrets
- Exposure to vicarious liability for the unlawful acts of employees.
- Productivity or lost working time.

However, in all of the above cases, and others, the level of monitoring should be no greater than is reasonably required to contain or guard against the risk. For example, a retailer may be able to justify subjecting sales staff to occasional 'mystery shopping' using a video camera so that the employer may determine the consistency and quality of service rendered by retail staff to customers. In such circumstances retail staff should be informed on or before any monitoring or recording is made. However, it would be difficult to justify placing sales staff under perpetual video or audio monitoring,

which records not only their interaction with customers but also their discussions with friends or relatives.

A further example is provided by those employers who claim that E-mail monitoring is necessary to prevent the loss of trade secrets. However, trade secrets can be communicated in many ways and have been well before the advent of E-mail. Unless there is some evidence that the use of E-mail poses a particular risk to trade secrets, that the organisation is particularly vulnerable, or that E-mail monitoring is part of a package of carefully considered measures to tackle the problem, it is difficult to see how indiscriminate or routine monitoring can be justified. Where monitoring is justified it should be limited to the E-mail of those employees who actually have access to trade secrets.

In the context of proportionality, even if some employees were to misuse facilities provided by the employer, it is reasonable to question whether employees who do not have the opportunity to access those facilities should be subjected to intrusive monitoring. Would it not be preferable for poor performance or inappropriate behaviour to be detected in other ways, and dealt effectively with by management? Even if some degree of monitoring was considered to be necessary, would it not be possible to reduce the level of such monitoring to an absolute minimum (e.g. through conducting occasional spot-checks)?

3.4.2 The Principle of Transparency

A second value that pervades the provisions of the Code, as it does the PD(P)O, is that of transparency or openness. More specifically, this would include the communication to employees of the nature of, and justification for, the monitoring of employees' activities and behaviours. In many areas of activity covered by the PD(P)O, transparency regarding the handling of personal data assists individuals in making an informed choice about whether to deal with an organisation or not. Conversely, without transparency, choice can never be fully informed. In an employment context however, there will rarely be an opportunity to exercise individual choice. If monitoring is justified at all, then it will be appropriate for all employees. It would defeat the purpose of monitoring to allow some employees to opt-out. However, this does not reduce the employers need to provide such information that will enable the employee to make an informed choice. As significant, is the fact that transparency is an important privacy value in its own right, and allows employees

and others to determine whether the principle of proportionality is being upheld.

Data Protection Principle 1 of the PD(P)O reinforces this view by regulating the purpose and manner of collection of personal data. The means of collection must be “fair in the circumstances of the case” and the data must be “adequate but not excessive in relation to the purpose”. These criteria may influence the lawfulness, under the PD(P)O, of the monitoring of employees. It is the responsibility of employers therefore to clearly specify the purposes served by employee monitoring, the data to be collected and the circumstances under which collection may take place. There can be little doubt that the most judicious way of informing employees is by the employer promulgating and disseminating a clear policy on employee monitoring. Such a policy would make employee monitoring activities transparent, and enable employees to make decisions on the basis of informed choice.

- 3.5 The draft Code of Practice contained in Part II of this document represents an initiative designed to assist employers in complying with certain aspects of the requirements of the PD(P)O applicable to employee monitoring. In addition, the Code offers employers good practice guidelines in the management of personal data obtained from employee monitoring records.

4 The Draft Code of Practice

4.1 Scope

The original recommendation made by the Law Reform Commission in its report entitled **Civil Liability for Invasion of Privacy**, issued in August 1999 was as follows:

“We recommend that the Privacy Commissioner for Personal Data should give consideration to issuing a code of practice on all forms of surveillance in the workplace for the practical guidance of employers, employees and the general public.”

This would be a comprehensive exercise and would take the Code of Practice into many areas such as drug testing, psychological profiling and productivity monitoring by automated equipment. After careful consideration the PCO has decided, at this stage, to restrict the scope of the Code to four commonly used types of employee monitoring.

- Monitoring of Telephone Calls
- Monitoring of E-mail
- Monitoring of Computer Usage e.g. Internet access
- Video Monitoring.

4.2 Terminology and Definitions

For the purposes of this consultation document, and taking into account the comments above, the following definitions have been adopted.

- **Telephone Monitoring.** All forms of monitoring voice calls made or received by employees on telecommunications equipment, including mobile phones, made available by the employer.
- **E-Mail Monitoring.** All forms of monitoring employees' use of E-mail sent and received on equipment made available to them by the employer.
- **Computer Usage (Internet access) Monitoring.** All forms of monitoring the activities of employees who use computer based 'browsers' to access the World Wide Web using equipment made available to them by the employer.
- **Video Monitoring.** All forms of monitoring the activities of employees by the use of video recording devices or closed circuit TV systems, or similar such equipment, excluding any assisted or unassisted direct (line of sight, or "eyeball") visual monitoring.
- **Employee Monitoring.** Employee monitoring means Telephone Monitoring, E-Mail Monitoring, Computer Usage (Internet access) Monitoring or Video Monitoringg Employee Monitoring.

4.3 Locations Where Employee Monitoring May Happen

The monitoring of employees by employers may happen wherever the employees happen to be located physically. Many employees carry out at least part of their duties outside a formal workplace e.g. visiting clients, on a site remote from the employer's premises, while

travelling etc. A related issue is that of the boundary between employees' work and their private lives. This boundary has become increasingly blurred as working from home becomes more common, and as employees may be expected to take calls and attend to E-Mail outside formal hours of work.

Another definitional issue that has arisen in Hong Kong is the position of domestic helpers or guest workers. It is clear in law that domestic helpers are in an employment relationship, usually with a member of the household, and as a consequence of that relationship the same issues arise in respect of phone call and video monitoring. Employers of domestic helpers should respect the reasonable expectation of privacy that accompanies an employee's personal life in the household, as distinct from the work duties performed in that household.

Given the features outlined above it is intended that the Code on employee monitoring should cover the employers of domestic helpers.

4.4 Structure

The contents of the draft Code comprise two types of text.

- i) The fundamental principles and mandatory provisions of the Code of Practice appear in normal typeface.
- ii) The sections in *italics* provide amplification of the provisions, general explanatory notes and illustrations of good practice. The intention is to assist the reader in both applying and complying with the mandatory provisions of the Code.

The draft Code provides guidance on the application of the provisions of the PD(P)O to employee monitoring. Specific references to the PD(P)O and the Data Protection Principles ("DPP") are contained in footnotes and provide the statutory basis for particular requirements of the Code. The full text of the DPP is reproduced in Appendix 1 of this draft.

4.5 Key Provisions

- 4.5.1 It is intended that the contents of the draft Code should provide a reasonably comprehensive guide to employers and employees on the

application of the provisions of the PD(P)O to employee monitoring. The substance of the draft Code is contained in three sections.

■ **The Collection of Monitoring Records**

The provisions under this heading of the draft Code are designed to ensure that any monitoring practices engaged by employers are proportional to the benefits to be derived from monitoring. In essence these provisions draw upon the concept of fair collection of personal data.

■ **The Notification of Monitoring Practices**

Secondly, the draft Code draws attention to the need for employers to be entirely open about the employee monitoring policies they adopt. It is recommended that such policies be formulated in consultation with employees and that their provisions, and the consequences of infringing those provisions, be drafted in unambiguous language that minimizes the prospect of any mis-understanding. The employer's policy on employee monitoring should be disseminated to all employees and, where there is any subsequent revision of that policy, those revisions should be clearly communicated to all personnel.

■ **The Handling of Monitoring Records**

The final section of the draft Code deals with restrictions upon the use of employee monitoring records, their management and compliance with security, right of access, and retention requirements.

4.6 Issues for Consultation

4.6.1 The draft Code has been prepared from the perspective of the employer who engages in employee monitoring practices. It offers a platform from which employers may develop a tailored approach to policy formulation that more specifically targets the needs of particular organizations and their activities. The general principles of proportionality and transparency, and the Data Protection Principles, remain equally applicable to any person or organization that monitors those in its employ.

4.6.2 In addition to any matters that may arise from the application of the draft provisions of the Code, comments are also invited on the more specific issues detailed below.

■ **Issue 1 - Employee Monitoring where no Record is Collected by the Employer**

The provisions of the PD(P)O apply to those circumstances in which employee monitoring practices result in a record of information that contain personal data in a form in which access to, or processing of, the data is practicable. Although most equipment used in connection with monitoring would tend to have some kind of recording capability, the possibility cannot be ruled out that, perhaps in some situations, employee monitoring may be done without any record being kept. (An example of this would be a security camera that scans an area of the employer's premises without simultaneously keeping a record on tape or disk.) Even so, in the draft Code it might be beneficial for employers to be provided with best practice guidelines that encompass the practice of monitoring where no record of employee personal data are kept.

Views are invited on the scope of the Code and, more specifically, whether it should address the situation depicted.

■ **Issue 2 - Grounds for Exception from Specific Provisions of the Code**

The draft Code applies to all employers irrespective of size: a view that is consistent with the position taken in The Code of Practice on Human Resource Management. However, in order to accommodate the individual requirements of employers operating in different sectors, the draft Code includes provisions that are subject to exceptions. Examples of these are contained in clause 2.1.4 (continuous and universal monitoring), 2.1.5 (video monitoring on a perpetual basis) and 2.1.6 (covert monitoring) of the Code. The PCO recognize that there should be a degree of flexibility in the application of these provisions to reflect the needs of employers involved in a wide range of industries and activities. Accordingly, certain provisions allow for a number of exceptions that are designed to address those needs.

Views are invited on any exceptions, other than those stated, that employers would like the PCO to give consideration to when preparing the final version of the Code.

■ **Issue 3 – The Retention Period for Employee Monitoring Records**

Data Protection Principle 2 of the PD(P)O makes provision for the retention of personal data. In clause 2.3.7 of the draft Code it is suggested that, as a matter of good practice, employee monitoring records should not be held for longer than six months after their date of collection. This period is consistent with the view taken by the Inter-departmental Working Group on Computer Related Crime. Please refer to paragraphs 8.4, 8.6 and 8.24 of that report.

An exception to the proposed retention period of six months would be where the retention of a record or personal data captured in the course of employee monitoring is required as evidence of wrongdoing.

Views are invited on the good practice guidance that employee monitoring records be kept no longer than six months, and any other mitigating circumstances, that might justify the retention of monitoring records for a period in excess of six months.

■ **Issue 4 – Alternative Approaches**

In the PCO's discussion with interested parties in the course of the preparation of this Consultation Document, the suggestion has been made that, rather than issuing the draft Code as a Code of Practice, the PCO may consider turning this into a set of guidelines for employers on Monitoring and Personal Data Privacy at Work, and issuing the document as such.

There are similarities and differences between the 2 approaches. Both the issuing of a Code of Practice, and that of a set of guidelines, by the Privacy Commissioner, will be empowered by the PD(P)O, the former under section 12(1), and the latter under section 8(5).

In addition, section 13 of the PD(P)O essentially provides that, any failure by a data user to observe a requirement in a Code of

Practice issued under section 12(1) will, in legal proceedings under the PD(P)O, give rise to a rebuttable presumption of contravention of the corresponding requirement of the PD(P)O. (For a more detailed explanation of this, please refer to the “Introduction” section of the draft Code in Part II.) This does not apply, however, to guidelines issued by the Privacy Commissioner under section 8(5).

It appears that there may be merits or demerits in each of the two alternative approaches.

Views are invited as to which approach is considered the more appropriate, having regard to the actual provisions of the draft Code, any difference in their likely effectiveness in promoting employees’ personal data privacy whether as requirements under a Code or as guidelines, and such other factors as may be considered relevant.

PART II – DRAFT CODE OF PRACTICE ON EMPLOYEE MONITORING

Introduction

THIS CODE OF PRACTICE (“the Code”) has been issued by the Privacy Commissioner for Personal Data (“the Commissioner”) in the exercise of the powers conferred on him by Part III of the Personal Data (Privacy) Ordinance (Cap.486) (“the PD(P)O”). Section 12 of the PD(P)O empowers the Commissioner to issue codes of practice “for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users.”

This Code was notified in the Gazette of the Hong Kong SAR Government on

The related Gazette Notice, as required by Section 12 of the PD(P)O, specified that:

- i) the Code will take effect on; and
- ii) the Code is approved in relation to the provisions of the PD(P)O and the Six Data Protection Principles contained in Schedule 1.

The primary purpose of this Code is to provide practical guidance to data users, being employers, who engage in practices that monitor and record the activities and behaviour of employees at work. In this regard, a breach of the Code by a data user will give rise to a presumption against the data user in any legal proceedings under the PD(P)O. Basically, the PD(P)O provides (in section 13) that:

- (a) where a Code of Practice has been issued in relation to any requirement of the Ordinance;
- (b) the proof of a particular matter is essential for proving a contravention of that requirement;
- (c) the specified body conducting the proceedings (a magistrate, a court or the Administrative Appeals Board) considers that any particular provision of the Code of Practice is relevant to that essential matter; and if
- (d) it is proved that that provision of the Code of Practice has not been observed;

then that essential matter shall be taken as proved unless there is evidence that the requirement of the PD(P)O was actually complied with in a different way, notwithstanding the non-observance of the Code of Practice.

Aside from legal proceedings, failure to observe a Code of Practice by a data user will weigh unfavourably against the data user in any case before the Privacy Commissioner.

Interpretation

Unless the context otherwise requires, the terms used in the Code have the following meanings:

“Communications monitoring” means Computer usage (Internet access) monitoring, E-mail monitoring or Telephone monitoring.

“Computer usage (Internet access) monitoring” means all forms of monitoring the activities of employees who use computer based ‘browsers’ to access the World Wide Web using equipment made available to them by the employer.

“Covert monitoring” means practices engaged by an employer to monitor and record the activities and behaviours of employees at work by the use of any hidden equipment, systems or other means where the operation of those equipment or systems is not made known to employees.

“DPP” means a data protection principle in Schedule 1 of the PD(P)O.

“E-mail monitoring” means all forms of monitoring employees’ use of E-mail sent and received on equipment made available to them by the employer.

“Employee monitoring” means Computer usage (Internet access) monitoring, E-mail monitoring, Telephone monitoring or Video Monitoring.

“Employer” means any person who has entered into a contract of employment to employ any other person as an employee and the duly authorized agent of such first-mentioned person.

“PD(P)O” means the Personal Data (Privacy) Ordinance.

“Telephone monitoring” means all forms of monitoring voice calls made or received by employees on telecommunications equipment, including mobile phones, made available by the employer.

“Video monitoring” means all forms of monitoring the activities of employees with video recording devices, closed circuit TV systems or equipment of the like, excluding any assisted or unassisted direct (line of sight, or “eyeball”) visual monitoring.

Using this Code

In this document the contents of the Code are arranged to indicate which parts of the text are mandatory, and which are illustrative of best practice.

- The fundamental principles and mandatory provisions of the Code are all printed in normal typeface.
- The text in *italics* offers illustrative examples and best practices. They amplify the Code to assist the reader to comply with the mandatory provisions of the Code.
- The footnotes provide specific references to the provisions of the PD(P)O or other sources that provide the statutory basis for the Code.

1 Fair Employee Monitoring Principles

1.1 Introduction

1.1.1 The monitoring of employees by employers must be lawful and fair to employees. Employers should be open and unequivocal about the operation of any employee monitoring practices, the personal data collected, the purpose of collection, and use of personal data gathered in the course of employee monitoring. A fundamental principle to be applied to employee monitoring is that it should be designed to operate in such a way that it does not intrude unnecessarily upon employees' dignity, privacy and autonomy. In this respect privacy means more than just respect for employees' private life or behaviour. Employees have a legitimate entitlement to be treated with respect and dignity by their employer¹, and this includes an expectation of respect for their personal privacy, especially those behaviours, movements and communications that are clearly unrelated to their performance at work.²

1.2 Principles Applicable to Employee Monitoring

1.2.1 Under the PD(P)O, personal data generally include any information about an individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained. Applying this to employee monitoring, any monitoring records compiled about employees' activities and behaviour at work would amount to personal data of the employees concerned.

1.2.2 To the extent that information contained in monitoring records amount to personal data, they should be collected in a way that is fair in the circumstances and for a lawful purpose related to a function or activity of the employer³. Furthermore, the data should be adequate but not excessive in relation to such purpose⁴.

¹ The Constitution of the International Labour Organisation (ILO), adopted in 1946 includes the provision that "... workers shall labour in freedom and dignity".

² *Protection of Workers' Personal Data*, An ILO code of practice, 1997, and *Conditions of Work Digest: Workers' Privacy: Part II: Monitoring and surveillance in the workplace. 1996*

³ DPP1(2) and DPP1(1)(a)

⁴ DPP1(1)(c)

1.2.3 Underlying the above requirements are two fundamental tenets that are of most relevance to employee monitoring:

1.2.3.1 **The Principle of Proportionality.** This provides that any intrusion into an employee's privacy at work should be in proportion to the benefits of the monitoring to a reasonable employer, which, in turn, should be related to the risks which the monitoring is intended to reduce.

In the application of this principle, an employer is required to assess the benefits of monitoring and to identify the risks that are to be managed. The employer should be able to justify that the level of monitoring is no greater than is reasonably required to contain or guard against such risks. In other words, higher levels of monitoring may only be considered where a lower level of monitoring would be ineffective and where the circumstances justify a higher level of intrusiveness.

1.2.3.2 **The Principle of Transparency.** This provides for the communication to employees the business interests served by employee monitoring, the data to be collected, the circumstances under which collection may take place and the purposes to which the data may be used.

Under this principle, an employer is obliged to develop, implement and disseminate a written policy in relation to any monitoring practices that it may introduce. Where the monitoring is directed towards ensuring an employee's compliance with the employer's standards of conduct or "house rules" in relation to the use of facilities provided to them, the employer should include in the policy a clear statement regarding the conditions of use of such facilities.

The existence of a policy makes monitoring activities transparent i.e. employees understand the "house rules" pertaining to employee monitoring. In that respect employees are informed of the consequences of their actions and can make appropriate decisions based upon that understanding.

2 Fair Employee Monitoring Practices

2.1 The Collection of Monitoring Records

The following clauses seek to ensure that employee monitoring is proportionate, having regard to the legitimate interests of the employer and the personal data privacy interests of the employee.

- 2.1.1 An employer should not introduce employee monitoring unless it is reasonably satisfied that any adverse impact on employee's privacy is proportionate to the benefits to be derived. In assessing the benefits of monitoring, therefore, an employer should realistically identify the risks that are to be managed.

Monitoring should be designed to operate in such a way that it does not intrude unnecessarily on employees' privacy. It is important that employers give due consideration to the privacy interests of employees such that an equitable balance is struck between the interests of both parties. This balance can best be achieved by employers consulting with their employees on the matter of employee monitoring.

When assessing the adverse impact of monitoring employers should take into account the impact of monitoring on the privacy of third parties such as customers visiting the employer's premises or those communicating by telephone or E-mail with employees. For example, when assessing the adverse impact of telephone or E-mail monitoring, employers should give consideration to the rights of those making phone calls or sending E-mail to, or receiving them from the organization, as well as those of employees or individuals referred to in communications where they are neither the sender nor recipient.

- 2.1.2 Before introducing any form of employee monitoring, employers should ensure that:

2.1.2.1 the monitoring serves a legitimate interest that is employment-related and concerned with the inherent nature of the job for which staff are employed¹; and

2.1.2.2 where comparable benefits can reasonably be achieved by other readily available methods that are less intrusive

¹ DPP1(1)

upon employees' privacy, then those alternative methods should be deployed.

Not all monitoring results in the collection of personal data and to that extent the activity of monitoring is not governed by the provisions of the PD(P)O. However, where employee monitoring practices result in a record of personal data e.g. that relate to the identities, activities and behaviours of employees, customers or visitors to the employer's premises then those records are subject to the provisions of the PD(P)O.

In assessing alternative methods, employers should give due consideration to the types of data that are likely to be collected in the process of monitoring. For example, in E-mail monitoring, employers should not retrieve and access the content of stored E-mail messages unless it is established that the business purpose for which the monitoring is undertaken cannot be achieved by recourse to a log of E-mail traffic data. Similarly, in computer (Internet) usage monitoring, employers should not monitor sites visited or content viewed if the monitoring of time spent on-line (accessing the Internet) will suffice in serving the business purpose(s).

- 2.1.3 An employer who undertakes communications monitoring should limit monitoring to the log record of communications, rather than the content of communications, unless it is clear that information contained in log records fails to suffice in achieving the business purpose(s) for which the monitoring is undertaken.

The monitoring or interception of content of communications should be subject to critical assessment and justification. As a matter of good practice, employers should engage a two step process in assessing first, the effectiveness of the communications log record and secondly the justification for accessing the content of communications in achieving the business purpose(s) of monitoring. For example, an employer should only consider monitoring the content of outbound E-mails sent by employees if neither a record of the E-mail traffic log nor a record of both traffic and the subject of E-mails can achieve the business purpose(s) for which monitoring is undertaken. In some circumstances access to the traffic log or subject header will not satisfy the business purpose. An example would be where it is necessary to open an E-mail attachment to verify a suspicion of misconduct or wrongdoing. In assessing whether the monitoring of E-mail content is justified, the employer should take into account the privacy of those sending E-mails as well as the privacy of those receiving them.

Monitoring the content of inbound E-mails can rarely be justified. Employees have no control over the substance of E-mails that are sent to them. For example, if it is necessary to detect computer viruses that may accompany

inbound E-mails, the proper preventative measure would be to install appropriate automated virus-check software so that employees are able to detect suspect messages. A need for virus detection to protect computer security does not warrant the employer opening and reading all inbound E-mail addressed to their employees.

2.1.4 Employers should not subject employees to monitoring practices that are continuous or universal in nature unless such monitoring takes place under the following circumstances.

2.1.4.1 **Continuous Monitoring**

Where continuous monitoring serves a legitimate purpose that is employment-related and this is the **only** means of ensuring the security of the employer's assets, the safety of persons, the integrity of the employer's business transactions, or the effective monitoring of exchanges of a sensitive business nature between employees and non-employees.

2.1.4.2 **Universal Monitoring**

Where the employer has prima facie evidence that leads to a suspicion of improper behaviour or serious wrongdoing and, on the basis of that evidence, it is not possible to attribute the improper behaviour or serious wrongdoing to a particular employee or group of employees.

Where appropriate, employee monitoring should be targeted and applied on a limited duration basis. For example, in the absence of strong grounds for suspecting that all employees are using employer provided networks for personal E-banking during normal working hours, contrary to the employer's established policy, then monitoring the traffic log of suspect employees, and only those employees, may be justified.

Continuous or universal monitoring can only be justified in very limited circumstances. In most circumstances, selective checks made on a random basis should suffice for the purpose(s) concerned. As a matter of good practice, where exceptions are likely to be applied by employers they should document and notify employees in writing of the exceptional circumstances in which continuous or universal monitoring may be justified.

2.1.5 Employers should not monitor particular locations on a perpetual basis in such a way that employees are under continuous video monitoring, unless such monitoring takes place in circumstances

where there is a paramount need to maintain high levels of security over sensitive information, protect property, or the safety of persons.

Monitoring devices deployed in these types of situations may involve the use of video cameras or closed circuit TV systems. Continuous monitoring by means of video devices is particularly intrusive to employees. Examples in which the exception circumstances may apply are situations where there are particular safety or security risks that cannot be adequately addressed by other less intrusive means. For example, the need for absolute security in correctional institutions or a banking hall. However, video cameras or closed circuit TV systems should not be installed or used in toilets, showers or changing rooms located within a workplace.

As a matter of good practice employers should set aside areas or facilities that employees may use in the confidence that those areas or facilities are not subject to monitoring. This might include rest areas, pantries and the provision of designated phones to facilitate personal and private calls.

2.1.6 Employers should not engage in the practice of covert monitoring of employees at work¹ except in circumstances where **all** of the following conditions are satisfied:

2.1.6.1 where specific criminal activity or serious wrongdoing have been identified by the employer; and

2.1.6.2 where the need to resort to covert monitoring to obtain evidence of that criminal activity has been established; and

2.1.6.3 where an explanation by the employer to employees of the need to engage in covert monitoring would likely prejudice the successful gathering of such evidence; and

2.1.6.4 where the employer has made a determination on the length of time over which the covert monitoring should be undertaken.

The covert monitoring of employees at work is highly intrusive. Covert monitoring conducted without cause, or the knowledge of employees, may amount to an act of unfair collection of personal data. For example, recording the contents of employees' E-mail by interception of E-mail communications.

¹ DPP1(2)

Where an employer has reasonable grounds for suspecting an act of criminal wrongdoing it may not be feasible, using overt monitoring, for the employer to identify the parties concerned. In such circumstances, and as a last resort, the employer may undertake 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.

Employers should document the process outlined in clause 2.1.6 and ensure that information obtained through covert monitoring is used only for the prevention or detection of criminal activity, or the apprehension or prosecution of offenders to whom the monitoring was directed.

- 2.1.7 Covert monitoring should be selectively applied by an employer only to those employees that, on the evidence to hand, are suspected of any serious wrongdoing, rather than indiscriminately subjecting all staff to this form of monitoring.

For example, in the absence of a strong suspicion of theft of the employer's property by all employee(s), covert monitoring should target those employees that have access to the property that is believed to have been stolen, and only those employees.

As a general rule, covert monitoring using video recording devices such as video cameras or closed circuit TV systems targeted at locations where individuals have a reasonable expectation of privacy should be avoided. For example, in the bedroom of a domestic helper.

2.2 The Notification of Monitoring Practices

The following clauses seek to ensure that employers are open and unequivocal in their statements about, and communication of, monitoring practices to employees.

- 2.2.1 Before introducing any form of employee monitoring, an employer should implement a comprehensive written policy that explicitly states the purposes to which the personal data collected may be applied (the “Employee Monitoring Policy”)¹. The Employee Monitoring Policy should be brought to the attention of employees on a regular basis.

It is not intended that employers of domestic helpers issue a written Employee Monitoring Policy to those in their employ.

As a matter of good practice, even under circumstances where no record of personal data is made, an employer should implement a policy detailing its monitoring practices. A copy of the policy may, for example, be posted on staff notice boards, retained in a computer file accessible to all employees, inserted in an employee handbook or, by periodic distribution of the policy to all employees.

Employers of domestic helpers should respect the dignity and privacy rights of their employees. They should notify any person in their employ of any monitoring equipment e.g. a video camera, that has been installed, and which may be used to record employees’ personal data or capture their actions and behaviour at work.

In the case of first hiring of a domestic helper, or renewal of contract, employers may consider appending to the employment contract a note that clearly indicates the nature of any monitoring equipment installed in the premises at which the employee is to work.

All employers of domestic staff should respect the needs of those staff for solitude and seclusion by ensuring that there is no monitoring in private places such as the bedroom, toilet and bathroom.

- 2.2.2 Employers should ensure that their Employee Monitoring Policy gives coverage to matters such as the business interests served, the type of monitoring systems employed, locations at which monitoring devices are operative, except where covert monitoring

¹ DPP1(2) and DPP5

is justified, times at which monitoring is in effect, criteria for accessing monitoring records, and the retention period of records.

The monitoring of employees can cover a very wide range of activities. An effective employee monitoring policy should state explicitly the business purpose and employees' activities to which the monitoring is directed. To the extent that the monitoring system creates data records that amount to personal data of employees, the policy should also indicate, in general terms, under what circumstances the employer may disclose or transfer such records. Where, under exceptional circumstances, covert monitoring is justified the employer should notify employees of this possibility in the policy. In developing the policy, consultation with staff may be beneficial to enhancing understanding and gaining acceptance of it by employees.

- 2.2.3 Employers who seek to monitor employees' activities relating to their use of work-related communication facilities should inform employees of the conditions of use (i.e. "house rules") of these facilities. These rules should be an integral part of the Employee Monitoring Policy communicated to all employees.

In this context, employee monitoring practices may include telephone, E-mail and computer usage (Internet access) monitoring. Very often, these forms of communication monitoring are directed towards ensuring an employee's compliance with the employer's standards of conduct or "house rules" in relation to the use of resources provided by the employer for use by employees. It is anticipated that these "house rules" will vary between organizations. However, as a matter of good practice, they should include, but not be limited to, the following:

- ~ An unambiguous statement informing employees whether the use of the employer's telephones, including mobile phones, E-mail systems and Internet access for personal usage is, or is not, permitted.*
- ~ Where employees are permitted to use employer provided telephones, E-mail systems and Internet access for personal use, the conditions governing their use for private purposes should be clearly conveyed to employees.*
- ~ The procedures and sanctions to be applied where employees, upon investigation, are found to have violated the conditions stipulated by the employer for the private use of telephones, E-mail systems and Internet access.*

- ~ *Whether the employer reserves the right to access telephone, E-mail and Internet logs to determine usage of the system on an individual account basis.*
- ~ *Whether the employer reserves the right to access the content of telephone conversations, E-mail messages sent or received by employees that are personal in nature.*
- ~ *Whether employees should separate personal E-mail from work-related E-mail and clearly indicate which messages are personal in nature. This may be achieved by labeling the message "Personal and Private" in the header field.*
- ~ *Whether use of the employer's systems for sending and receiving E-mails that are personal and private in nature is subject to the employee opening and accessing a Web-based E-mail account.*
- ~ *Specific procedures that apply to the distribution of incoming or outgoing E-mail and the erasure of unnecessary E-mail that are personal or have an attachment that is personal.*

When the "house rules" are introduced or revised employers may wish, as part of their contractual obligations, to consider requiring all employees to sign a letter indicating that they have read, understood, and agree to comply with the terms and conditions of the rules.

2.2.4 Employers who undertake communications monitoring to retrieve and access stored communications content should ensure that their conditions of use of communication facilities explicitly state those activities that are permitted and those that are forbidden.

While it is generally speaking the employer's prerogative to determine whether to permit employees to use employer provided systems for personal communications, where the employer permits this, it should also notify employees of conditions that apply to such use, if any. In particular, employees should not be misled, either by action or inaction, into false expectations regarding the extent to which their communications are private. For example, to the extent that monitoring of communications content may be justified, an employer may need to notify all staff that they are not permitted to use a company provided E-mail system to transmit salacious material or defamatory messages.

Similarly, where employers permit employees to use computer equipment and networks to access the Internet for non-work related purposes e.g. shopping

vacation booking or news sites, they should inform employees to exercise good judgement when selecting appropriate sites to visit. Employers should further emphasize that the URL of all sites visited will be routinely recorded on the Internet access traffic log.

Where an employee is permitted to make personal phone calls on a mobile phone supplied by the employer, the employer should make clear whether there are any conditions attached to the use of the phone for personal calls. For example, the employer may reserve the right to log all calls made on a mobile phone issued to an employee, and to access the call log. Alternatively, where a mobile phone, in conjunction with other technologies, is used to monitor the location of employees they should be clearly informed of this practice and the conditions attached to the location monitoring. For example those conditions may distinguish between normal working hours and an employee's private time.

- 2.2.5 Employers who undertake video monitoring in places accessible to the general public should ensure that a clearly written sign is prominently displayed in the proximity of the monitoring equipment such that the public are notified that monitoring is, or may be, in operation¹. This requirement does not apply to circumstances where covert monitoring may be justified.

The text of the sign should be in a language(s) which all employees and members of the public can understand having regard to the nature of business activities that are likely to take place in the locations being monitored. 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 premise.”

Where there is no intention whatsoever to identify any member of the public, not being an employee, whose image may appear in the video recording, there is no collection of the personal data of such unidentified person. Still, the display of the sign described above should be considered as a matter of good practice.

- 2.2.6 Employers who undertake telephone monitoring to record conversations between employees and members of the public should take all reasonably practicable steps to notify the public of this practice.²

¹ DPP1(2)

² DPP1(2)

The monitoring of employees' telephone calls will come within the scope of the PD(P)O if the calls are recorded and the data therein amount to personal data as defined under the PD(P)O. One way of making the notification is to activate a prerecorded telephone message that informs incoming callers that the ensuing telephone conversation may be recorded, and the purpose(s) to which that recording may be put. A message along the following lines may be considered.

"We wish to notify you that the contents of this telephone conversation may be recorded for the purposes of ensuring the consistency and quality of our customer service."

Where there is no intention whatsoever to identify any member of the public, not being an employee, whose voice may happen to be recorded, there is no collection of the personal data of such unidentified person. Still, the giving of the notification described above should be considered as a matter of good practice.

2.3 The Handling of Monitoring Records

The following clauses seek to provide practical guidance on the limitation of use, security, right of access to, and retention of monitoring records.

- 2.3.1 Subject to any exemptions provided for in the PD(P)O, personal data collected in the course of employee monitoring should only be used for a purpose, or directly related purpose, for which the monitoring was introduced¹.

Data collected in the process of employee monitoring would depend on the methods employed. For example, with video monitoring the videotape may contain recorded images of the interaction between employees and customers. In E-mail monitoring, the data collected may be log records or, where justified, contents of E-mail that an employee receives or sends. To the extent that employee-monitoring records contain data that amount to the personal data of employees, the use of these data would be subject to the requirements of the PD(P)O.

Generally speaking, 'directly related purposes' should be purposes that are within the reasonable expectations of employees. For example, a 'directly related purpose' of a video recording a group of employees conducting a presentation skills exercise would be the subsequent use of the videotape for training new employees in presentation skills. Other examples would be for quality control purposes, reviewing customer service standards or facilitating statistical analysis and reporting.

- 2.3.2 Access to employee monitoring records should be restricted to authorized personnel on the condition that accessing the records is for a notified purpose and proportional to the benefits to be derived. Logs should be kept of all instances of access to, and use of, the monitoring records.

Generally speaking, access to employee monitoring records should not be allowed by parties external to the workplace or by persons other than those whose activities are recorded. To the extent that the monitoring records contain data that amount to personal data of an employee, the employee should be entitled to access such monitoring records. However, disclosure of employee-related monitoring records by the employer would require the consent of the employee(s) concerned unless the employer has reasonable grounds for believing

¹ DPP3

that non-disclosure would be likely to prejudice a purpose that falls within the ambit of section 58(1) of the PD(P)O.

The purposes referred to in Section 58(1) of the PD(P)O include, inter alia, purposes used for the prevention or detection of crime, the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, dishonesty or malpractice by individuals. The words “unlawful or seriously improper conduct” extend beyond criminal conduct to include civil wrongs¹. Hence an employer may disclose monitoring records that contain the personal data of an employee to a third party if the employer has reasonable grounds for believing that the data disclosed will be used by the third party in civil proceedings and that non-disclosure of the data would be likely to prejudice the prevention, preclusion or remedying of a civil wrong by the employee.

However, it should be noted that the requirement is for the employer to have reasonable grounds for holding the belief referred to above and that the PD(P)O does not oblige the employer to accede to such a request for disclosure by the third party.

- 2.3.3 Employers should not use employee-monitoring records to engage in ‘fishing’. Fishing means trawling through employee monitoring records with no prescribed purpose in mind, other than to happen upon some illuminating incident by chance.

For example, where an employer retains an archive of video recordings taken by on-premise security cameras, those records should not be used for any purpose other than that which justifies their collection in the first place. Employers, or their authorized personnel, should only view information of monitoring records where there is a need to do so, either because an incident has been reported or is suspected to have occurred.

- 2.3.4 If the information contained in employee monitoring records is to be used for the purpose of taking adverse action against an employee, that employee should be presented with the information and given the opportunity to challenge or explain it before it is used.²

It should be noted that information collected through employee monitoring systems might be misleading, misinterpreted or even deliberately falsified. It may also be inaccurate due to equipment or software malfunction. For

¹ Court of First Instance in case HCPI 828/97

² DPP2(1)

example, in computer (Internet) usage monitoring, search results may differ with different search engines and links to web sites may also be misleading.

There are situations where employers rely on the use of monitoring records to discipline employees for breaching company policies, such as “improper” E-mail usage or web browsing “misconduct”. If an employer wishes to use these as grounds for dismissing an employee, the employer should give the employee access to the monitoring records and the opportunity to respond to all allegations.

- 2.3.5 Employers should take all reasonably practical measures to ensure that persons responsible for administering employee monitoring, and authorizing access to employee monitoring records, possess the requisite integrity, prudence and competence.¹

It is common for security staff to be deployed to administer video-monitoring devices. With E-mail monitoring, IT staff may be given the responsibility to implement specific monitoring software to retrieve stored messages from staff E-mail boxes. These staff may or may not be employees of the employer as some of the tasks may be contracted out to a service provider. It is important that persons entrusted with this responsibility should exercise due diligence in the application of the employer’s monitoring policies and be subject to periodic procedures designed to ensure their compliance with those policies.

- 2.3.6 Employers should ensure that personal data contained in employee monitoring records are protected by measures, which are appropriate in the circumstances, against their unauthorized and accidental access, use, disclosure and erasure.²

For example, videotapes or storage formats that are not in use should be stored securely in a locked cabinet located in a controlled access area. When old storage formats have to be disposed of, they should be destroyed by secure methods and should not be left unattended in public areas.

- 2.3.7 Personal data obtained from monitoring records should not be retained for a period longer than that necessary for the fulfillment of the purpose, including any directly related purpose, for which the records are to be used³.

For example, information recorded on videotape used in a CCTV system should be routinely erased where no incident has been reported over a

¹ DPP4(d)

² DPP4

³ DPP2(2)

reasonable predetermined period, for example 7 days. However, records may be retained for longer than 7 days if they are required for evidentiary purposes. For example, a recorded telephone conversation between an employee and a customer in phone-banking transactions, or in circumstances where there is a legal or contractual obligation on the part of the employer to retain the records. Generally, retention periods of not more than 6 months are preferred, although different circumstances may necessitate different retention periods.

- 2.3.8** Employers should ensure that employees are able to exercise their rights to access personal data¹ in monitoring records that relate to them, and request correction², unless exempted from doing so under the provisions of the PD(P)O.

An employee who is the subject of monitoring has a right to request access to his or her personal data derived from monitoring records under section 18 of the PD(P)O. Unless exempted from doing so under the PD(P)O, the 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 the employer being unable to provide the copy within the 40-day limit, the employer must communicate that fact in writing to the employee concerned before the expiry of that period and must provide the copy as soon as practicable thereafter.

Access in full or in part may only be refused on one of the grounds set out in section 20 of the PD(P)O or where there is an applicable exemption provided for in Part VIII of the PD(P)O.

¹ Section 18

² Section 22(1)

Appendix I - PD(P)O Definition, principles and key sections

PD(P)O Definitions

"data" means any representation of information (including an expression of opinion) in any document, and includes a personal identifier;

"data access request" means a request under section 18;

"data correction request" means a request under section 22 (1);

"document" includes, in addition to a document in writing -

- (a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and
- (b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

"employment" means employment under -

- (a) a contract of service or of apprenticeship; or
 - (b) a contract personally to execute any work or labour,
- and related expressions shall be construed accordingly;

"personal data" means any data -

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- (c) in a form in which access to or processing of the data is practicable;

"personal identifier" means an identifier -

- (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and
 - (b) that uniquely identifies that individual in relation to the data user,
- but does not include an individual's name used to identify that individual;

"use" in relation to personal data, includes disclose or transfer the data.

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 are 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 are 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 are or are 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 are 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 they were collected, of -
 - (A) his rights to request access to and to request the correction of the data; and
 - (B) the name and address of the individual to whom any such request may be made,
 unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are 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 are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
 - (b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used -
 - (i) the data are 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 are 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 are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and
 - (ii) that data were inaccurate at the time of such disclosure.
 that the third party -
 - (A) is informed that the data are inaccurate; and
 - (B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.
- (2) Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.

3 Principle 3 – Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than -

- (a) the purpose for which the data were 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

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 or other 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 are stored;
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are 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.

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 are or are 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).

Key Sections Referred to in the Text of the Draft Code

2 Interpretation

- (3) Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent -
 - (a) means the express consent of the person given voluntarily;
 - (b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).

18 Data Access Request

- (1) An individual, or a relevant person on behalf of an individual, may make a request -
 - (a) to be informed by a data user whether the data user holds personal data of which the individual is the data subject;
 - (b) if the data user holds such data, to be supplied by the data user with a copy of such data.
- (2) A data access request under paragraph (a) of subsection (1) shall be treated as being a single request, and the provisions of this Ordinance shall be construed accordingly.
- (3) A data access request under paragraph (a) of subsection (1) may, in the absence of evidence to the contrary, be treated as being a data access request under both paragraphs of that subsection, and the provisions of this Ordinance (including subsection (2)) shall be construed accordingly.
- (4) A data user who, in relation to personal data -
 - (a) does not hold the data; but
 - (b) controls the use of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with a data access request which relates to the data,shall be deemed to hold those data, and the provisions of this Ordinance (including this section) shall be construed accordingly.

20 Circumstances in which Data User shall or may Refuse to Comply with Data Access Request

- (1) A data user shall refuse to comply with a data access request -
 - (a) if the data user is not supplied with such information as the data user may reasonably require -
 - (i) in order to satisfy the data user as to the identity of the requester;
 - (ii) where the requester purports to be a relevant person, in order to satisfy the data

user-

(A) as to the identity of the individual in relation to whom the requester purports to be such a person; and

(B) that the requester is such a person in relation to that individual;

- (b) subject to subsection (2), if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the data user is satisfied that the other individual has consented to the disclosure of the data to the requester; or
- (c) in any other case, if compliance with the request is for the time being prohibited under this Ordinance.

(2) Subsection (1)(b) shall not operate -

- (a) so that the reference in that subsection to personal data of which any other individual is the data subject includes a reference to information identifying that individual as the source of the personal data to which the data access request concerned relates unless that information names or otherwise explicitly identifies that individual;
- (b) so as to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise.

22 Data Correction Request

(1) Subject to subsection (2), where -

- (a) a copy of personal data has been supplied by a data user in compliance with a data access request; and
- (b) the individual, or a relevant person on behalf of the individual, who is the data subject considers that the data are inaccurate,

then that individual or relevant person, as the case may be, may make a request that the data user make the necessary correction to the data.

58 Crime, etc.

(1) Personal data held for the purposes of -

- (a) the prevention or detection of crime;
- (b) the apprehension, prosecution or detention of offenders;
- (c) the assessment or collection of any tax or duty;
- (d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
- (e) the prevention or preclusion of significant financial loss arising from -
- (i) any imprudent business practices or activities of persons; or
- (ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(f) ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything -

- (i) to which the discharge of statutory functions by the data user relates; or
- (ii) which relates to the discharge of functions to which this paragraph applies by virtue of subsection (3); or

(g) discharging functions to which this paragraph applies by virtue of subsection (3),

are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to -

- (i) prejudice any of the matters referred to in this subsection; or
- (ii) directly or indirectly identify the person who is the source of the data.

(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which-

- (a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purpose); and
- (b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of those matters.