THE MEANING OF "PERSONAL DATA" AND THE SIX DATA PROTECTION PRINCIPLES I. THE MEANING OF "PERSONAL DATA" AND THE SIX DATA PROTECTION PRINCIPLES Personal data means any data "relating directly or indirectly to a living individual, from which it is possible and practical to ascertain the identity of the individual from the said data, in a form in which access to or processing of the data is practicable" (e.g. a document or a video tape). The legal definition of personal data can be found in section 2 of the Personal Data (Privacy) Ordinance (Cap. 486)("the Ordinance"). Obvious examples of personal data are an individual's identity card number and fingerprints, through which he or she can be identified. Alternatively, it may also be practicable to ascertain an individual through a combination of data such as telephone number, address, sex and age of an individual. The Ordinance came into force on 20 December 1996. It applies to any person who collects, holds, processes and uses personal data within the private and public sectors as well as government departments. Generally speaking, the Ordinance governs the ways of collecting and using personal data, and prevents any abuse of data that is considered as intruding on an individual's privacy. Under current statutory and common law in the Hong Kong SAR, only personal data is protected under the Ordinance. Article 14 of the Hong Kong Bill of Rights stipulates that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." However, the Ordinance does not cover privacy matters other than personal data. The six data protection principles Any person or organization collecting, holding, processing or using personal data must comply with the six data protection principles laid down in section 4 and schedule 1 of the Ordinance. (Note: The person from whom personal data are or will be collected is called the "data subject", and the person or organization that is collecting the personal data is called the "data user".) Principle 1 - purpose and manner of collection of personal data Personal data must be collected for a lawful purpose. The purpose of collection must be directly related to a function or activity of the data user. The data collected should be adequate but not excessive in relation to that purpose. Personal data should also be collected by lawful and fair means. Unauthorized access to another person's bank account records or credit card information is an example of unlawful means of collecting personal data. If a person/organization intentionally uses a misleading way to collect personal data, this amounts to an unfair means of data collection. A company collecting the personal data of job applicants by means of recruitment activities when in fact they are not really recruiting any one is an example of unfair means of collecting personal data. When personal data are collected from an individual, that person (the data subject) must be provided with the following information, which includes: the purpose for which the data are to be used; the classes of persons to whom the data may be transferred; whether it is obligatory or voluntary for the data subject to supply the data; the consequences arising if the data subject fails to supply the data; and the data subject has the right to request access to and correction of the data. Principle 2 - accuracy and duration of retention of personal data Data users must ensure that the data held are accurate and up-to-date. If there is doubt as to the accuracy of the data, data users should stop using the data immediately. They should not keep the data any longer than is necessary for the purpose for which the data were collected. Principle 3 - use of personal data Unless personal data are used with the prescribed consent of the data subject, the data must not be used for any purpose other than the one mentioned at the time the data were collected (or a directly related purpose). "Prescribed consent" means the express consent given voluntarily by the data subject. Principle 4 - security of personal data Data users must take appropriate security measures to protect personal data. They must ensure that personal data are adequately protected against unauthorized or accidental access, processing, erasure, or use by other people without authority. Principle 5 - information to be generally available Data users must publicly disclose the kind (not the content) of personal data held by them and their policies and practices on how they handle personal data. The best practice is to formulate a "Privacy Policy Statement" that encompasses information such as the accuracy, retention period, security and use of the data as well as measures taken regarding data access and data correction requests. Principle 6 - access to personal data A data subject is entitled

to ask a data user whether or not the data user holds any of his/her personal data, and to request a copy of such personal data held by that user. If it is found that the data contained therein is inaccurate, the data subject has the right to request the data user to correct the record. The data user must accede to the access and correction requests within a statutory period of 40 days. If the data user could not process the request within the period specified, it must provide a reply and state its reasons within 40 days. Individuals/data subjects who wish to make data access requests may download the Data Access Request Form (OPS003) from the Privacy Commissioner's Office and send the completed form to the company which holds the personal data. It should be noted that the Ordinance permits data users, in complying with the data access requests, to charge a reasonable fee. However, the data users concerned should not charge more than the direct cost of complying with the requests. 1. WHAT ARE THE CONSEQUENCES OF BEACHING THE DATA PROTECTION PRINCIPLES? 1. WHAT ARE THE CONSEQUENCES OF BEACHING THE DATA PROTECTION PRINCIPLES? The Privacy Commissioner's Office (PCO) may issue an enforcement notice to the person or company who committed the breach, with intent to direct that wrongdoer to stop violating the data collection principles and take any necessary remedial action. Non-compliance with the PCO's enforcement notice is an offence and is liable to a fine or imprisonment. The victim who suffers damage, including injury to feelings, as a result of such violation may also be entitled to compensation from the wrongdoer through civil proceedings. Please go to Part VII for more information regarding complaint procedures, enforcement and penalties. 2. ARE THERE ANY SITUATIONS IN WHICH THE PERSONS/COMPANIES HOLDING PERSONAL DATA MAY BE EXEMPT FROM THE ORDINANCE OR THE DATA PROTECTION PRINCIPLES? 2. ARE THERE ANY SITUATIONS IN WHICH THE PERSONS/COMPANIES HOLDING PERSONAL DATA MAY BE EXEMPT FROM THE ORDINANCE OR THE DATA PROTECTION PRINCIPLES? In some situations, data users may be exempt from the restrictions imposed by the Ordinance or the six Data Protection Principles (DPP). The Personal Data (Privacy) (Amendment) Ordinance 2012 (the Ordinance) introduces further new exemptions. The situations for exemptions are summarised below: Household affairs or recreational purposes According to section 52 of the Ordinance, personal data for household affairs or recreational purposes is exempt from "DPP 4 and 5, and Ordinance sections 36 and 38(b). Keeping the phone numbers of your family members for daily communication or keeping the phone numbers of your friends to arrange leisure activities are examples in this category. Performance of judicial functions According to section 51A of the Ordinance (created by the Amendment Ordinance 2012), personal data held by courts, magistrates or judicial officers in the course of performing judicial functions is exempt from the provisions of all DPPs, Part 4, Part 5, and sections 36 and 38(b) of the Ordinance. Employment-related purposes Under certain circumstances, data users may be exempt from some (but not ALL) of the restrictions of the six DPPs. Sections 53, 54, 55 and 56 of the Ordinance state that personal data used for employment-related purposes is exempt from the provisions of data-access requests. DPP 6 and section 18(1)(b) of the Ordinance require data users to supply the personal data they hold to the data subject. Such data includes, for example: personal data relating to staff planning proposals; personal data which is the subject of certain evaluative processes prior to the decision being taken and where an appeal can be made against such a decision, including the processes of recruitment, promotion, awarding, removal or disciplinary action; or a personal reference for an appointment up to the time when the position is filled. Prevention or detection of crime According to section 58 of the Ordinance, personal data held for the purpose of prevention or detection of a crime may be exempt from the provisions in respect of data-access requests (DPP 6 and section 18(1)(b) of the Ordinance) and restrictions on the use of personal data (DPP 3). Health grounds Under section 59 of the Ordinance, personal data relating to the physical or mental health of a data subject is exempt from the provisions of data access requests (DPP 6 and section 18(1)(b) of the Ordinance) and restrictions on data use (DPP3) if the application of those provisions would be likely to cause serious harm to the physical or mental health of the data subject or any other individual. In addition, according to section 59(2), enacted in 2012, if the application of restrictions on data use would be likely to cause serious harm to the physical or mental health of a data subject or any other individual,

personal data relating to the identity or location of the data subject would also be exempt from DPP 3. Care and guardianship Personal data in relation to a minor which is transferred or disclosed to the minor's parent or guardian by the Hong Kong Police Force or the Customs and Exercise Department is exempt from the restrictions on personal data use (DPP 3) if the transfer or disclosure is in the interest of the minor and would facilitate proper care and guardianship of the minor. (section 59A, enacted in 2012) Legal professional privilege Under section 60, when personal data includes information about which a claim to legal professional privilege could be maintained in law, that is to say, when communication between professional legal advisers and their clients can be protected from being disclosed, such data is exempt from the data-access provisions (DPP 6 and section 18(1)(b)). Legal proceedings Under section 60B, enacted in 2012, personal data is exempt from the restrictions on the use of such data (DPP 3) if the use of the data is: required by law, authorized under law, or by court orders; required in connection with any legal proceedings in Hong Kong; or required for establishing, exercising or defending legal rights. Self-incrimination According to section 60A, a data user is exempt from complying with data-access requests under the provisions of DPP 6 and section 18(1)(b) if the user might be self-incriminated of any offence other than an offence under the Ordinance because of such compliance. In addition, information disclosed by a data user in compliance with a request under these provisions is not admissible against the user in any proceedings for an offence under the Ordinance. News activities Under section 61, if personal data is held for the purpose of news activities, such data may be exempt from the provision in respect of data-access requests (DPP 6; sections 18(1)(b), 38(i), 36 and 38(b)), unless and until the data is published or broadcast. If the data user is of the view that the disclosure of the personal data is in the public interest, then such disclosure may also be exempt from the restrictions on use (DPP 3). In an appeal case reported by the Privacy Commissioner for Personal Data (PCPD) concerning the issue of public interest in news activities, the principal of an academic institute disclosed personal data of his staff to newspaper reporters in order to defend the reputation of the institute in response to accusations made by the complainant. It was held by the PCPD that such disclosure was in the public interest in facilitating fair and balanced reporting (please refer to Complaint Case Notes for full details). Statistics and research Under section 62, personal data that is used solely to prepare statistics or carry out research is exempt from the restrictions in DPP 3, if the resulting statistics or research is not made available in a form which identifies the data subjects. Human embryos Under section 63, personal data which consists of information showing that an identifiable individual was or may have been born in consequence of a reproductive technology procedure is exempt from the provisions of DPP 6 and section 18(1)(b), provided that its disclosure under those provisions is made in accordance with section 33 of the Human Reproductive Technology Ordinance (Cap 561). Due diligence exercise Under section 63B, amended in 2012, the transfer or disclosure of personal data by a data user for the sole purpose of a due diligence exercise conducted in connection with a business merger, acquisition or transfer of business is exempt from the restrictions on use (DPP 3). Emergency situations Under section 63C, enacted in 2012, personal data is exempt from the restrictions on the collection of data (DPP 1(3)) and on the use of data (DPP 3) if the application of those provisions would be likely to prejudice the identification of an individual involved in a life-threatening situation, informing the individual's immediate family members of his situation, the carrying out of emergency rescue operations, or the provision of emergency relief services. Transfer of records to the Government Records Service Under section 63D, enacted in 2012, the personal data contained in records that are transferred to the Government Records Service is exempt from the restrictions on use (DPP 3) when the records are used by the Government Records Service solely for the purpose of appraising the records to decide whether they are to be preserved, or for organizing and preserving the records. 3. DO THE DATA PROTECTION PRINCIPLES APPLY TO THE OUTSOURCED PROCESSING OF PERSONAL DATA? 3. DO THE DATA PROTECTION PRINCIPLES APPLY TO THE OUTSOURCED PROCESSING OF PERSONAL DATA? It is an increasingly common practice for data users to outsource and entrust personal data processing to third parties. There

have also been an increasing number of personal data leakage incidents which have occurred during the outsourced processing of personal data, which may have caused substantial and irreparable damage to the affected data subjects. All the data protection principles apply to the processing of personal data by a third party. Under the Ordinance, where personal data is entrusted to a data processor, a data user is liable as the principal for any act done by its authorised data processor. The Amendment Ordinance 2012 provides enhanced protection by amending DPP 2 and DPP 4. With effect from 1 October 2012, additional obligations are imposed on a data user which engages a data processor, whether within or outside Hong Kong, to carry out data processing on that 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 necessary for processing the data (DPP2(3)) and to prevent unauthorised or accidental access, processing, erasure, loss or other inappropriate use of the data (DPP 4(2)). Under the amended Ordinance, data processor means a person who: processes personal data on behalf of another person; and does not process the data for any of the person's own purposes. Please read the PCPD's leaflet for more details on the new obligations. With the rapid advancement in information and communication technologies (ICT) and the popularization of outsourcing the processing of personal data, the collection (other than from the data subject directly) and dissemination of personal data has become much easier. This also makes it easier for data subjects to suffer damage if a person, whether or not entrusted by the data user, intentionally discloses the personal data obtained from a data user. In view of the seriousness of any intrusions into personal data privacy and the gravity of the harm that may be caused to the data subjects, the Amendment Ordinance 2012 creates a new offence to combat the disclosure of personal data obtained without the consent of the data user under certain conditions. Under section 64, it is an offence for any person to disclose any personal data of a data subject obtained from a data user without the data user's consent: with the intent to obtain gain in money or other property, whether for the benefit of the person or another person; with the intent to cause loss in money or other property to the data subject; or irrespective of his intent, with the disclosure causing psychological harm to the data subject. The maximum penalty is a fine of $1,000,000 and imprisonment for five years. Please read the PCPD's leaflet for more details on the new offence and its justification. 4. WHILE BROWSING THE INTERNET, I DISCOVER THAT MY PHOTO HAS BEEN POSTED ON A LOCAL WEBSITE WITHOUT MY CONSENT. THAT PHOTO, I BELIEVE, WAS SECRETLY TAKEN BY SOMEONE WHILE I WAS WINDOW-SHOPPING IN AN ARCADE ONE WEEK AGO. CAN I SUE THE RELEVANT WEBMASTER OR THE PHOTOGRAPHER UNDER THE PERSONAL DATA (PRIVACY) ORDINANCE? 4. WHILE BROWSING THE INTERNET, I DISCOVER THAT MY PHOTO HAS BEEN POSTED ON A LOCAL WEBSITE WITHOUT MY CONSENT. THAT PHOTO, I BELIEVE, WAS SECRETLY TAKEN BY SOMEONE WHILE I WAS WINDOW-SHOPPING IN AN ARCADE ONE WEEK AGO. CAN I SUE THE RELEVANT WEBMASTER OR THE PHOTOGRAPHER UNDER THE PERSONAL DATA (PRIVACY) ORDINANCE? The legal question to ask is whether the photograph taken amounts to "personal data". If that photograph is not personal data, then the Ordinance is not applicable in this case. With reference to a Court of Appeal case in 2000 (Eastweek Publisher Limited and another v Privacy Commissioner for Personal Data), it was ruled that personal data can be collected by means of photographs. However, it does not mean that all photographs must necessarily be personal data. In order for personal data collection to existence, the data user must be compiling information about an identified person or about a person whom the data user intends or seeks to identify. In other words, a photo merely showing a person's visual image without mentioning his/her name or other personal data (i.e. the person is only an "anonymous photographic subject") is normally not classified as personal data. As elaborated in the judgment of the above case, the Ordinance only protects the privacy of individuals in relation to personal data. It is not intended to establish general privacy rights against all possible forms of intrusion into an individual's privacy sphere (a general right to be left alone). In reply to the subject question, you cannot be protected under the Ordinance if the photo does not contain your name or other personal data. Despite the above ruling, it is important to note that persons who publish photos with captions that contain personal data of the photo subjects (without

their consent) may have violated the Ordinance. If such captions contain unjustified adverse comments on the photo subjects, the publishers may also have incurred civil liability for defamation. Furthermore, persons who take photos on such occasions (i.e. in a public place without the photo subject's consent) and cause any person to be reasonably concerned for his/her safety may have committed the offence of loitering (section 160 of the Crimes Ordinance), or may be charged with behaving in a disorderly manner in a public place. 5. WHAT ARE THE FUNCTIONS OF THE PRIVACY COMMISSIONER'S OFFICE (PCPD)? 5. WHAT ARE THE FUNCTIONS OF THE PRIVACY COMMISSIONER'S OFFICE (PCPD)? The PCPD is an independent statutory body set up to oversee the enforcement of the Personal Data (Privacy) Ordinance. The PCPD is headed by the Privacy Commissioner appointed by the Chief Executive. The commissioner's main responsibilities are to monitor and supervise compliance with the provisions of the Ordinance. This may include the investigation of complaints, the issuance of codes of practice and guidelines. For more details about the roles and duties of the PCPD, please go to the webpage of PCPD. According to section 13 of the Ordinance, a contravention of a code of practice (實務守則) approved by the PCPD does not of itself constitute a breach of the Ordinance. However, such a contravention may be used as evidence in any legal proceedings relating to the Ordinance against the relevant data user. In simple words, data users may incur civil or criminal liabilities if they have breached any provisions of the codes. CONSUMER CREDIT DATA (RELATING TO RECORDS OF ANY LOAN OR CREDIT PROVIDED BY BANKS OR FINANCIAL INSTITUTIONS) II. CONSUMER CREDIT DATA (RELATING TO RECORDS OF ANY LOAN OR CREDIT PROVIDED BY BANKS OR FINANCIAL INSTITUTIONS) The Privacy Commissioner's Office first issued a Code of Practice on Consumer Credit Data under the Ordinance in February 1998. It was revised in April 2011 . Any breach of the Code may be used as evidence in any legal proceedings relating to the Ordinance against the relevant data user. The Code governs the sharing and use of consumer credit data by credit providers (including banks and financial institutions but excluding persons who lend money to friends/relatives) through a credit reference agency ("CRA") . Under the Code, consumer credit data refer to personal data relating to an individual's consumer credit transactions collected by a credit provider in connection with the provision of consumer credit. Consumer credit generally means any loans, overdraft facilities or other kinds of credit provided by a credit provider to and for the use of an individual. Credit providers, who subscribe to the service of a CRA, may provide consumer credit data to the CRA and in return obtain credit reports (see question 1 below) of individuals for credit checking and assessment purposes. For example, when you apply for a credit card, loan or overdraft facility, hire purchase or leasing arrangement with a bank, the bank may obtain a credit report about you from a CRA. The bank makes reference to information in your credit report to assess your credit worthiness and repayment ability. If you have been granted a loan or credit facility, the bank may report your credit data to the CRA. In the event of any default in repayment, the bank may pass your credit information to a debt collection agency for collection of payment (but not for other purposes), and may also report such data to the CRA. NOTE: The above questions and answers only highlight the general points of the Code. For further information, please refer to the whole content of the Code on the PCO webpage . It is recommended that you contact the PCO or consult a lawyer if you have any queries about the Code. 1. WHAT INFORMATION WOULD BE WRITTEN ON A CREDIT REPORT? HOW CAN I CONTACT THE CREDIT REFERENCE AGENCY ("CRA") TO OBTAIN MY OWN CREDIT REPORT? 1. WHAT INFORMATION WOULD BE WRITTEN ON A CREDIT REPORT? HOW CAN I CONTACT THE CREDIT REFERENCE AGENCY ("CRA") TO OBTAIN MY OWN CREDIT REPORT? Generally speaking, a credit report would contain the following information: personal details such as the name, ID card number, address and telephone number of an individual (the data subject); information about the current and closed credit/loan accounts of the data subject (including the loan amount, repayment data and any overdue balance); information about the current and closed credit/loan accounts of the data subject (including the loan amount, repayment data and any overdue balance); records of any legal proceedings (especially about bankruptcy or debt recovery lawsuits) against the data subject. You may obtain the contact details of the relevant CRA from your bank, and then approach that CRA directly to obtain a copy of your own credit report. Under normal circumstances, you will have to pay a charge for

using this service as the Ordinance provides that a data user, in complying with a data access request (data protection principle 6), can impose a reasonable charge on the supply of the data. The major CRA operating in Hong Kong is called "TransUnion Limited". 2. WHAT CAN I DO IF I FIND OUT THAT THE INFORMATION CONTAINED IN MY CREDIT REPORT IS NOT ACCURATE? 2. WHAT CAN I DO IF I FIND OUT THAT THE INFORMATION CONTAINED IN MY CREDIT REPORT IS NOT ACCURATE? If you find any information to be inaccurate, you should first bring it to the attention of the lender/credit provider who provided the information to the CRA. Your credit provider is required to include an indication of the existence of a dispute by you on any data that it provides to the CRA (i.e. the relevant data are under dispute). Alternatively, you may make a correction request to the CRA with appropriate supporting documents. Upon receipt of your request, the CRA will promptly verify the data with your credit provider. If it does not receive from your credit provider any written confirmation or correction of the disputed data within 40 days from the correction request, the relevant data will upon expiry of the 40 days be deleted or otherwise amended as requested. If the CRA fails to respond to the data correction request, this may result in a contravention of section 23 of the Ordinance. 3. CAN CREDIT PROVIDERS OBTAIN A CREDIT REPORT ABOUT ME AT ANYTIME THEY WANT? 3. CAN CREDIT PROVIDERS OBTAIN A CREDIT REPORT ABOUT ME AT ANYTIME THEY WANT? No. A credit provider can only obtain a credit report about you in limited situations. The Code allows a credit provider to obtain your credit report when a credit provider: considers your application for a new credit facility (e.g. a new loan); conducts a credit review of your existing credit facilities; or conducts a renewal of those existing credit facilities when due. (Note: The word "review" means consideration by your credit provider of an increase or decrease in the credit amount.) Your credit provider may also obtain your credit report when you fail to repay an amount that is overdue so that it can monitor your indebtedness. However, your credit provider is not allowed to access your credit data for other purposes such as using the data for direct marketing purposes. 4. IS THERE ANY INFORMATION (ABOUT A BORROWER/DEBTOR) THAT A CREDIT PROVIDER MUST NOT REPORT TO A CRA? 4. IS THERE ANY INFORMATION (ABOUT A BORROWER/DEBTOR) THAT A CREDIT PROVIDER MUST NOT REPORT TO A CRA? A credit provider must not disclose account data about a person's residential mortgage loan (unless that person has defaulted in repayment for a period in excess of 60 days) to a CRA. Also, a credit provider must not disclose non-credit based information such as income, bank deposits, other assets or employment information. 5. IF I ACT AS A GUARANTOR FOR MY FRIEND'S LOAN FROM A BANK, WILL THE BANK DISCLOSE MY ROLE AS A GUARANTOR TO A CRA? DOES THE CODE ALSO COVER THE SCENARIO OF AN INDIVIDUAL BEING THE GUARANTOR FOR A CORPORATE LOAN? 5. IF I ACT AS A GUARANTOR FOR MY FRIEND'S LOAN FROM A BANK, WILL THE BANK DISCLOSE MY ROLE AS A GUARANTOR TO A CRA? DOES THE CODE ALSO COVER THE SCENARIO OF AN INDIVIDUAL BEING THE GUARANTOR FOR A CORPORATE LOAN? Yes, the bank may report this information to a CRA. A credit provider may provide credit data collected from the borrower to a CRA. These credit data will include information regarding the borrower and the guarantor (if any). The definition of "consumer credit" under the Code makes reference to the user of the facility, i.e. whether it is granted to and for the use of an individual, or to and for the use of another person for whom an individual acts as a guarantor. As the meaning of the word "person" includes not only a natural person but also a legal person (e.g. a limited company), a corporate loan guaranteed by an individual will thus fall within the definition of "consumer credit" under the Code. 6. IS IT COMPULSORY FOR CREDIT PROVIDERS TO PROVIDE ALL OF AN INDIVIDUAL'S (BORROWER OR GUARANTOR) LOAN ACCOUNT INFORMATION TO A CRA? 6. IS IT COMPULSORY FOR CREDIT PROVIDERS TO PROVIDE ALL OF AN INDIVIDUAL'S (BORROWER OR GUARANTOR) LOAN ACCOUNT INFORMATION TO A CRA? Going back to question 4, account data relating to a residential mortgage loan is specifically excluded from provision to the CRA, unless such account data reveal a currently outstanding material default (the mortgage repayment is overdue for more than 60 days). In the case of such a default, the credit provider may give the CRA data relating to the material default together with the account general data. However, there is no mandatory requirement to report credit data under the Code (clause 2.4 of the Code says: ".....it may thereafter provide to a CRA any of the following items of consumer credit data....."). It is

entirely a matter for the credit provider and the CRA to agree among themselves on what types of loan products will be subject to what data requirements, provided that they stay within the boundaries of the Code. The Code sets the rules on what can or cannot be provided and shared in respect of consumer credit data and the provisions which should be followed by credit providers so that they are in compliance with the Ordinance. 7. HOW LONG CAN A CRA RETAIN MY CREDIT DATA? IF I SETTLE MY LOAN ACCOUNT, WILL MY CREDIT DATA HELD BY A CRA BE DELETED FROM ITS DATABASE? 7. HOW LONG CAN A CRA RETAIN MY CREDIT DATA? IF I SETTLE MY LOAN ACCOUNT, WILL MY CREDIT DATA HELD BY A CRA BE DELETED FROM ITS DATABASE? A CRA can retain your personal particulars and account general data for credit reporting purposes as long as you have a borrowing relationship with a credit provider. The general rule on data retention is that account repayment data may be retained for 5 years from the date of the creation of such data, or until the expiry of a period of 5 years from the date of the termination of the account. However, there are certain exceptions. For example, if you have defaulted on repayment for a period in excess of 60 days, then account data relating to the default may be retained for a period of 5 years following the date on which the amount in default was fully settled. (Note: "Account general data" include the loan amount/credit limit, identity of the credit provider, and the dates on which the account was opened & closed. "Account repayment data" include the amount of payment made during the last reporting period, the outstanding balance, and any amount past due (overdue amount). For more details, please refer to schedule 2 of the Code issued by the PCO.) When you settle your loan account, you have the right to instruct your credit provider to make a request to the CRA to delete the closed account data from its database. Your credit provider should have informed you of this right at the time when you applied for the loan. Alternatively, you should receive a written reminder from that company upon your settlement of the account. However, you should note that the right to request deletion of the data is conditional upon there having been, within the 5 years immediately before the termination of the account, no default in repayment lasting for a period of more than 60 days, AND the account having been settled by full repayment. You should also note that your credit provider may at its own discretion retain your closed account data in its own system for internal accounting purposes even though you have requested deletion of the data from the CRA's database. 8. IS THERE ANY BENEFIT TO KEEPING MY CLOSED ACCOUNT DATA IN THE CRA'S DATABASE? 8. IS THERE ANY BENEFIT TO KEEPING MY CLOSED ACCOUNT DATA IN THE CRA'S DATABASE? If you settled your loan account with no record of late repayments, its record can provide you with a good credit history, and you may wish to retain it in the CRA database. If you subsequently apply for loans from other banks, your closed account information (with no record of late repayments) can put you in a stronger position to negotiate better terms of credit. 9. IF I HAD A TAX LOAN WITH A BANK THAT I FULLY REPAID BEFORE THE EFFECTIVE DATE OF THE CODE, AND I HAVE HAD A CREDIT CARD WITH THE SAME BANK FOR MANY YEARS. CAN MY BANK PROVIDE DATA CONCERNING THESE ACCOUNTS TO THE CRA AFTER THE CODE HAS TAKEN EFFECT? 9. SUPPOSE I HAD A TAX LOAN WITH A BANK THAT I FULLY REPAID IN JANUARY 2003 (BEFORE THE EFFECTIVE DATE OF THE CODE). I ALSO HAVE A CREDIT CARD WITH THE SAME BANK FOR MANY YEARS UP TO NOW. CAN MY BANK PROVIDE DATA CONCERNING ALL THESE ACCOUNTS TO THE CRA AFTER THE CODE HAS TAKEN EFFECT ON 2 JUNE 2003? Now that the Code has taken effect on 2 June 2003, your bank may provide the CRA with data regarding any account (credit or loan account) which involves a current borrowing relationship, even if there is no default in repayment. However, the bank is not allowed to report data relating to any account that had been settled by full repayment prior to the effective date. As regards an account that remains active after the effective date, the bank cannot report past repayment data (that existed prior to the effective date) unless there is a current outstanding default on the account, in which case, the bank can report such default data. (Note: "Current outstanding default" means an overdue amount that has not yet been settled.) In your case, since you fully repaid your tax loan before 2 June 2003, the bank is not allowed to report the loan account data to the CRA. As regards your credit card account, provided you have no current outstanding default in any repayment, your past payment transactions (that occurred before the effective date) will not be reported by your bank. However, if you only made the minimum repayment according to the monthly credit

card statements before the effective date, the remaining portion after each monthly due date may be considered as default data. Subject to the terms of agreement between you and the bank, the bank may be permitted to report such data to the CRA. 10. IF I DECLARE BANKRUPTCY, WILL MY CREDIT DATA HELD BY A CRA BE DELETED FROM ITS DATABASE? WHAT IF I DO NOT DECLARE BANKRUPTCY BUT HAVE ENTERED INTO AN INDIVIDUAL VOLUNTARY ARRANGEMENT (IVA, A DEBT REPAYMENT SCHEME RECOGNIZED BY THE COURT) WITH MY CREDITORS? 10. IF I DECLARE BANKRUPTCY, WILL MY CREDIT DATA HELD BY A CRA BE DELETED FROM ITS DATABASE? WHAT IF I DO NOT DECLARE BANKRUPTCY BUT HAVE ENTERED INTO AN INDIVIDUAL VOLUNTARY ARRANGEMENT (IVA, A DEBT REPAYMENT SCHEME RECOGNIZED BY THE COURT) WITH MY CREDITORS? Your declaration of bankruptcy is made available in official public records (you may go to the topic of bankruptcy and winding-up for more information). A CRA may collect this type of information from public sources for credit reporting purposes. The Code provides that public record data relating to a declaration of bankruptcy may be retained for a period of 8 years from the relevant declaration of bankruptcy. Concerning an Individual Voluntary Arrangement (in which the debtor does not declare bankruptcy), the CRA may collect such public record data and retain the data for a period of 7 years from the date of the IVA. If you strictly comply with the repayment proposal as agreed in the IVA, the relevant account repayment data will be deleted from the CRA's record upon the expiry of a period of 5 years from the date of the final settlement of the debt. You should note that, despite the fact that your credit provider might have written off your defaulted accounts pursuant to your bankruptcy, the CRA could continue to retain the account repayment data relating to your defaulted accounts so long as you have not settled the amount in default. It is incumbent upon you to provide evidence of your discharge from bankruptcy (either a certificate of discharge issued by the Court of First Instance of the High Court, or a written notice from the Official Receiver) to the CRA. If you can provide such evidence, the CRA will delete such account repayment data upon the expiry of a period of 5 years from the date of your discharge. 11. ARE THERE ANY SAFEGUARDS TO PROTECT MY CREDIT DATA AGAINST IMPROPER ACCESS BY CREDIT PROVIDERS? 11. ARE THERE ANY SAFEGUARDS TO PROTECT MY CREDIT DATA AGAINST IMPROPER ACCESS BY CREDIT PROVIDERS? Credit providers and credit reference agencies are governed by the Code and the Ordinance. Under the Code, each time a credit provider accesses a CRA's credit reference database, the credit provider is required to inform the CRA of the reasons and circumstances under which the access has been made. The CRA is required to maintain a record of all access to its database by credit providers. In the event of there being any suspected abnormal access by a credit provider, the CRA is required to report such incident to the senior management of that credit provider and the Privacy Commissioner. To ensure compliance with the requirements of the Code, the CRA is required to conduct a compliance audit at intervals not exceeding 12 months and to submit an audit report for consideration by the Privacy Commissioner. 12. WHAT CAN I DO IF I FIND OUT THAT A CREDIT PROVIDER OR A CRA IS NOT HANDLING MY DATA PROPERLY? 12. WHAT CAN I DO IF I FIND OUT THAT A CREDIT PROVIDER OR A CRA IS NOT HANDLING MY DATA PROPERLY? Improper handling of credit data may arise from the release of data to the wrong persons, the failure to accede to a data access or a data correction request made by the data subject, or failure to take proper security measures to protect the data, etc. If you are unable to resolve the matter with the credit provider or the CRA concerned, you may make a complaint in writing to the PCO. For details about the complaint procedures and the possible penalties, please go to Part VII. 13. ENQUIRY CASE NOTES FROM THE PCO - SHOULD THE BANK NOTIFY ME (AS THE GUARANTOR OF A LOAN FACILITY) IF MY CREDIT REPORT IS ACCESSED WHEN (I) THE LOAN FACILITY IS APPLIED FOR; AND (II) WHEN THE EXISTING LOAN FACILITY IS REVIEWED? 13. ENQUIRY CASE NOTES FROM THE PCO - SHOULD THE BANK NOTIFY ME (AS THE GUARANTOR OF A LOAN FACILITY) IF MY CREDIT REPORT IS ACCESSED WHEN (I) THE LOAN FACILITY IS APPLIED FOR; AND (II) WHEN THE EXISTING LOAN FACILITY IS REVIEWED? WHAT IF I AM THE ACTUAL ACCOUNT HOLDER INSTEAD? Please read the answer provided by the PCO website. 14. BY REQUEST OF A LAW FIRM WHICH ACTS FOR THE ADMINISTRATOR OF A DECEASED PERSON, IF A BANK DISCLOSES RECORDS OF THE DECEASED ALSO CONTAIN INFORMATION OF THIRD PARTIES, IS SUCH DISCLOSURE A CONTRAVENTION OF THE ORDINANCE? 14. ENQUIRY CASE NOTES FROM THE PCO - A BANK HAS RECEIVED A LETTER FROM A FIRM OF SOLICITORS ACTING FOR THE ADMINISTRATOR OF THE

ESTATE OF A DECEASED PERSON. THE BANK IS REQUESTED TO DISCLOSE CERTAIN RECORDS IN RELATION TO ACCOUNTS WHICH ARE IN THE NAME OF THE DECEASED. HOWEVER THE RECORDS ALSO INCLUDE INFORMATION RELATING TO THIRD PARTIES. IS SUCH DISCLOSURE A CONTRAVENTION OF THE ORDINANCE? Please read the answer provided by the PCO website. USE OF ID CARD NUMBERS AND ID CARD COPIES III. USE OF ID CARD NUMBERS AND ID CARD COPIES The Code of Practice on the Identity Card Number and other Personal Identifiers and its compliance guide for data users (issued by the Privacy Commissioner's Office) came into force on 19 December 1998 . Any breach of the Code may be used as evidence in any legal proceedings relating to the Ordinance against the relevant data user. The Code gives practical guidance to data users on the application of the Ordinance in relation to the collection, accuracy, retention, use and security of: (a) identity card ("ID card") numbers and copies of ID cards; and (b) other personal identifiers that uniquely identify individuals, e.g. passport numbers, employee/staff numbers, examination candidate numbers and patient numbers. Where a data user has collected an ID card number or copy of an ID card for a purpose allowed under the Code, the data should generally be used ONLY for that purpose. The records of ID card numbers or ID card copies should not be kept for longer than is necessary to fulfill the purpose for which they were collected. Data users should also implement adequate security safeguards for data that they hold or transmit. Specifically, the Code requires that a copy of an ID card in paper form should be marked "copy" across the image of the ID card. Records of ID card numbers and ID card copies should also be treated as confidential documents which should be kept in locked cabinets or secure areas when they are not in use. Due to advances in easy-to-use technology and lower costs, fingerprint data for personal identification has been put to use for purposes other than the investigation of crime. To regulate the use of this sensitive personal data, the Commissioner revised the note entitled Guidance on Collection of Fingerprint Data in May 2012. NOTE: The above questions and answers only highlight the general points of the Code. For further information, please refer to the whole content of the Code on the PCPD webpage . It is recommended that you contact the PCPD or consult a lawyer if you have any queries about the Code. 1. GENERALLY SPEAKING, UNDER WHAT CIRCUMSTANCES CAN A PERSON ASK ME TO PROVIDE MY ID CARD NUMBER OR ID CARD COPY? 1. GENERALLY SPEAKING, UNDER WHAT CIRCUMSTANCES CAN A PERSON ASK ME TO PROVIDE MY ID CARD NUMBER OR ID CARD COPY? ID card number Unless authorized by law, no data user may compel an individual to provide his or her ID card number. A data user may request an individual to provide his or her ID card number under the circumstances where the collection of the ID card number is permitted by the Code. The following list contains some daily examples (this is not an exhaustive list): Where there is an Ordinance which requires data users to collect ID card numbers, e.g. section 17K of the Immigration Ordinance (Cap. 115) requires employers to keep a record of the number of the document, which is usually an ID card, by virtue of which each employee is lawfully employable. Where the use of the ID card number is necessary for any of the purposes mentioned in section 58(1) of the Ordinance, which includes the prevention or detection of crime, and the assessment or collection of any tax or duty. To enable the data user to identify the individual concerned or to attribute data to him or her where any of the following is necessary: to advance the interests of the individual, e.g. to ensure that the correct medical record is referred to when treating a patient; to prevent any third party other than the data user from suffering a detriment, e.g. to ensure that someone else is not given the wrong medication because the wrong medical record is referred to; to enable the data user to safeguard against damage or loss that is more than trivial, e.g. drivers involved in a traffic accident may exchange ID card number in order to identify each other when pursuing a claim arising from the accident. For inclusion in a document that establishes or is evidence of any legal or equitable right or interest or legal liability that is not trivial, e.g. in documents that establish an individual's right of ownership of a flat. As the means of future identification of an individual who is permitted to enter premises where monitoring of the activities of the individual inside the premises is not reasonably practicable, e.g. entry to a commercial building outside office hours. As a condition for allowing an individual to have custody or control of property which is of a value that is more than trivial, e.g. rent a flat or car. ID card

copy Again, no data user may compel an individual to provide a copy of his or her ID card unless authorized by law. A data user may request an individual to provide a copy of his or her ID card under the circumstances where the collection of the copy is permitted by the Code. The following list contains some daily examples (this is not an exhaustive list): To carry out any of the purposes mentioned in section 58(1) of the Ordinance, which includes the prevention or detection of crime, and the assessment or collection of any tax or duty. To provide proof of compliance with any statutory requirement, e.g. an employer may collect a copy of an ID card to prove compliance with the requirement of section 17J of the Immigration Ordinance (Cap.115) to inspect the ID card of an individual when the employer intends to confirm the employment of that person. To comply with a requirement to collect an ID card copy which is included in any code, rules, regulations or guidelines applicable to the data user and which requirement has been endorsed in writing by the Privacy Commissioner, e.g. banks may collect copies of the ID cards of their customers according to the Money Laundering Guidelines issued by the Hong Kong Monetary Authority. To collect or check the ID card number of the individual, but only if the individual has been given the choice of presenting his or her ID card in person instead (e.g. Transport Department is permitted to collect copies of ID cards for this purpose in relation to applications for driving licences made by post, as individuals are given the choice of presenting their ID cards in person). For the issuing of an officially recognised travel document, e.g. the BN(O) passport. Collection of copies of ID cards is specifically NOT permitted in the Code under the following circumstances: merely to safeguard against a clerical error in recording the name or ID card number of the individual (i.e. the copy should not be collected in order only to enable the person to check the accuracy of the record that has been made of the individuals name or ID card number); or merely in anticipation of a prospective relationship with the individual (e.g. it would not be permissible for an employer to collect a copy of the ID card of an individual only because the employer may wish to offer him or her employment at a later stage). 2. CAN THE SECURITY STAFF OF A BUILDING ASK ME TO ENTER MY ID CARD NUMBER IN A VISITORS' LOG BOOK AT THE ENTRANCE OF A BUILDING? 2. CAN THE SECURITY STAFF OF A BUILDING ASK ME TO ENTER MY ID CARD NUMBER IN A VISITORS' LOG BOOK AT THE ENTRANCE OF A BUILDING? This depends on whether the monitoring of your activities inside the building is feasible or not (e.g. is it feasible to arrange a security guard to accompany you inside the building). If this is feasible, the security staff should not collect your ID card number. If such monitoring is not feasible, they are allowed to collect your ID card number. However, the security staff should take appropriate security measures to ensure that such entries in a visitors' log book are concealed from subsequent visitors who enter their details. If you are unwilling to provide your ID card number, you can suggest other alternatives. Examples of such alternatives include identification by another identification document (e.g. a staff card), or identification by someone known to the security staff (e.g. by a resident in the case of a residential building). It is recommended by the Privacy Commissioner's Office that in normal circumstances, entries in the visitor log book can be retained for a period of not more than one month. If there are any valid grounds justifying a longer retention period (e.g. where the records are required for evidentiary purposes or to assist a police investigation of detected or reported unlawful activities), the security staff can retain the data for more than one month. For more guidelines on this matter, please refer to the PCO's publication "Personal Data Privacy: Guidance on Property Management Practices". 3. CAN A POLICE OFFICER ASK ME TO SHOW HIM/HER MY ID CARD? 3. CAN A POLICE OFFICER ASK ME TO SHOW HIM/HER MY ID CARD? A request to show your ID card, without the requester making a record of any information on the card, is not covered by the Code. Generally, however, if police officers or other public officers (e.g. an immigration officer) ask to record your ID card number in your dealings with them, you should let them do so, as these officers have statutory powers to require individuals to furnish their ID card numbers in dealings with the Government. For further information about the power the police have to check ID cards, please go to another topic - Police and Crime. 4. CAN A PROSPECTIVE EMPLOYER RECORD MY ID CARD NUMBER OR COLLECT A COPY OF MY ID CARD WHEN I ATTEND A JOB INTERVIEW? 4. CAN A PROSPECTIVE EMPLOYER RECORD MY ID

CARD NUMBER OR COLLECT A COPY OF MY ID CARD WHEN I ATTEND A JOB INTERVIEW? In order to check whether you have applied for or held a position in the company before, the prospective employer can collect your ID card number. However, a copy of your ID card should not be collected unless and until you become an employee of that company. As regards the retention of personal data of unsuccessful job applicants, please refer to the relevant question and answer. 5. IF I HAVE ACCEPTED AN EMPLOYMENT OFFER, CAN MY EMPLOYER COLLECT A COPY OF MY ID CARD? 5. IF I HAVE ACCEPTED AN EMPLOYMENT OFFER, CAN MY EMPLOYER COLLECT A COPY OF MY ID CARD? Yes, as a copy of your ID card is evidence of your employer's compliance with the requirements of the Immigration Ordinance to inspect your ID card before employing you. However, companies are required by the Code to mark the word "copy" across the image of copies of ID cards to reduce the chance for misuse and abuse. 6. CAN A CLUB ASK ME TO PROVIDE MY ID CARD NUMBER AND A COPY OF MY ID CARD IF I APPLY TO BE A MEMBER? 6. CAN A CLUB ASK ME TO PROVIDE MY ID CARD NUMBER AND A COPY OF MY ID CARD IF I APPLY TO BE A MEMBER? Generally speaking, collection of ID card numbers of its members by a membership club may be permitted under the Code to enable the club management to check membership. However, there appears to be no justification to collect copies of members' ID cards. 7. CAN COMPANIES PROVIDING MOBILE PHONE SERVICES RECORD MY ID CARD NUMBER OR COLLECT A COPY OF MY ID CARD IF I APPLY FOR THEIR SERVICES? 7. CAN COMPANIES PROVIDING MOBILE PHONE SERVICES RECORD MY ID CARD NUMBER OR COLLECT A COPY OF MY ID CARD IF I APPLY FOR THEIR SERVICES? These companies operate on the basis of deferred payment (i.e. customers are usually required to make monthly payment after using their services). Hence, they require a means of proving the identity of their customers in order to obtain payment. Moreover, they face the problem that the services concerned are not provided to a fixed location. On the other hand, there have been a number of reported cases of individuals fraudulently obtaining such services using another person's name and address, and of the salespersons opening accounts for fictitious persons to defraud their company. For these reasons, the collection of the ID card numbers and copies of the ID cards is generally justified under the Code. However, these companies should mark the word "copy" across the image of the copies. 8. CAN BANKS/INSURANCE COMPANIES COLLECT A COPY OF MY ID CARD WHEN I APPLY TO BE THEIR CUSTOMER? 8. CAN BANKS/INSURANCE COMPANIES COLLECT A COPY OF MY ID CARD WHEN I APPLY TO BE THEIR CUSTOMER? Yes, because they are required to do this under the guidelines issued by the relevant regulatory bodies. These requirements have been endorsed by the Privacy Commissioner. However, the word "copy" should be marked across the image of the copies of their customers' ID cards. 9. WHAT SHOULD I BE AWARE OF BEFORE I PROVIDE MY ID CARD NUMBER OR ID CARD COPY TO OTHER PERSONS? 9. WHAT SHOULD I BE AWARE OF BEFORE I PROVIDE MY ID CARD NUMBER OR ID CARD COPY TO OTHER PERSONS? The Code requires organizations or persons (the data users), before recording an ID card number, to consider alternatives that are less privacy intrusive. If you are not happy about a request to provide your ID card number, suggest to the requestor/data user alternatives that are reasonable and acceptable to you. For example, try to arrange for identification of yourself by someone else who is already known to the organization. An organization may be contravening the Code if it refuses to accept an alternative without a good explanation . Compared to ID card numbers, stricter limits are imposed on the collection of ID card copies because of the greater dangers they carry in relation to possible fraud or other misuse. Generally speaking, this gives you greater justification in querying a request to provide a copy of your ID card. The Code generally requires the data users to mark photocopies of ID cards they keep with the word "copy". This marking should be made across the entire image of the ID card. The only exception to this marking requirement you are likely to encounter is where the photocopy is going to be converted into some other form, e.g. microfilm. If you provide a photocopy of your ID card in person to a data user, you can insist that it must be marked "copy" in your presence. Unless otherwise required or permitted by law, data users should ensure that an ID card number and the name of the holder are not displayed together publicly. One common situation in which a breach of the above requirement may occur is the publication of notices including individuals' names and ID card numbers in a newspaper (e.g. notices carrying the result of a lucky draw or a competition). Another is the display of notices containing individuals' names

and ID card numbers on a notice board in places such as a school, an office, or the lobby of a residential building. A further one is the inadvertent disclosure of the names and ID card numbers of visitors to subsequent visitors to a building in a visitors' log-book. Where you encounter a situation such as those described above, ask the organization/data user to stop displaying or disclosing those data (or else to justify the display/disclosure). An organization is likely to have contravened the Code if it cannot provide good justification. 10. UNDER WHAT CIRCUMSTANCES CAN A PERSON ASK ME TO PROVIDE OTHER PERSONAL IDENTIFIERS (E.G. STAFF NUMBER, PASSPORT NUMBER OR PATIENT NUMBER)? 10. UNDER WHAT CIRCUMSTANCES CAN A PERSON ASK ME TO PROVIDE OTHER PERSONAL IDENTIFIERS (E.G. STAFF NUMBER, PASSPORT NUMBER OR PATIENT NUMBER)? In general, the requirements of the Code in relation to ID card numbers also apply to other personal identifiers. In other words, other personal identifiers may be collected only under the circumstances and by the means permitted for ID card numbers and are subject to similar requirements as regards retention and use. However, the above does not apply to the collection or use of such other personal identifiers for a purpose that is directly related to the functions and activities of the person that assigned the identifier to the individuals concerned. For example, a staff number may be collected and used for purposes directly related to the functions or activities of the employer that assigned the number, such as managing employee records and the payment of employee salaries. Data users that assign personal identifiers to individuals should take all reasonably practicable steps to ensure the security of the system under which this is done. Such steps should include security measures to safeguard against the unauthorized assignment of the identifier or production of any document (e.g. the unauthorized production of a staff card with a false staff number printed on it). 11. COMPLAINT CASE NOTES FROM THE PCPD - A PROPERTY MANAGEMENT COMPANY COLLECTED IDENTITY CARD NUMBERS OF RESIDENTS WHO WERE APPLYING FOR ELECTRONIC ENTRANCE CARDS GAINING ACCESS TO THE BUILDING. IS THIS VIEWED AS AN EXCESSIVE COLLECTION OF PERSONAL DATA? 11. COMPLAINT CASE NOTES FROM THE PCPD - A PROPERTY MANAGEMENT COMPANY COLLECTED IDENTITY CARD NUMBERS OF RESIDENTS WHO WERE APPLYING FOR ELECTRONIC ENTRANCE CARDS GAINING ACCESS TO THE BUILDING. IS THIS VIEWED AS AN EXCESSIVE COLLECTION OF PERSONAL DATA? Please read the answer provided by the PCPD website. 12. COMPLAINT CASE NOTES FROM THE PCPD - A PERSON REQUESTED A REFUND OF A TOUR FEE AND CHARGES FROM A TRAVEL SERVICE AGENT. IN PROCESSING THE REQUEST, THE TRAVEL AGENT REQUIRED HIM TO PROVIDE A PHOTOCOPY OF HIS HONG KONG IDENTITY CARD. IS THIS VIEWED AS AN EXCESSIVE COLLECTION OF PERSONAL DATA? 12. COMPLAINT CASE NOTES FROM THE PCPD - A PERSON REQUESTED A REFUND OF A TOUR FEE AND CHARGES FROM A TRAVEL SERVICE AGENT. IN PROCESSING THE REQUEST, THE TRAVEL AGENT REQUIRED HIM TO PROVIDE A PHOTOCOPY OF HIS HONG KONG IDENTITY CARD. IS THIS VIEWED AS AN EXCESSIVE COLLECTION OF PERSONAL DATA? Please read the answer provide by the PCPD website. PRIVACY IN RECRUITMENT, HUMAN RESOURCES MANAGEMENT AND AT WORK IV. PRIVACY IN RECRUITMENT, HUMAN RESOURCES MANAGEMENT AND AT WORK The Privacy Commissioner's Office has issued a Code of Practice on Human Resource Management which came into force on 1 April 2001. The Code is designed to give practical guidance to data users who handle personal data in performing human resource management actives (such as recruitment, management of personal data of current and former employees, etc.). Any breach of the Code may be used as evidence in any legal proceedings relating to the Ordinance against the relevant data users. In that case, individuals (employees) will also benefit from reading the Code in order to understand more about their legal rights concerning personal data protection. To provide more information about this topic, the PCPD issued the Privacy Guidelines: Monitoring and Personal Data Privacy at Work in December 2004. Although these guidelines are not legally binding, they are made with reference to the Six Data Protection Principles of the Ordinance and therefore have substantial reference value. The guidelines list out some recommended steps that should be taken by employers when they monitor employees using the following means: Telephone Monitoring (telephone calls and voice mail made or received by employees); E-mail Monitoring (employees' incoming and outgoing e-mail messages); Internet Monitoring (employees' web browsing activities); Video Monitoring (using video cameras or closed circuit TV system ("CCTV") to monitor or record employees' work activities and behaviours). With regard to the employment of domestic

helpers, the PCPD also issued the document Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers in December 2004. It contains points that are related to video monitoring of activities of domestic helpers working at home. It is pertinent to note that employers must not disclose their employees' employment-related data to a third party without first obtaining the employees' consent, unless the disclosure is for purposes directly related to their employment, or such disclosure is required by law or by statutory authorities (e.g. for tax assessment/collection purposes or criminal investigation). NOTE: You should contact the PCPD or consult a lawyer if you have any queries about these Codes or Guidelines. 1. WHAT IS A "BLIND" RECRUITMENT ADVERTISEMENT? DOES THE CODE OF PRACTICE ON HUMAN RESOURCE MANAGEMENT APPLY TO ALL RECRUITMENT ADVERTISEMENTS? 1. WHAT IS A "BLIND" RECRUITMENT ADVERTISEMENT? DOES THE CODE OF PRACTICE ON HUMAN RESOURCE MANAGEMENT APPLY TO ALL RECRUITMENT ADVERTISEMENTS? A "blind" recruitment advertisement is one that does not identify either the employer or the employment agency acting on its behalf. The Code only applies to recruitment advertisements that directly solicit personal data from job applicants. Under the Code, an employer or the employment agency acting on its behalf is not permitted to place a "blind" recruitment advertisement that directly invites job applicants to submit their résumés or CVs. Where there is no direct solicitation of personal data in a recruitment advertisement, such an advertisement would not be subject to the requirements of the Code. For example, if the advertisement merely invites job seekers to write in to obtain an application form or contact a representative person, there is no direct solicitation of personal data. On the other hand, an employer or recruitment agency who clearly indicates its identity (the company name) in a recruitment advertisement can ask job applicants to submit personal data, provided that the data requested are adequate but not excessive in relation to recruitment purposes and are to be used lawfully. 2. WHY IS AN EMPLOYER REQUIRED TO IDENTIFY ITSELF IN RECRUITMENT ADVERTISEMENTS THAT SOLICIT PERSONAL DATA FROM JOB APPLICANTS? 2. WHY IS AN EMPLOYER REQUIRED TO IDENTIFY ITSELF IN RECRUITMENT ADVERTISEMENTS THAT SOLICIT PERSONAL DATA FROM JOB APPLICANTS? An employer, who collects personal data from job applicants without identifying itself (or an appointed recruitment agency) might have engaged in an act of unfair collection of personal data contrary to the requirement of data protection principle 1. It would generally not be fair for persons collecting personal data not to identify themselves when collecting data. Secondly, personal data collected from job applicants are subject to access and correction by the person concerned (data protection principle 6). Unless exempted from doing so under the Ordinance, an employer is required to provide a copy of the data no later than 40 days after receiving a data access request. Job applicants would not be able to exercise their data access rights if they don't know the identity of the company that collected their personal data. 3. CAN AN EMPLOYER DIRECTLY SOLICIT PERSONAL DATA FROM JOB APPLICANTS IF IT MERELY USES ITS COMPANY EMAIL ADDRESS, TELEPHONE NUMBER OR FAX NUMBER AS A MEANS OF IDENTIFYING ITSELF IN A RECRUITMENT ADVERTISEMENT? 3. CAN AN EMPLOYER DIRECTLY SOLICIT PERSONAL DATA FROM JOB APPLICANTS IF IT MERELY USES ITS COMPANY EMAIL ADDRESS, TELEPHONE NUMBER OR FAX NUMBER AS A MEANS OF IDENTIFYING ITSELF IN A RECRUITMENT ADVERTISEMENT? No. A company email address, telephone number or fax number by itself is generally not considered to be sufficient identification of the employer. If the employer does not wish to disclose its identity, it may simply provide a telephone number in the advertisement and indicate that the applicants can make further enquiries before submitting any personal data. 4. SOME EMPLOYERS ONLY PROVIDE THEIR FAX NUMBERS, POSTAL ADDRESSES OR E-MAIL ADDRESSES IN RECRUITMENT ADVERTISEMENTS WITHOUT EXPLICITLY ASKING JOB APPLICANTS TO SUBMIT THEIR PERSONAL DATA. IS THIS PRACTICE ACCEPTABLE UNDER THE CODE? 4. SOME EMPLOYERS ONLY PROVIDE THEIR FAX NUMBERS, POSTAL ADDRESSES OR E-MAIL ADDRESSES IN RECRUITMENT ADVERTISEMENTS WITHOUT EXPLICITLY ASKING JOB APPLICANTS TO SUBMIT THEIR PERSONAL DATA. IS THIS PRACTICE ACCEPTABLE UNDER THE CODE? No. The practice of employers providing fax numbers, postal addresses or e-mail addresses in recruitment advertisements is perceived as a way of inviting job applicants to submit their personal data. This is not permissible under the provisions of the Code. 5. SHOULD AN EMPLOYER PROVIDE, WITHIN A RECRUITMENT ADVERTISEMENT, A STATEMENT REGARDING THE PURPOSE FOR WHICH THE PERSONAL DATA

SUBMITTED BY JOB APPLICANTS WILL BE USED? 5. SHOULD AN EMPLOYER PROVIDE, WITHIN A RECRUITMENT ADVERTISEMENT, A STATEMENT REGARDING THE PURPOSE FOR WHICH THE PERSONAL DATA SUBMITTED BY JOB APPLICANTS WILL BE USED? Recruitment advertisements that directly ask job applicants to provide their personal data should include a statement, as an integral part of the advertisement, informing applicants about the purposes for which their personal data are to be used. Here is an example of such statement: "Personal data collected will be used for recruitment purposes only". Alternatively, a statement to the following effect may be included: "Personal data provided by job applicants will be used strictly in accordance with the employer's personal data policies, a copy of which will be provided immediately upon request." In this case, contact information for the employer should be stated in the advertisement. If you want to obtain an example of an employer's personal data policies relating to recruitment (or called "Personal Information Collection Statement"), please refer to Annex A of the Compliance Guide for Employers and HRM Practitioners issued by the PCO. 6. CAN AN EMPLOYER ASK JOB APPLICANTS WHETHER THEY HAVE ANY CRIMINAL RECORD? 6. CAN AN EMPLOYER ASK JOB APPLICANTS WHETHER THEY HAVE ANY CRIMINAL RECORD? Data protection principle 1 stipulates that only personal data that are necessary for the purposes for which the data are to be used should be collected. Further, it requires that the data collected should be adequate for those purposes, but not excessive. No hard and fast rules have been laid down as to what data are necessary for human resources management purposes and what are not. This will depend on the facts of the individual case. For some jobs, it may be necessary to ask whether or not an applicant has a criminal record (e.g. where the employment position involves the control of valuable items, or to undertake a treasury position). In deciding whether it is necessary to collect a particular piece of information, data users should carefully consider whether the purpose for which the data are being collected could still be satisfied if such data are not collected. For more information about criminal records, please go to another topic – Police and Crime. 7. ON A COMPANY'S JOB APPLICATION FORM, THERE IS A COLUMN REQUESTING PERSONAL DATA CONCERNING THE APPLICANT'S SPOUSE/CHILDREN'S OCCUPATIONS. THE PURPOSE OF THIS IS TO ASCERTAIN WHETHER THE RELATIVES WORK FOR ONE OF ITS COMPETITORS. IS THIS ACCEPTABLE? 7. ON A COMPANY'S JOB APPLICATION FORM, THERE IS A COLUMN REQUESTING PERSONAL DATA CONCERNING THE APPLICANT'S SPOUSE/CHILDREN'S OCCUPATIONS. THE PURPOSE OF THIS IS TO ASCERTAIN WHETHER THE RELATIVES WORK FOR ONE OF ITS COMPETITORS. IS THIS ACCEPTABLE? The test is whether the data collected are necessary to fulfill the employer's purpose of ascertaining whether relatives of the job applicant work for a competitor. To find this out, it is only necessary to ask whether or not the applicant's relatives work in the same or a similar field. If they do, further questions could be asked to ascertain whether this should be a source of concern. But if they do not, the employer does not need to know what their actual occupations are, and hence the employer should not collect this information. 8. CAN AN EMPLOYER COLLECT COPIES OF THE IDENTITY CARDS OF JOB APPLICANTS? HOW LONG IS AN EMPLOYER ALLOWED TO KEEP THE PERSONAL DATA OF UNSUCCESSFUL JOB APPLICANTS? 8. CAN AN EMPLOYER COLLECT COPIES OF THE IDENTITY CARDS OF JOB APPLICANTS? HOW LONG IS AN EMPLOYER ALLOWED TO KEEP THE PERSONAL DATA OF UNSUCCESSFUL JOB APPLICANTS? Generally speaking, an employer must not collect a copy of the identity card of a job applicant during the recruitment process unless and until the individual has accepted an offer of employment. Personal data of unsuccessful applicants (for future recruitment purposes) can be retained for a period of up to two years from the date of rejecting the applicants, and must then be destroyed. The data can be retained for a longer period if there is a subsisting reason that obliges the employer to do so (e.g. to fulfill a legal obligation), or the applicants have given their consent for the data to be retained beyond two years. 9. ARE THERE ANY SITUATIONS IN WHICH EMPLOYERS HOLDING PERSONAL DATA MAY BE EXEMPT FROM THE ORDINANCE OR THE DATA PROTECTION PRINCIPLES? 9. ARE THERE ANY SITUATIONS IN WHICH EMPLOYERS HOLDING PERSONAL DATA MAY BE EXEMPT FROM THE ORDINANCE OR THE DATA PROTECTION PRINCIPLES? Sections 53 and 55 of the Ordinance state that personal data relating to the following purposes are exempt from the provisions of right of access (data protection principle 6): personal data relating to staff planning; personal data generated by certain evaluative processes, including a recruitment or promotion

exercise, prior to a decision being taken and where an appeal can be made against such a decision; a personal reference for an appointment up to the time when the position is filled. It should be noted that the use of any exemption is discretionary but not mandatory. In other words, an employer can still choose to comply with access requests to personal data irrespective of the above exemption. 10. HOW LONG IS AN EMPLOYER ALLOWED TO KEEP THE PERSONAL DATA OF FORMER EMPLOYEES? 10. HOW LONG IS AN EMPLOYER ALLOWED TO KEEP THE PERSONAL DATA OF FORMER EMPLOYEES? Data protection principle 2 requires that personal data should not be kept for any longer than is necessary to fulfill the purposes for which the data were to be used, or a directly related purpose. Whether personal data can be retained for a long time will depend on whether or not the purposes for which the data were collected have already been exhausted, or whether there is any public interest reason for keeping the data (see section 26 of the Ordinance). The Code of Practice on Human Resource Management specifies that the personal data of former employees may be retained for a period of up to seven years from the date the former employee ceases employment. The data may be retained for a longer period if it is necessary for the employer to fulfill contractual or legal obligations, or the former employee has voluntarily given express consent for such retention. 11. AN EMPLOYER WANTS TO ANNOUNCE THE RESIGNATION OF A FORMER EMPLOYEE IN A NEWSPAPER. WHAT SHOULD THE EMPLOYER BE AWARE OF? 11. AN EMPLOYER WANTS TO ANNOUNCE THE RESIGNATION OF A FORMER EMPLOYEE IN A NEWSPAPER. WHAT SHOULD THE EMPLOYER BE AWARE OF? In any public announcement regarding a former employee having left his/her employment, the employer should take care not to disclose the identity card number of the employee concerned in the notice. 12. DO EMPLOYEES HAVE THE RIGHT TO OBTAIN A COPY OF THEIR PERSONAL RECORDS INCLUDING APPRAISAL REPORTS? 12. DO EMPLOYEES HAVE THE RIGHT TO OBTAIN A COPY OF THEIR PERSONAL RECORDS INCLUDING APPRAISAL REPORTS? Data protection principle 6 stipulates that an individual has the right to ascertain whether a data user holds personal data about him/her and to request access to such data. However, as per the previous answer for question 9, the Ordinance stipulates that employment-related data for the purpose of staff planning or evaluative processes are exempt from the data access request principle. In other words, the employees may not be entitled to obtain their appraisal reports from their boss. As mentioned in question 9, however, this exemption is discretionary but not mandatory. An employer can still choose to comply with data access requests and release those personal records to employees. 13. WHO IS LIABLE FOR A CONTRAVENTION OF THE ORDINANCE IN RELATION TO EMPLOYMENT-RELATED PERSONAL DATA - THE EMPLOYER OR THE HUMAN RESOURCES MANAGER? 13. WHO IS LIABLE FOR A CONTRAVENTION OF THE ORDINANCE IN RELATION TO EMPLOYMENT-RELATED PERSONAL DATA - THE EMPLOYER OR THE HUMAN RESOURCES MANAGER? This depends on the offence in question. Section 64 of the Ordinance specifies a number of offences, some of which may be committed by "persons" (i.e. organizations or individual persons). Under the Criminal Procedure Ordinance, where a statutory offence has been committed by a company which can be both a "person" or a "data user" under the Personal Data (Privacy) Ordinance, and it is proved that the offence was committed with the "consent or connivance" of a director or other officer concerned in the management of the company, that director or other officer is personally liable. Accordingly, both the employer and the human resources manager could be liable for a contravention of the Ordinance in relation to employment-related personal data. In practice, where the human resources manager acts in accordance with the instructions of the employer, the efforts of the PCO in enforcing compliance would normally be directed at the employer. On the other hand, if the employer has taken all reasonable practical steps to ensure compliance with the Ordinance and the human resources manager has contravened the Ordinance by acting in a manner contrary to company policy and practice, enforcement action taken by the PCO may be directed at the human resources manager. 14. COMPLAINT CASE NOTES FROM THE PCPD - CAN EMPLOYMENT AGENTS, FOR THE PURPOSE OF GUARANTEEING THEIR COMMISSION PAYMENTS, COLLECT ID CARD COPIES FROM JOB APPLICANTS? 14. COMPLAINT CASE NOTES FROM THE PCPD - CAN EMPLOYMENT AGENTS, FOR THE PURPOSE OF GUARANTEEING THEIR COMMISSION PAYMENTS, COLLECT ID CARD COPIES FROM JOB APPLICANTS? Please read the answer provided by the PCPD website. 15. COMPLAINT CASE NOTES FROM THE PCPD - IS THE POSTING OF AN EMPLOYEE'S COMPLAINT LETTER ON A NOTICE BOARD AN INTRUSION

OF PERSONAL DATA PRIVACY? 15. COMPLAINT CASE NOTES FROM THE PCPD - IS THE POSTING OF AN EMPLOYEE'S COMPLAINT LETTER ON A NOTICE BOARD AN INTRUSION OF PERSONAL DATA PRIVACY? Please read the answer provided by the PCPD website. 16. WHAT ARE THE THINGS THAT EMPLOYERS SHOULD CONSIDER BEFORE CONDUCTING WORK MONITORING MEASURES (E.G. TELEPHONE, VIDEO, E-MAIL OR INTERNET MONITORING)? CAN COVERT/SECRET MONITORING OF EMPLOYEES BE ADOPTED? 16. WHAT ARE THE THINGS THAT EMPLOYERS SHOULD CONSIDER BEFORE CONDUCTING WORK MONITORING MEASURES (E.G. TELEPHONE, VIDEO, E-MAIL OR INTERNET MONITORING)? CAN COVERT/SECRET MONITORING OF EMPLOYEES BE ADOPTED? Employers should examine whether or not there are alternatives to these measures that they may resort to. For example, would selective/random checking, rather than continuous monitoring, be effective and sufficient for the employers' purposes? Can the monitoring measures be confined to areas of high risk? If employers plan to use CCTV, can the camera recording be only confined to selected areas instead of all areas of the company? As a general rule, employee monitoring should be conducted in an open/overt manner. Covert monitoring (e.g. using hidden "pinhole" cameras) should not be adopted unless it is justified by the existence of special circumstances (e.g. a reasonable suspicion that an unlawful activity is about to be committed or has been committed by certain employees). Employers who have decided to monitor employees at work should accept responsibility and be accountable for proper conduct when carrying out their monitoring activities. For example, they should develop privacy complaint measures to protect their employees. 17. SHOULD EMPLOYERS NOTIFY THEIR EMPLOYEES BEFORE COMMENCING THE ABOVE-MENTIONED WORK MONITORING MEASURES? HOW SHOULD EMPLOYERS MANAGE THE DATA COLLECTED? 17. SHOULD EMPLOYERS NOTIFY THEIR EMPLOYEES BEFORE COMMENCING THE ABOVE-MENTIONED WORK MONITORING MEASURES? HOW SHOULD EMPLOYERS MANAGE THE DATA COLLECTED? Employers should inform their employees of any monitoring policy. It is good practice to prepare a comprehensive written privacy policy/employee monitoring policy and release it to the employees, preferably before any monitoring begins. As recommended by the PCO, such policy should explicitly refer to the following matters: the business purpose(s) that employee monitoring seeks to fulfill; 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 may be used. An example of a privacy policy statement concerning e-mail monitoring is provided in Appendix I of the Privacy Guidelines - Monitoring and Personal Data Privacy at Work (which is published by the PCO). Unless an employer has obtained the express consent of an employee (and the consent is given voluntarily), or unless there is an applicable exemption provided for under the law, an employee's personal data collected by monitoring measures can only be used for the purposes stated in the employee monitoring policy, or for a directly related purpose. Personal data collected should not be kept any longer than is necessary for fulfilling the stipulated purpose. For example, recorded information contained on CCTV tapes should be routinely erased according to a pre-determined schedule. A longer retention period may be appropriate in special circumstances (e.g., where the recorded information is required for evidentiary purposes in legal or disciplinary proceedings). Employers should also implement security and access control measures to safeguard the protection of the personal data collected. For example, CCTV tapes should be securely locked in a storage facility located in a controlled access area. 18. CAN I INSTALL A VIDEO CAMERA AT HOME TO MONITOR MY DOMESTIC HELPER? 18. CAN I INSTALL A VIDEO CAMERA AT HOME TO MONITOR MY DOMESTIC HELPER? The PCO issued the document Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers in December 2004. The following provides a summary of this publication for your reference. The use of video cameras to monitor domestic helpers' activities is in general an intrusion of privacy. Before using this monitoring method, employers must seriously consider whether it is necessary to do so, and whether there are alternative means available. In the event of a complaint made to the PCO, the alleged employers may be called upon to explain and prove the initial evidence or suspicion which justifies the use of video monitoring. If you decide to implement video monitoring at home, you should note 3 important points: reasonableness of the monitoring practice, openness of the monitoring practice, and use and retention of video records. a) Reasonableness of the monitoring

practice Employers should conduct the monitoring in an overt/open manner unless there are special circumstances which justify the use of covert/secret means (e.g. use of hidden "pinhole" cameras). The existence of the following situations may justify covert monitoring: there is a reasonable suspicion that a child or an elderly person has suffered (or is likely to suffer) from abuse or neglect, e.g. there are signs of unexplained injuries found on the body of that person, or where abnormal behaviours are observed in the domestic helper; it is highly likely that the suspected abuse occurred at home; and there is no realistic alternative to obtaining evidence of these abusive acts other than by way of covert monitoring. However, employers should note that no cameras (whether hidden or not) should capture images showing activities inside the private area where the domestic helper rests after work. b) Openness of the monitoring practice It is important that domestic helpers be notified of the presence of any video monitoring system in the premises where they work. This notification should not be omitted except in very exceptional situations such as to collect evidence of abuse based on reasonable suspicion. The PCO recommends that a written notification should be given instead of an oral one. Employers are reminded that such notification does not confer upon them a legal right to adopt employee monitoring under all circumstances nor does it release them from their obligations under the Ordinance to observe the six data protection principles. c) Use and retention of video records Employers must ensure that video records are only used for the purposes stated in the notification given to domestic helpers or a directly related purpose, unless otherwise permitted by law. The PCO recommends that video records which contain the personal data of domestic helpers be retained for not more than 7 days. A longer retention period may be considered if the recorded data are required for evidentiary purposes (e.g. to assist an investigation conducted by the PCO or the police). PRIVACY ON THE INTERNET V. PRIVACY ON THE INTERNET Some people may have the view that privacy on the Internet is more of an IT issue than a legal issue. In practice, it is a combination of the two. The following questions and answers are given with reference to the PCPD's publication: "Internet Surfing with Privacy in Mind - A Guide for Individual Net Users". More leaflets are available on the PCPD's website which correspond to the rapid advancing Internet applications and services: Guidance for Data User on the Collection and Use of Personal Data through the Internet (December 2011) Protecting Privacy - Using Computers and the Internet Wisely (March 2012) Online Behavioural Tracking (July 2012) Cloud Computing (November 2012) Protect Privacy by Smart Use of Smartphones (November 2012) Personal data privacy protection: what mobile apps developers and their clients should know (November 2012) Protecting Online Privacy - Be Smart on Social Networks (April 2013) Children Online Privacy - Practical Tips for Parents and Teachers (December 2015) Cyber-bullying - What you need to know (Revised in March 2017) 1. HAVE YOU CHECKED YOUR INTERNET SERVICE PROVIDER (ISP)'S POLICIES ON USING "CLICKTRAILS" (YOUR WEBPAGE BROWSING RECORD)? 1. HAVE YOU CHECKED YOUR INTERNET SERVICE PROVIDER (ISP)'S POLICIES ON USING "CLICKTRAILS" (YOUR WEBPAGE BROWSING RECORD)? Ask your ISP about its use of "clicktrails" data collected from you. Your ISP can keep track of the Internet pages you have visited by looking at computer log files held in its server. These are "clicktrails" data about you and are normally used only for the purpose of system maintenance and troubleshooting. ISPs are not allowed to use the data for other purposes, such as market research, without your consent (data protection principle 3). 2. ARE YOU ASKED TO PROVIDE YOUR PERSONAL DATA ON-LINE? 2. ARE YOU ASKED TO PROVIDE YOUR PERSONAL DATA ON-LINE? If yes, you should do the following before you press the "submit" button to provide your personal data via an on-line form, or send an e-mail containing your personal data. Look for identity details of the web site. It is possible that a site appears to be at an electronic address that does not belong to it. Visit the "About the Organization" page and check the organization's identity details such as its name, physical location, and contact telephone/fax number. An organization may be considered as using unfair means to collect personal data if it does not disclose its identity (in which case it might have contravened data protection principle 1). Look for the site's privacy policy notice. It is safer to know what the site's personal data handling policy is before you provide them with your own. The Ordinance requires that organizations in Hong Kong should be

open about their policy and practices with respect to the handling of personal data (data protection principle 5). Search for an on-line notification of a Personal Information Collection (PIC) statement. The PIC statement is a means by which the site should inform you: how your data are to be used; to what other parties they may transfer your data; your right to request a copy of your personal data and correct any errors; and who should be contacted for such requests. Under the Ordinance, organizations in Hong Kong must provide this information at or before the time they collect personal data from you. 3. HAVE YOU SET YOUR INTERNET BROWSER TO ASK YOU BEFORE ACCEPTING A "COOKIE"? 3. HAVE YOU SET YOUR INTERNET BROWSER TO ASK YOU BEFORE ACCEPTING A "COOKIE"? Cookies are small files that can be stored in your computer when you visit a web page. When you visit a web site, the server of that site may request a unique ID from your Internet browser. If your browser does not have an ID, that server will deliver one to your computer and this is the process of "passing a cookie". Sometimes when you visit a web site, you may be asked to fill in a form providing information such as your name and interests, and such information may also be stored in cookies. The host of that web site may then use cookies to track your behaviour and interests. To enhance the degree of security of your browser, you may consider setting an option in your browser to ask your permission to accept a cookie each time one is presented. You may also use "anonymous cookies" software. You can search the Internet using the word "cookies" to find software that can keep your computer clear of cookies or make your cookies files ineffective for access. This would help to reduce your loss of privacy. 4. ARE YOU ANNOYED ABOUT DIRECT MARKETING E-MAILS ADDRESSED TO YOU? 4. ARE YOU ANNOYED ABOUT DIRECT MARKETING E-MAILS ADDRESSED TO YOU? Under section 34 of the Ordinance, a company in Hong Kong that makes a direct marketing approach to you has an obligation to offer you an "opt-out" opportunity not to receive further marketing information from it. This gives you the right to request the sender to stop sending marketing e-mails to you. You should also take precautions to avoid receiving unsolicited advertising e-mails. To reduce the chances of making yourself a marketing target, you should avoid registering with free e-mail services or e-mail directory services. If you use a "signature file" (note) in your e-mail correspondence , you should be careful not to provide unnecessary details about yourself in the signature file which may expose you as a marketing target. (Note: A signature file is small text file that can be automatically attached to the end of e-mail messages. It may include the sender's name, job title, company name, phone/fax number, etc.) 5. COMPLAINT CASE NOTES FROM THE PCPD - SYSTEM LOOPHOLES MENDED TO PREVENT UNAUTHORIZED OR ACCIDENTAL ACCESS TO PASSWORD PROTECTED PERSONAL DATA FILES OF CUSTOMERS. 5. COMPLAINT CASE NOTES FROM THE PCPD - SYSTEM LOOPHOLES MENDED TO PREVENT UNAUTHORIZED OR ACCIDENTAL ACCESS TO PASSWORD PROTECTED PERSONAL DATA FILES OF CUSTOMERS. Please read the case details provided by the PCPD website. PRIVACY REGARDING DIRECT MARKETING VI. PRIVACY REGARDING DIRECT MARKETING The Amendment Ordinance 2012 introduced a new regime governing the use of personal information in direct marketing, which took effect on 1 April 2013. The new regime provides stronger protection for individuals. When data users intend to use or provide an individual's personal data in direct marketing, they are required to inform the individuals of the prescribed information and obtain their consent. Under section 35A of the Ordinance, "direct marketing" (in the context of personal data privacy) means: offering or advertising the availability of goods, facilities or services; or soliciting donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, by means of: information or goods sent to specific persons by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or telephone calls made to specific persons. Corresponding to the amendment of the Ordinance, the Commissioner published guidance notes entitled New Guidance on Direct Marketing in January 2013. A. USE OF PERSONAL DATA FOR THE DATA USER' S OWN DIRECT MARKETING PURPOSES A. USE OF PERSONAL DATA FOR THE DATA USER' S OWN DIRECT MARKETING PURPOSES With reference to section 35C of the amended Ordinance, before using personal data in direct marketing, data users must follow the specific steps listed below: 1. Data users must inform the data subjects of their intention to use the data subjects' personal data for direct

marketing, and they may not so use the data unless they have the data subjects' consent. 2. Data users must provide the data subjects with information on the intended use of the data, including the kinds of personal data to be used and the classes of marketing subjects in relation to which the data is to be used. 3. Data users must provide the data subjects with a free-of-charge channel through which the data subjects may communicate their consent to the intended use. 4. In order to help data subjects make an informed choice, the information provided by data users must be presented in a manner that is easily understandable and, if in written form, easily readable. In addition, according to section 35F, if data users are using the data in direct marketing for the first time, they must notify the data subjects of their op-out right, and the data users must, without charge to the data subjects, stop using the data in direct marketing if the data subjects opt out. Data users can use the personal data in direct marketing only after they have received the data subjects' consent to the intended use of the personal data. Consent, in this context, includes an indication of no objection to the use or provision of the personal data (section 35A(1)). If the data subjects give their consent orally, the data users must confirm in writing to the data subjects within 14 days from receiving their consent the permitted kind of personal data and the permitted class of marketing subjects (section 35E). Data users must comply with the data subjects' request at any time to stop using the data subjects' personal data in direct marketing without charge to the data subject (section 35G). Data users who contravene any of the requirements in the sections mentioned above commit an offence. For each offence, the data user is liable on conviction to a maximum fine of $500,000 and to a maximum imprisonment of three years. In contrast to this new regime which is an "opt-in" regime, the old regime offered data subjects only a limited "opt-out" option: i.e., when data users used data subjects' personal data in direct marketing for the first time, the users had to inform the subjects that they could request the data user to cease using their personal data for direct marketing purposes. If data subjects made such a request, the data users had to stop using the data; if the data subjects made no such request, their personal data could be used without any further notice. It should be noted that the old regime still applies to personal data that was used in direct marketing before the new amendment took effect, pursuant to section 35D of the amended Ordinance (also called a "Grandfather arrangement": i.e. an old rule continues to apply to certain existing cases, while a new rule applies to all future cases). In other words, if before 1 April 2013 a data user used the personal data in direct marketing in compliance with the existing requirements of the Ordinance, that data user could continue to do so on or after 1 April 2013, in relation to the same class of marketing subjects, without being subject to the obligations imposed under the new regime. B. PROVISION OF PERSONAL DATA TO THIRD PARTIES FOR USE IN DIRECT MARKETING B. PROVISION OF PERSONAL DATA TO THIRD PARTIES FOR USE IN DIRECT MARKETING In addition to the regulation on the use of personal data by data users for their own direct marketing purposes, the amended Ordinance introduces more stringent regulations on providing personal data to third parties for use in direct marketing, including the sale of personal data. When data users intend to provide personal data to third parties for use in direct marketing, the data users must follow a procedure similar to that outlined above in part A. Additionally, they must inform the data subjects of two other kinds of information in relation to the intended use (section 35J): whether the data is to be provided for gain; and the classes of persons to whom the data is to be provided. The form of notification and response of the data subject must be in writing. Furthermore, the data users must not provide personal data to a third party unless the data users have received written consent from the data subject. (section 35K) Data subjects may at any time and irrespective of whether they have previously given consent to the provision of their personal data to a third party require the data user— to stop providing the data subjects' personal data to a third party for use by that party in direct marketing; and to notify any third party to whom the data has been so provided to stop using the data in direct marketing. Accordingly, data users who receive these instructions must, without charge to the data subjects, comply with them. The notification made by the data users to the third party must be in writing. Any third

party who receives such a notification from the data user must stop using the personal data in direct marketing in accordance with the notification. (section 35L) Contraventions of the requirements in relation to the provision of personal data to third parties for use in direct marketing are offences. For contraventions involving the provision of personal data for gain (including the sale of personal data), the maximum penalty is a fine of $1,000,000 and imprisonment for five years. For other contraventions, the maximum penalty is a fine of $500,000 and imprisonment for three years. Unlike the use of personal data for the data users' own direct marketing purposes, the provision of personal data to third parties for use in direct marketing is not subject to a "Grandfather arrangement" (i.e. when an old rule continues to apply to certain existing cases, while a new rule applies to all future cases). In other words, any provision of personal data to third parties, whether it happened before or after 1 April 2013, must comply with the requirements of the amended Ordinance. With regard to cold-calling (note), staff members of the data user are recommended to give an opt-out message along the following lines:We are not allowed to use your personal data in direct marketing without your consent. If you do not wish to receive marketing calls from us, please tell me anytime and we will not call again." If the data user fails to inform a data subject of his opt-out right or other information required by sections 35C-35F as mentioned above, a data subject may lodge a complaint with the Office of the Privacy Commissioner for Personal Data. (Note: Cold-calling is the practice of making a marketing approach by telephone to a potential customer with whom the caller has had no previous dealings.) The PPCD published a leaflet that introduces the ways for individuals to exercise their right of consent to opt-out of direct marketing activities under the amended Ordinance. 1. REGARDLESS OF THE PROPERTY OWNER'S OBJECTIONS, IF AN ESTATE AGENT REPEATEDLY CALL THE OWNER TO PERSUADE HIM/HER TO SELL THE PROPERTY, WILL THIS VIOLATE SECTION 35G OF THE ORDINANCE? 1. COMPLAINT CASE NOTES FROM THE PCPD - STAFF OF AN ESTATE AGENCY HAD BEEN APPROACHING A PROPERTY OWNER THROUGH HER HOME AND MOBILE TELEPHONE NUMBERS (NOTWITHSTANDING HER REPEATED OBJECTIONS) IN AN EFFORT TO PERSUADE HER TO SELL HER PROPERTY. IS THIS A VIOLATION OF SECTION 35G OF THE ORDINANCE? Please read the answer provided by the PCPD website. 2. IS IT AN APPROPRIATE USE OF PERSONAL DATA IN POLITICAL DIRECT MARKETING IF A COUNCILLOR'S OFFICE USES THE CONTACT INFORMATION FROM CITIZENS WHO HAVE SOUGHT ASSISTANCE FROM THE OFFICE TO MAKE ELECTION PUBLICITY CALLS? 2. COMPLAINT CASE NOTES FROM THE PCPD - A COUNCILLOR'S OFFICE USES THE CONTACT INFORMATION OF CITIZENS WHO HAVE SOUGHT ASSISTANCE FROM THE COUNCILLOR TO MAKE ELECTION PUBLICITY CALLS. IS THIS AN APPROPRIATE USE OF PERSONAL DATA IN POLITICAL DIRECT MARKETING? Please read the answer provided by the PCPD website. COMPLAINTS, PENALTIES AND LEGAL ASSISTANCE VII. COMPLAINTS, PENALTIES AND LEGAL ASSISTANCE After receiving a complaint in relation to possible contraventions of the Personal Data (Privacy) Ordinance, the staff of the Office of the Privacy Commissioner for Personal Data (PCPD) would first conduct preliminary enquires to see if the complainant holds substantial grounds. After preliminary enquiries into the complaint, the PCPD may inform the complainant of its preliminary views and ask the opposite party to take remedial action to resolve the issues surrounding the complaint. If the dispute cannot be resolved by mediation, the PCPD may conduct a formal investigation. If the complaint involves suspected contravention of a serious nature, the PCPD would immediately conduct a formal investigation instead of making preliminary enquiries. If after investigation it is found that there are contraventions on the part of the data user, an enforcement notice would be served on that data user by the PCPD directing him/her to take any necessary remedial action. Data users who do not comply with the PCPD's enforcement notice commit an offence and are liable to a fine or imprisonment. The Commissioner can also instigate prosecution action. Under the amended Ordinance. The time for preparing information for prosecution was extended from six months to two years from the date of the commission of the offence. If a data subject suffers damage (including injury to feelings) as a result of a contravention of the Ordinance by a data user, the data subject can sue the data user for compensation through civil proceedings. Under the amended Ordinance, the Commissioner can grant legal assistance to that person. A. COMPLAINT-HANDLING POLICY AND COMPLAINT PROCEDURES Data subjects should first lodge a

complaint with the data user who does not handle his or her personal data in accordance with the Ordinance. If the alleged offender fails to give a satisfactory reply and the data subject decides to lodge a complaint with the PCPD, the complainant is advised to first learn about the complaint-handling policy of the PCPD. For details, please visit the PCPD webpage on this policy or call its hotline at 2827 2827. The complaint procedure, accompanied by a flowchart, can be found on the PCPD website. Complainants should note that the time limit for lodging a complaint is two years from the date of their actual knowledge of the privacy-intrusive act or practice, but it is recommended that they lodge the complaint as soon as possible. B. ENFORCEMENT NOTICE AND PENALTIES Under section 50 of the amended Ordinance, the Commissioner has wider power to serve enforcement notices. If he finds a contravention of a requirement under the Ordinance, the Commissioner can serve an enforcement notice on the data user concerned to direct it to take the necessary steps to remedy the contravention, irrespective of whether the contravention will continue or be repeated. Any data user who fails to comply with the PCPD's enforcement notice commits an offence and is liable to a fine at level 5 (currently $50,000) and to imprisonment for two years. The amended Ordinance provides for a heavier penalty for a second and subsequent conviction for contravening an enforcement notice. The penalty is a fine at level 6 (currently $100,000) and imprisonment of two years and, in the case of a continuing offence, a daily fine of $2,000. (Section 50A(1)) If data users comply with an enforcement notice issued against them within a specified period, and subsequently intentionally commit the same offence, they are liable to a fine of $50,000 and to imprisonment for two years and, in the case of a continuing offence, a daily fine of $1,000. (Section 50A(3)) For more details of other offences under the Ordinance, please refer to section 64 of the Ordinance. C. LEGAL ASSISTANCE If data subjects suffer any damage caused by a data user in contravention of the requirements under the Ordinance, they can make a civil claim for compensation from the data user for the damage: i.e. sue the data user in a court (section 66). However, the data subject may have difficulty in pursuing the lawsuit because some cases may be more complex and may incur considerable legal costs and expenses. In view of this, section 66B of the amended Ordinance authorises the Commissioner to grant legal assistance to aggrieved individuals seeking such compensation. This legal assistance takes the form which the Commissioner considers most appropriate, including but not limited to the following: giving advice; mediation; arranging for advice or assistance from a solicitor or counsel; or arranging for representation by any person, including such assistance as is usually given by a solicitor or counsel, in the steps preliminary or incidental to any proceedings, or in arriving at or giving effect to a compromise to avoid or bring to an end any proceedings. The assistance may be rendered through the Commissioner's legal staff or external lawyers engaged by the Commissioner on behalf of the person seeking legal assistance. The Commissioner's legal staff will advise the individual independently without any influence from anyone else. The Commissioner will normally bear the cost of legal assistance. If the assisted person is successful in the claim for compensation, and in recovering the costs and expenses related to the claim, whether through legal proceedings or any other settlement, the Commissioner has the first charge on such costs and expenses payable to the assisted person (i.e. the payment will be used to settle the Commissioner's legal costs or expenses first). Data subjects seeking legal assistance should normally lodge a complaint against the relevant data user with the Commissioner before applying for legal assistance. They should meet the abovementioned requirements during the complaint-handling process, providing all information to the PCPD.They may lodge an application for legal assistance after the Commissioner concludes the complaint. All applications must be made on the PCPD's Application Form. The Commissioner may grant assistance if he thinks fit to do so. In exercising his discretion, the Commissioner will consider a series of factors, including in particular: whether the case raises a question of principle; or whether it is unreasonable, having regard to the complexity of the case or the applicant's position in relation to the respondent or another person involved or any other matter, to expect the applicant to handle the case unaided. The Commissioner lists the factors that he may take into

account in the Leaflet entitled “Legal assistance for civil claims under the Personal Data (Privacy) Ordinance”. Normally, an applicant for legal assistance will be informed of the result within three months after submitting all the relevant information for the application. If the Commissioner decides to grant assistance, the applicant will be asked to sign an agreement which sets out the terms and conditions under which the assistance will be given. If the Commissioner refuses the application, the applicant will be notified in writing with reasons. At any stage of the provision of legal assistance, the Commissioner may use his discretion to review his decision to grant assistance and discontinue such assistance. The leaflet provides the circumstances under which legal assistance may be discontinued, including, in particular, a situation in which the applicant knowingly gives false or misleading information to the Commissioner. The Ordinance provides no right of appeal against the Commissioner’s decision to refuse to grant legal assistance or to discontinue such assistance. However, if there is any material change of circumstances, the Commissioner may review, at his discretion, his decision upon receiving a written request from the applicant. His review decision is final. RECRUITMENT RECRUITMENT HUMAN RESOURCES MANAGEMENT HUMAN RESOURCES MANAGEMENT PRIVACY AT WORK PRIVACY AT WORK