Data Protection Principles in the Personal Data (Privacy) Ordinance

– from the Privacy Commissioner's perspective (2nd Edition)

Data Protection Principles in the Personal Data (Privacy) Ordinance

– from the Privacy Commissioner's perspective (2nd Edition)

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

Website: www.pcpd.org.hk
Enquiry Hotline: (852) 2827 2827

Contents

Preface to the Second Revised Edition

Time passes quickly. The first edition of this book has now been around for nearly four years. More significantly, the last few years have witnessed some astounding technological developments which seriously impact on the individuals' rights to privacy in relation to their personal data. I therefore think that it is timely for this second revised edition to go to print.

Another very good reason why I want the book to be revised and re-printed is to make it more accessible to the public. A record number of visits has been made to the website of the Privacy Commissioner for Personal Data over the last four years reflecting the fact that increasingly the public wants to know more about the working of the Personal Data (Privacy) Ordinance. The original edition appeared only in book form and I feel very strongly that its contents should be accessible to all electronically free of charge. This is in accord with one of my chief functions, i.e. to promote awareness and understanding of the provisions of the Ordinance, in particular, the data protection principles.

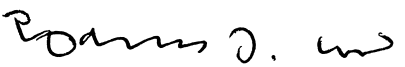
Of course there will always be people who wish to see a copy of the book and be able to feel its weight and flip its pages. I have therefore decided that this revised edition should be available in the conventional form of a book and also electronically accessible on our website. Those who wish to have this book on their book shelves will need to pay.

Since the first edition there has been quite a number of Administrative Appeals Board decisions touching on the interpretation of the data protection principles. Unless and until these decisions have been reversed or modified by the Court, they will largely be followed in the Privacy Commissioner's handling of enquiries and complaints. The effects of these decisions are appropriately reflected in this new revised edition.

The format of this revised edition has largely followed the original edition. However some conscientious attempts have been made to make it more reader-friendly. I hope the result is that the readers can find answers to their questions more easily.

Both editions of this book are the products of the collective efforts of many members of the Privacy Commissioner for Personal Data past and present. It is tedious and probably impossible to name all contributors. Still justice requires of me to name Margaret Chiu, our then legal counsel, as the de facto editor of the original edition and Wilson Lee, one of our current legal counsel, as the person largely responsible for this revised edition.

We are not professional authors and this book has been written in between the normal duties of my colleagues and in their spare time. It is inevitable that there will be errors, misprint and slip-ups. I hope the readers will be kind and point out to us anything they may find wanting or needing improvements so that the next revised edition will yet be better.



Roderick B. Woo
Privacy Commissioner for Personal Data
Hong Kong SAR
July 2010

Preface to the First Edition

In Hong Kong, personal data privacy law is a relatively new subject which gained legislative recognition in December 1996 when the principal provisions of the Personal Data (Privacy) Ordinance were brought into effect.

A decade is a short period of time in terms of development of the law on this subject. Yet within that time, the notion of personal data privacy has achieved rapid and avid acceptance by the community and attracted the regular attention of the popular media. The awareness of data privacy as a personal right, and the public attention accorded to it, have given rise to an enhanced level of expectation and a broad demand for protection against improper collection and use of personal data.

Technological advancements in recent years have given a new meaning to the processing and use of information, much of which is of a personal nature, and the phenomenal growth of internet users in their millions, who log on for information, communication and electronic commerce, have accentuated the demand for an effective regulatory structure that is underpinned by a legislative framework which is clear and easily understood. Data users, particularly those in the business sector are increasingly concerned about whether acts or practices undertaken by them are privacy compliant and individuals as data subjects are also anxious to know more about what the personal data privacy legislation can do to protect their privacy rights.

For those who are more seriously concerned with the topic, there is only a limited collection of texts to refer to and a few judicial precedents to consider. There is a paucity of legal research materials. Generic references to privacy are found mainly in international declarations and constitutional instruments[1], which do not readily serve as useful aids in the interpretation of the Personal Data (Privacy) Ordinance.

In comparison with many other jurisdictions, Hong Kong has the advantage of having the Ordinance which is supplemented by various codes of practice and guidelines which my Office has issued. However, the statutory provisions and the regulatory requirements (notably the six Data Protection Principles) owe their origins to concepts and principles which critics have described as lacking in legal clarity. The truth of the matter is they reflect the evolving nature of the concept of personal data protection and its relatively recent recognition as a legal right in Hong Kong and abroad.

---

[1] See, Article 12, United Nations Universal Declaration of Human Rights; Article 8, European Convention on Human Rights; Article 17, International Covenant on Civil and Political Rights; the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Article 14, Hong Kong Bill of Rights Ordinance (Cap. 383, Laws of Hong Kong); Articles 30 & 39, Basic Law of the HKSAR.

Over the years the Office of the Privacy Commissioner for Personal Data has handled over 6,900 complaint cases and more than 157,000 enquiries. In that period, my Office has accumulated valuable experience in the range and types of privacy concerns expressed by the community and in the process it has developed certain criteria, principles and an operational stance in the application of the relevant statutory provisions and enforcement of regulatory requirements.

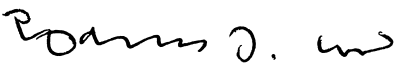
This book seeks to share with the reader the experience that my Office has gained since its establishment. Necessarily, the views expressed and stance taken are based on facts and evidence presented to my Office in the course of handling complaints, information available at the material time and social conditions then prevailing within the community that were relevant to the subject of personal data privacy. Readers will appreciate that such conditions may change over time and the future regulatory approach will be thereby affected.

An earlier draft of this book was sent to selected academics, legal professionals, organizations and institutions. I wish to thank them for their time and kind attention. In particular, I am grateful to the following organizations (mentioned in alphabetical order) for their substantial contribution in the form of detailed constructive suggestions to the original text: –

- The British Chamber of Commerce in Hong Kong;
- School of Law, The Chinese University of Hong Kong;
- Employers' Federation of Hong Kong;
- The Hong Kong Association of Banks;
- Hong Kong Bar Association; and
- Hong Kong General Chamber of Commerce.

This book is a joint effort of members of the staff of my Office, past and present, and without their research, writing and preparation, the publication of this book would not have been possible. A debt of gratitude is owed to them.

I hope that this book will provide those who wish to acquaint themselves in greater depth with the analytical reasoning adopted in upholding personal data protection, a meaningful insight into the work of my Office. I also hope that the book will offer those persons having responsibilities in the handling and processing of personal data a better understanding of the regulatory philosophy and the way my Office has been applying the law in dutiful discharge of its statutory obligations.



Roderick B. Woo
Privacy Commissioner for Personal Data
Hong Kong SAR
August 2006

Chapter 1
Introduction

1.1 The Personal Data (Privacy) Ordinance (PDPO) (Cap. 486)("the Ordinance") is unlike other ordinances in Hong Kong in that it is principle-based. Its core provisions are encapsulated in the six data protection principles which are found in Schedule 1 to the Ordinance. These principles are the cornerstones of the Ordinance which aims to protect the privacy of individuals in relation to their personal data.

1.2 The intention behind the six data protection principles is the creation of a new culture in effecting the handling of personal data during their whole life cycle from their collection to their destruction. The principles do not regulate the conduct of the data users in detail. In most cases, contraventions of the principles do not constitute criminal offences. It is when a data user fails to comply with the terms of an enforcement notice issued by the Privacy Commissioner for Personal Data ("the Commissioner") after a finding of a contravention that he becomes liable to be punished under the Ordinance. The enforcement notice to the offending data user is normally issued after an investigation and when certain conditions are met. However, a contravention of a data protection principle can form the basis of a civil suit against the data user whether or not an enforcement notice has been issued.

1.3 Since a contravention of any of the data protection principles may lead to legal sanctions, it pays every data user to understand them. Knowing their existence and their ordinary meaning may not be sufficient in every case. This is because the principles are not couched in definitive terms. A data user will benefit from expert explanations and advice in some situations.

1.4 Up to now there has not been a strong body of judicial decisions giving authoritative interpretations on all the principles. Be that as it may, the Commissioner has over the last 13 years dealt with more than two hundred thousand enquiries and complaints in respect of alleged contraventions of the data protection principles. In performing his statutory function the Commissioner has to adopt certain stances and provide fuller meanings to these principles. His decisions based on such stances have from time to time been tested in the Court and in the course of appeals to the Administrative Appeals Board ("AAB") whose determinations are treated as having a quasi-judicial authority. The Commissioner has in the past adopted the interpretations elucidated by the AAB in the subsequent handling of enquiries and complaints.

1.5 In the absence of any similar professional reference materials, it is certainly in the public interest for the Commissioner to state openly the criteria and principles upon which he, as the statutory regulator, has interpreted the six data protection principles as well as some related provisions of the Ordinance. In so doing he may : –

- help data users to comply with the requirements of the Ordinance in a way that will minimize the risk of sanction by the Commissioner regarding their handling of personal data;
- help the legal advisers of both data users and data subjects in giving practical advice to their clients;
- help individuals to understand the Commissioner's likely position on a particular issue before they consider lodging a complaint;
- provide reference materials for consideration by the Court or the AAB in cases before them involving the six data protection principles; and
- provide legal academics and other interested persons with materials for further study and research.

The regulatory approach

1.6 The Commissioner's regulatory approach has been consistent with the general common law rules on statutory interpretation[1] and in particular the principles of interpretation laid down by the **Interpretation and General Clauses Ordinance (Cap. 1, Laws of Hong Kong)**, in particular, **section 19** which provides:

"An Ordinance shall be deemed to be remedial and shall receive such fair, large and liberal construction and interpretation as will best ensure the attainment of the object of the Ordinance according to its true intent, meaning and spirit."[2]

---

[1] They are commonly categorized as the "literal rule" which accorded primacy to the literal meaning of the language used in the legislation; the "golden rule" with the presumption that an absurd result is not intended; and the "mischief rule" that legislation has targeted a particular mischief and provided a remedy for it.

[2] In how to apply the rule of *"fair, large and liberal"* construction and interpretation, the Court of Final Appeal in the case of *The Medical Council of Hong Kong v David Chow Siu Shek* [2000] 2 HKLRD 674, in determining the proper interpretation of sections 21(1) and 25(3) of the Medical Registration Ordinance, Cap 161 as to whether there is automatic restoration of the name of the medical practitioner who was removed for a specified period, had taken the following five interpretative factors into account, namely, (i) striking a balance; (ii) interpretation in the context of other statutes dealing with comparable matters; (iii) avoiding circularity; (iv) according meaning and substance to each provision; and (v) reluctance to find a radical change by a side-wind.

1.7 The Commissioner is constantly mindful of the generally recognized principle of "presumption against absurdity" in statutory interpretation[3], which is cited in Bennion's *Statutory Interpretation*[4] as follows:

> ***"Section 312. Presumption that 'absurd' result not intended***
>
> *(1) The court seeks to avoid a construction that produces an absurd result, since this is unlikely to have been intended by Parliament. Here the courts give a very wide meaning to the concept of 'absurdity', using it to include virtually any result which is unworkable or impracticable, inconvenient, anomalous or illogical, futile or pointless, artificial, or productive of a disproportionate counter-mischief*[5].
>
> *(2) In rare cases there are overriding reasons for applying a construction that produces an absurd result, for example where it appears that Parliament really intended it or the literal meaning is too strong.*"

1.8 Hence, in dealing with a case involving a particular data protection principle that, according to its language, seems to be open to more than one interpretation, the Commissioner tries not to adopt an interpretation that may produce an absurd or impractical result. He must always remind himself that the primary purpose of the Ordinance is to protect the individual's privacy right in relation to their personal data. When in doubt, he is inclined to take the line which results in providing such protection.

1.9 Since the Commissioner does not have the power to provide any definitive interpretation of the provisions of the Ordinance, there is always the possibility that an interpretation previously adopted by him may later be shown to be erroneous or incomplete by the Court or the AAB[6]. Once the Commissioner has adopted a certain interpretation of a data protection principle in one case, an attempt at consistency will be made to apply the same interpretation in subsequent cases. However, this practice is not immutable. A stance on a particular data protection principle may evolve according to experience gained since when the stance was first taken. Due to changed circumstances, the Commissioner may find it necessary to re-consider a stance he has previously adopted. Such

---

[3] Otherwise also known as the "golden rule" of interpretation, that whatever the literal meaning of the language which the legislature used, there was a presumption that it did not truly intend to bring about an absurd result.

[4] Fifth Edition, Butterworths

[5] The rule was followed in the case of *HKSAR v Hung Chan Wa* [2005] 3 HKLRD 291 concerning the proper interpretation of section 47 of the Dangerous Drugs Ordinance, Cap 134 in which the Court stated clearly that *". . . any exercise in statutory interpretation should seek an interpretation, that does not result in absurdity, provided it is reasonably possible so to do."* (paragraph 58 of the judgment).

[6] To which, pursuant to the Ordinance and the Administrative Appeals Board Ordinance (Cap. 442, Laws of Hong Kong), appeals from certain decisions of the Commissioner lie.

circumstances may include views of judicial authorities, developments in the handling and processing of personal data and social values.

1.10 "Grey areas" in the Ordinance touching on the interpretations of data protection principle are as far as possible identified and dealt with in this Book. Needless to say, the Commissioner will not be deterred from applying and interpreting the provisions of the Ordinance in any case that comes before him which falls within such "grey areas".

Disclaimer

1.11 Generally speaking, any statements made or views expressed in this Book are intended for reference only. They shall not give rise to any liability on the part of the Commissioner nor to any defence or estoppel of any kind in proceedings involving the Commissioner. They shall not bind the Commissioner in the exercise of his statutory functions in any way. The Commissioner gives no guarantee or assurance whatsoever as to their applicability to any given set of facts, especially when no two cases are identical in every aspect. Hence, rather than relying on such statements or views (which reliance, where made, would always be at the party's own risk) as the basis for any action or inaction, the reader is urged to exercise his independent judgment on the interpretations of the data protection principles and, where appropriate, avail himself of professional advice.

Copyright

Abbreviations used in this book

1.13 **"AAB"** means the Administrative Appeals Board established under section 5 of the Administrative Appeals Board Ordinance (Cap. 442, Laws of Hong Kong);

"Book" means this book;

"the Commissioner" means the office of the Privacy Commissioner for Personal Data established under section 5(1) of the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong) in general and where the context otherwise permits, also means and includes the person appointed by the Chief Executive under section 5(3);

"DPP" means data protection principle(s);

"*Eastweek* case" means the case of *Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83;

"HKID" means Hong Kong Identity Card;

"Ordinance" means Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong);

"PICS" means the notification given under DPP1(3) and commonly known as Personal Information Collection Statement;

"PPS" means the Privacy Policy Statement incorporating the privacy policy and practices adopted by the data user to be made generally available under DPP5.

1.14 In the same way as most of Hong Kong's laws are drafted, unless the context otherwise requires, all words in the masculine gender appearing in this Book include the feminine gender and the neuter gender, and all words in the singular include the plural, and vice versa.

Chapter 2

Meaning of "Personal Data"

The main questions:

- What constitutes "data"?
- What constitutes "personal data"?
- In particular, how does each of the conditions laid down in paragraphs (a), (b) and (c) of the definition of "personal data" apply?
- Are IP address, email address, fingerprint and examination script personal data?

The questions discussed in this chapter concerning the meaning of *"personal data"* have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

Meaning of the term "data"

2.1 The definition of the term "**data**" is given in **section 2(1)** of the Ordinance as follows:

> *"'data' means any representation of information (including an expression of opinion)* ***in any document****, and includes a personal identifier."*(emphasis added)

2.2 The term **"document"** is in turn defined in **section 2(1)** as follows:

> *"'document' includes, in addition to a document in writing –*
>
> *(a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and*
>
> *(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device."*

2.3 It follows from the above that, in order for any information to constitute "*data*", such information must have been recorded in a "*document*" as defined. This point may seem obvious enough, but it is worth making this clear at the outset to avoid any possible misunderstanding.

2.4 Information not being represented in any document (hence not constituting personal data) may be found in situations where, for example, there is real time CCTV monitoring of activities without turning on its recording function, and information committed to a person's memory or information as spoken (but not recorded). The question whether verbal utterance amounts to disclosure of "personal data" was considered in *AAB No. 21/1999* in which a civil servant who came to know certain sensitive personal information of the complainant through handling the complainant's complaint. Since there was no evidence to prove that the sensitive personal information ever existed in a recorded form, the AAB ruled that there was no "personal data" involved and thus the case fell outside the jurisdiction of the Commissioner.

Definition of "personal data"

2.5 The definition of the term "**personal data**" is given in **section 2(1)** of the Ordinance as follows:

> *" 'personal data' means any data –*
>
> *(a) relating directly or indirectly to a living individual;*
>
> *(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and*
>
> *(c) in a form in which access to or processing of the data is practicable."*

2.6 As explained above, the meaning of the term "*data*" is reasonably clear. Whether any data constitute "personal data", therefore, depends on whether such data satisfy all of the three conditions laid down in paragraphs (a), (b) and (c) in the definition of "*personal data*". However, given the generic nature of the terms used in those paragraphs, it is not surprising that uncertainty may sometimes arise in their application in specific situations, as discussed below.

Paragraph (a) – "relating directly or indirectly to a living individual"

2.7 The condition laid down in paragraph (a) in the definition of "*personal data*" requires the data in question to be "*relating directly or indirectly to*" a living individual. However, given that in the ordinary meaning of the word, the concept of "relatedness" is very much a matter of degree, this may give rise to difficulty in the application of paragraph (a).

2.8 The question of "relatedness" was considered by the UK court in detail. In *Durant v Financial Services Authority* [2003] EWCA Civ 1746, it was held that what constituted information that related to an individual to be personal data was (i) whether the information is biographical in a significant sense; and (ii) that the information should have the individual as its focus rather than some other person with whom he may have been involved. This judicial ruling became useful authority being followed by the UK privacy authority in interpreting the meaning of "personal data" under the Data Protection Act 1998. However, application of the arguments or principles used in this English authority to Hong Kong cases must be considered with great care. As pointed out by the learned judge in *Wu Kit Ping v. Administrative Appeals Board* [2007] 5 HKC 450, "*I have come to the conclusion that the substantial differences between the English legislation and the Hong Kong legislation means that great care must be taken in attempting to apply either arguments or principles used in the English cases when considering issues arising under the Ordinance. Consequently, rather than attempt to approach the issues on same point of view as the English courts I have found it more appropriate to*

examine the language of the legislation and to attempt to discern its true interpretation."

2.9 In the case of data that bear only an indirect relationship to an individual, it is questionable whether there in fact exists a certain point (and, if so, how to determine such a point) beyond which the relationship may be considered to be so remote that it fails to satisfy the condition laid down in paragraph (a). For example, while it should be reasonably obvious that in the case of an unincorporated business owned by an individual, data about debts owed by the business "relate" directly to the sole proprietor, whether or not a "relationship" exists may become progressively less clear in other cases where, say, the business is owned by a partnership in which the individual is one of the partners, or where the business is owned by a company and the individual is merely one of many shareholders, and so forth.

2.10 In the case of *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450, a lady made a data access request to a data user requesting the data user to supply to her written statements concerning her health condition given by medical officers to the data user. The data user supplied the relevant documents to the lady but made certain redactions which can be divided into three categories: (i) in several letters and a statement concerning the diagnosis, treatment and use of medications of the lady, the names of the writers and recipients, not being the lady, were redacted; (ii) in a letter from a writer to a recipient, not being the lady, the writer's statement directed at his conduct, in his professional capacity, of the treatment of the data subject, was redacted; and (iii) a writer's general statements made in a letter were redacted.

2.11 The Court considered that the names of the writers and recipients in category (i) were personal data of the writers and recipients, not the lady, nor did they fall within the scope of personal data "relating directly or indirectly" to the lady. The redactions were therefore lawful. In respect of category (ii), the Court considered that the redacted part was an opinion related directly to the lady, hence her personal data, and should have been disclosed to the lady. Since category (iii) were general statements having broad general application and did not directly or indirectly relate to the lady, the Court concluded that they were not the lady's personal data.

2.12 Indeed, even for data that relate directly to an individual, question may arise as to whether such relationship may be so trivial that it would appear strange for the data to be considered to give rise to obligations or liability under the Ordinance. Take the example of a simple telephone note informing a colleague that, in his absence, a friend has called and asked him to call back. Such a recorded note would apparently satisfy the condition under paragraph (a) (and those under paragraphs (b) and (c)) of the definition of "*personal data*", thus constituting the personal data of the colleague concerned. The same may be said, for example, about a seating plan of students in a classroom.

2.13 In *AAB No. 49/2001*, a sentence contained in the minutes of a meeting stating that "*. . . as Mr. X did not have the contact telephone number of Mr. Y . . .*" was ruled not to be personal data collected about Mr. Y but merely recording the reason why Mr. Y could not be reached for an appraisal interview and thus it was proper to have edited out the sentence when complying with the data access request made by Mr. Y.

2.14 From a plain reading of the section, it is perhaps difficult to infer a strict requirement in paragraph (a) that the relationship in question must be important, rather than trivial. However, for the purpose of the Commissioner's operation, any absurd result arising from this may usually be avoided in that, if a complaint should be brought to the Commissioner concerning data that "*relate*" to the complainant in none but a trivial sense, the Commissioner would be inclined to exercise his discretion to refuse to investigate the complaint on the ground of "*triviality*" provided under section 39(2)(b) of the Ordinance.

2.15 In *AAB No. 14/2007*, the AAB considered that an invoice, which was a document relevant to a legal proceeding to which the concerned individual was a party, was not personal data of the individual. The invoice, in the AAB's view, related to the trading price in a business transaction, rather than being related to the individual personally.

Paragraph (b) – "from which it is practicable for the identity of the individual to be directly or indirectly ascertained"

2.16 In applying the condition laid down in paragraph (b) to personal data, the first thing that should be taken note of is that the word "*practicable*" wherever it appears in the Ordinance, is defined under section 2(1) to mean "**reasonably practicable**".

2.17 In the case of *AAB No. 16/2000*, the appellant made a complaint to the Commissioner against a public transport company, about the fact that indicator lights came on and an electronic bell alarm went off whenever he entered or exited from the toll gates using his senior citizen concessionary Octopus card. This would reveal to all persons nearby the fact that he was over 65 which, according to him, amounted to a disclosure of his personal data. In its decision, however, the AAB (*inter alia*) confirmed the Commissioner's view that the Octopus card in question did not contain personal data belonging to the appellant and the card could be purchased or possessed by anyone. Thus, the fact that the light and sound were emitted when the complainant used the concessionary Octopus card to pass through the toll gate did not make it reasonably practicable for the identity of the complainant to be directly or indirectly ascertained.

2.18 Secondly, in deciding whether certain data held by a party satisfy the condition laid down in paragraph (b) and, in particular, in considering the meaning of the words "*from which*" in that paragraph, the Commissioner takes the view that the reference to the individual should be construed in the context of all the relevant information controlled by the data user, of which the personal data of that

individual form part. For example, where an employer holds a personnel file on one of his employees, there would of course be no need for every page in the file to bear explicitly the name of or other identifying information about the employee. If the employer should be asked whether the information contained in one such page constitutes the personal data of the employee, it would be unreasonable and contrary to the Commissioner's regulatory view for the employer to say "no" simply because reading that particular page alone does not reveal the identity of the employee. Conversely, when it is not practicable on the face of the data or from other information that it holds for the identity of the data subject to be directly or indirectly ascertained, the condition laid down in paragraph (b) is not fulfilled. For example, where a direct marketing letter is sent to the address of a company without naming any particular staff member as recipient, no personal data are collected by the direct marketing company as the identity of a targeted individual could not be ascertained from the face of the letter.

2.19 In applying the condition laid down in paragraph (b), the Commissioner will take into account all relevant data controlled by the party in question. If it is practicable for that party to ascertain from the totality of such data the identity of the individual, then each and every part of the data (including, in the example given above, any individual page within the personnel file) also satisfies the condition laid down in paragraph (b). This "totality" approach is equally applicable to the situation where the data are contained in several documents, which, when read or construed together, constitute the personal data of an individual. For example, when a separate note of address was found attached to a personnel file created for a particular employee, although no name was specifically stated on the note, it is likely to be construed as personal data belonging to the employee when read with other documents in the file and taking into account the nature of the matter as a whole.

2.20 On the other hand, where part or parts of the personal data are anonymous so that it is not reasonably practicable for the identity of the data subject to be ascertained from it, the Commissioner will generally regard the condition laid down in paragraph (b) not to be satisfied and hence not to amount to "*personal data*".

2.21 The question whether it is practicable to ascertain an individual's identity from the data was determined in a complaint in which an individual complained about his name being uploaded onto the web-page of a discussion forum. The individual alleged that the three Chinese characters of his name were used in a poetic expression posted in the forum. The Commissioner opined that it was not practicable to identify the individual from the data as such and decided not to investigate the complaint. On appeal in *AAB No. 67/2005*, the AAB took into account the individual's own interpretation of some other characters and numbers displayed in the forum being his nickname and address, and concluded that the

data, taken together, were personal data as there was room for speculation that the individual was referred to in the poetic expression.

Paragraph (c) – "in a form in which access to or processing of the data is practicable"

2.22 Regarding paragraph (c) in the definition of "*personal data*", the question as to the meaning of the word "**form**" arose in a complaint to the Commissioner relating to a data access request. In the decision made, as one of the alternative grounds to support the finding of no contravention, the Commissioner observed that, insofar as the minutes of the meeting being requested could not be located by the hospital to whom the request was made, such minutes (even if they existed somewhere in the hospital's records) might not have satisfied the requirement in paragraph (c) of the definition of "*personal data*" to constitute the complainant's personal data at all. On appeal by the complainant to the AAB in *AAB No. 24/1999*, the AAB expressed its view that the information contained in the minutes was not "*personal data*" of the complainant and even if it was, there was no evidence to suggest that the hospital had lied about its existence in refusing to comply with his data access request.

2.23 The complainant then applied for judicial review of the decision of the AAB. In the case of *Tso Yuen Shui v. Administrative Appeals Board (HCAL 1050/2000, CACV 960/2000, unreported)* heard in the Court of First Instance, Yeung J., while upholding the AAB's decision, commented on the alternative grounds relied on by the Commissioner referred to above.

2.24 In particular, Yeung J. accepted the complainant's submission that the word "**form**" (appearing in the Chinese text as "存在形式") refers to the physical shape, structure, type, etc. of the data in question. Accordingly, the inability of the hospital to locate the minutes in question did not have anything to do with the "*form*" (i.e. paper form) of such data within the meaning of paragraph (c) in the definition of "*personal data*".

2.25 In illustrating the point, Yeung J. cited an example in which the form of the data is indeed relevant, that is, where the data user, although in physical possession of certain computerized data, has no access to the decoder necessary for decoding encoded data. Other cases, Yeung J. also pointed out, may be less clear, for example, where certain minutes of a meeting exist in the form of a paper document, but are contained in a time capsule buried 100 feet beneath a building.

2.26 On appeal by the complainant, the decision of Yeung J. was confirmed by the Court of Appeal. Accordingly, it is now clear that the mere impracticability of locating certain data (which impracticability, however, has nothing to do with the "*form*" of the data in the sense of their physical shape, structure, type, etc.) does not therefore prevent such data from amounting to "*personal data*" according to

its definition[7]. The word "*form*" is thereby given a wider meaning, embracing not just the "physical form" of the data but also its "state of existence", which paradoxically seems closer to the Chinese text.

Consideration of certain types of information

IP address

2.27 IP address is a specific machine address assigned by the Internet Service Provider to the user's computer and is therefore unique to a specific computer. In *AAB No.16/2007 (Shi Tao v Privacy Commissioner for Personal Data)*, the Commissioner received a complaint relating to the disclosure of information, including an IP address of a computer that disseminated the information. The Commissioner viewed that an IP address was information about an inanimate computer, not an individual. It did not contain information that "relates" to an individual. Further, it was noted that an IP address alone could not reveal the identity of the computer user, and thus lacking the characteristic of identifying an individual directly or indirectly. However, in certain circumstances IP address can constitute "personal data" when it is read together with other information, provided that the identity of an individual can be ascertained. The AAB agreed that the information together with the IP address disclosed did not amount to personal data of the complainant. It further mentioned that when IP address was coupled with such verified personal information as names, identity card numbers and addresses, it would, indeed, constitute "personal data".

2.28 In reaching its decision, the AAB had considered the following parts of the judgment in *Cinepoly Records Co. Ltd. and others v Hong Kong Broadband Network Ltd. and others* [2006] 1 HKLRD 255:-

> *"12. . . . An IP Address itself does not directly reveal the identity of the subscriber. But the ISP can track the IP address at a specific time or period to the records of their subscribers, which include names, Hong Kong ID card numbers and addresses.*
>
> *13. In short, by cross checking the IP address marked at a specific time or period with the ISP's records, the identity and address of the subscriber, whose computer has been used to upload the music files on the Internet by P2P program, including the WinMX software, can be revealed.*
>
> *14. Accordingly, with the assistance of the ISPs, the cloak of anonymity can be pierced and the true identity of the infringers may be revealed."*

[7] On the question of how such impracticability on the part of a data user to locate certain data may affect its duty to comply with a request for access to such data, the reader is referred to paragraphs 10.27 to 10.33 in Chapter 10.

2.29 The AAB concluded that: –

"Short of CCTV evidence, it would not be reasonably practicable from such information to ascertain that it was actually the Appellant who used the computer identified by the IP address to send out the relevant email at the material time. It could have been anyone, as long as he had access to that computer (or had the necessary password if one was required at all)."

Email address

2.30 Whether an email address may constitute personal data of the email account holder was also considered in *AAB No. 16/2007*. In the appeal, the AAB considered that the email address of "huoyan_1989" was not the complainant's name and was not the complainant's personal data.

2.31 In *AAB No. 25/2008*, the AAB considered that email address in some circumstances could be information from which the identity of an individual may be directly or indirectly ascertained. However, the AAB did not accept that an email address which corresponded to the initials of the complainant was, without more, sufficient to lead to the conclusion that the complainant's identity would become reasonably ascertainable from such an address. The AAB decided that the email address in question was not the complainant's personal data.

Biometric data like DNA and fingerprint data

2.32 Biometric data possesses the characteristics of being universal, unique and permanent[8]. Examples include DNA[9], fingerprint[10], vein pattern, characteristics of iris or even voice. They are sensitive in nature, considering that they are not artificial information which can be rendered obsolete when the individual finds necessary. For instance, an individual whose wallet is stolen may apply for cancellation or renewal of a credit card immediately, but in no circumstances can an individual be disconnected from his unique biometric data.

2.33 As regards collection of fingerprints, question has arisen where, instead of collecting the image of fingerprint, only numerical codes generated from the fingerprint were collected. In a complaint, it was found that a company installed a fingerprint recognition system to record attendance of its staff. Instead of collecting the fingerprints of the staff, the system collected certain features of the

[8] Description in the "Working Document on biometrics" adopted by Article 29 Data Protection Party of EU on 1 August 2003.

[9] In case number 2004001 (http://www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=221&casetype=B&cid=17), the Commissioner accepted DNA as personal data.

[10] In case number 2005012 (http://www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=257&casetype=B&cid=17), the Commissioner accepted fingerprints as personal data.

fingerprints and converted the features into numerical codes and recorded in that format. The Commissioner was of the view that although the system adopted by the company did not collect the whole image of the fingerprint, since the system could ascertain the identity of the staff, the data collected were "personal data" as defined by the Ordinance[11].

Examination Script

2.34 Students' answers to examination questions are generally not relating to the students, hence, are not the students' personal data. If, however, an examination script was marked with the examiner's comments or evaluation of the student's answers, the examination script may contain the student's personal data. In a complaint, a student made a data access request to a University for copies of his examination answer books and coursework. The University refused to comply with the data access request on the ground, among others, that the requested documents were not the student's personal data as the identity of the student was never an item of information that affected their comments and marking. Upon investigation, the Commissioner found that since the requested examination scripts contained the examiners' comments, the examination scripts and the examiners' comments, considered as a whole, should constitute the student's personal data[12].

[11] Full findings of the Commissioner can be found in Report Number: R09-7884, which can be downloaded from http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf.

[12] Full findings of the Commissioner can be found in Report Number: R08-10578, which can be downloaded from www.pcpd.org.hk/english/publications/files/R08_10578_e.pdf.

Chapter 3

The Meaning of "Collect"

The main questions:

- What is the meaning of the word "collect" as applied to personal data, in the light of the ruling made in the *Eastweek* case?
- How does the ruling affect the scope and interpretation of the Ordinance?

These questions are discussed in this chapter concerning the *Eastweek* case and the meaning of *"collect"*. They have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

The Eastweek case

3.1 The *Eastweek* case is of cardinal importance in the following two aspects:

- It defines the meaning of the word "*collect*" as it applies to personal data;
- In addition, it contains other important judicial *dicta* which help to provide clarification on the scope of the Ordinance.

3.2 The case arose from a complaint to the Commissioner. The complainant, while walking in the street one day, had her photograph taken by a photographer working for a magazine, without her knowledge or consent. The photograph was subsequently published in the magazine, accompanied by unflattering and critical comments on her style of dress. The matter caused embarrassment and inconvenience to the complainant amongst her clients and colleagues.

3.3 After conducting an investigation of the case, the Commissioner decided that the magazine in question contravened DPP1(2)(b) of the Ordinance on the ground that the personal data of the complainant in her photograph were collected by the magazine by unfair means. The magazine publisher lodged an application to the Court of First Instance for an order of *certiorari* quashing the Commissioner's decision.

3.4 In the judicial review hearing held in the Court of First Instance, Keith JA dismissed the application and the magazine publisher appealed to the Court of Appeal.

3.5 The Court of Appeal, by a 2-1 majority, reversed the decision in the Court of First Instance, and quashed the Commissioner's finding of contravention. According to the judgment given by Ribeiro JA, in deciding whether there was contravention of DPP1(2)(b), two elements must be present, i.e. (i) an act of personal data collection; and (ii) doing this by means which are unfair in the circumstances of the case. Although a photograph taken of a person constitutes his or her "*personal data*" within the definition of the Ordinance, the Court ruled that in the circumstances of the present case, there had been no "*collection*" of personal data by the magazine publisher and hence DPP1 was not engaged at all. The tests relied on by the Court in deciding whether "*collection*" took place or not give useful judicial interpretation on the meaning of the word "*collect*" as used in the context of the Ordinance.

The meaning of "collect"

3.6 The following statement from the judgment of Ribeiro JA (at 90I), which was repeated almost word for word in the judgment given by Godfrey VP (at 102D), is of particular importance in understanding an act of collection of personal data:

"It is . . . of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify."

3.7 The above statement lays down two conditions for an act of collection of personal data:

- the collecting party must be thereby **compiling** information **about** an individual (hereinafter referred to as "**Condition A**"); and
- the individual must be one whom the collector of information **has identified or intends or seeks to identify** ("**Condition B**").

3.8 Furthermore, the following statement from Ribeiro JA's judgment (at 93C) seeks to provide efficacy to Condition B:

"In my view, many of the other provisions of the Ordinance and in the data protection principles can only operate sensibly on the premise that the data collected relates to a subject whose identity is known or sought to be known by the data user as an ***important item of information***." (emphasis added)

3.9 Elsewhere in Ribeiro JA's judgment, reference was made to the facts of the case as well as other hypothetical scenarios. Referring to the facts of the case, the judge mentioned the **irrelevance** of the identity of a person photographed to the Appellant that published the photograph in its magazine, and the Appellant's **indifference** to such identity (91E to H). In an example quoted, he mentioned the **lack of concern** on the part of market surveyors about the identity of respondents (91J to 92B). In yet another example, he mentioned the **lack of interest** on the part of the photographers and publishers of newspapers about the identity of individuals whose photographs are published in newspapers (93B), etc. All these were considered factors giving rise to the inference that there was no collection of personal data.

3.10 From the above, it appears that Condition B may be refined by the addition of the following condition:

- the identity of the individual must be an **important item of information**[13] to the collecting party (**"Condition C"**).

3.11 Indeed, before the Court of Appeal's decision in the *Eastweek* case, the Commissioner itself, and probably many others, would have tended to interpret the term "*collect*" in a purely mechanical sense, as meaning the act of **physical acquisition** and then applied that meaning to the term "*collection of personal data*".

3.12 In contrast, the three conditions arising from the *Eastweek* case seem to infuse a **subjective** element into the notion of collection of personal data. For Condition B to apply, the collecting party must have already identified the individual in

[13] What is viewed as an important item of information is illustrated by Ribeiro JA in his judgment that the information shall be such as would enable a search against the requesting individual's name or other personal identifiers to yield an answer to a data access request made under section 18 of the Ordinance, or to identify the data subject under section 30 (matching procedure) to obtain his consent, or to give the opt out choice under section 34 when direct marketing activities are engaged in (93C to 94I of his judgment).

question or, at least, must seek or intend to seek to identify the individual. Furthermore, under Condition C, the identity of the individual must be an important item of information to the collecting party.

3.13 As for the application of Condition A, additional reference to this may be found in the following *dicta* in Ribeiro JA's judgment (94I):

"This entitlement (to make a data access request under DPP6) *can only make sense if the data user has* ***compiled the data collected in relation to each identified data subject****."* (emphasis added)

3.14 In most situations, Conditions B and C will follow simply as a corollary to Condition A. This is because when one is compiling information about a certain person, it is usually important to the compiler that the information regarding that person is not confused with that regarding any other person. Hence, at least in this basic sense, the "identification" of the person is "an important item of information" to the compiler.

3.15 It is important to note that, while the *Eastweek* case, involving an anonymous individual, was clearly a case of non-fulfilment of Conditions B and C, there can be other cases in which the identity of the individual is known, but Condition A is not satisfied. In all these cases by applying the rationale and tests laid down in the *Eastweek* case, the result is the same in that there is no collection of personal data.

3.16 The importance of Condition A may be illustrated by the following examples. First, in the case of an organization, in recording the minutes of a meeting on a particular matter, there is compilation of information about that matter only, but usually no compilation of information about any member or employee (whose identity is, of course, known to the organization) who spoke at that meeting, unless the matter happens to be about the individual speakers. In *AAB No. 24/1999*, the complainant made a data access request for a copy of minutes kept by the data user as records of the meeting. The complainant attended the meeting and the subject matter covered in the minutes was about a report of a boiler accident. On appeal against the Commissioner's finding of no contravention, the Chairman of AAB ruled that the contents of the minutes did not amount to the personal data of the complainant but was primarily concerned with the piece of equipment in question although it had recorded some of the remarks made by the complainant. The complainant applied for judicial review of the AAB's decision. In the judicial review in HCAL 1050/2000, the Court of First Instance applied the *Eastweek* case and ruled that the minutes concerned issues arising from the maintenance and repair of the boiler only, and the identity of the complainant was not an important piece of information to the data user. In the circumstances, the Court ruled that the contents of the minutes did not contain the complainant's personal data. The decision of the Court of First Instance was affirmed by the Court of Appeal in CACV 960/ 2000.

If there is no compilation of information about the member or employee, then Condition A is not satisfied, hence, according to the *Eastweek* case, there is no collection of personal data of any members or employees present at the meeting whose words may happen to be recorded in the minutes.

3.17 In another example, where an individual acting on his own initiative provides his personal data to a data user, such data are, from the point of view of the data user, unsolicited data. Despite the physical receipt of such data, it may be argued that the data user has not thereupon "*collected*" the data (unless the data, by a subsequent act or intent on the part of the data user, become part of a compilation of information about the individual held by the data user). In the case of *AAB No. 55/2006*, the AAB was of the view that a company which received complaint letters written by an individual on behalf of an organization with a view to dealing with the complaints was not collecting the individual's personal data. The actual circumstances surrounding the delivery and receipt of the data will need to be examined. As will be seen in the following section, in the above examples, whether or not there has been any "*collection*" of personal data will have important implications in terms of the legal obligations of the party concerned[14].

Consequence of absence of "collection"

3.18 Apart from providing a judicial meaning to the word "*collect*" and a data user's act of "*collection of personal data*", the decision of the *Eastweek* case contains other *dicta* that seem to confine the scope of the Ordinance. Examples were quoted in the judgment (92G to I) where photos were taken and published in the newspaper by the business editor in order to illustrate a social phenomenon, such as a crowd jostling in a queue for an initial pubic offering of shares or the purchase of flats in a new property development. A features editor may also publish photographs of teenagers smoking cigarettes in an article on health concerns. Likewise, a sports editor may print a picture of race goers at Happy Valley to illustrate attendance in record numbers. Though the persons being photographed in these situations might not all like the idea of having pictures containing their images published, insofar as their identities are not known to the publisher and there is no evidence to prove that their identities are of relevant concern to the publisher, it does not amount to "*collection*" of their personal data in the *Eastweek* sense.

[14] For enquiries made to the Commissioner concerning the application of the *Eastweek* case to the collection of personal data in particular situations, the reader may refer to other relevant cases in the Complaint and Enquiry Case Notes Section on the Commissioner's website, *http://www.pcpd.org.hk/english/casenotes/case.html.*

3.19 Particularly noteworthy is the following passage in Ribeiro JA's judgment (92J) after quoting the examples mentioned above:

". . . in none of those cases is the publisher or editor in question seeking to collect personal data in relation to any of the persons shown in the photographs and, in my view, the taking of such pictures and their use in such articles ***would not engage the data protection principles . . .*** *"* (emphasis added).

3.20 Of the six data protection principles in Schedule 1 of the Ordinance, DPP1 deals with the collection of personal data. It follows that, without collection of personal data, DPP1 would not be engaged. Where DPP1 is not engaged (i.e. there has not been a collection of personal data) in a given situation, the Ordinance is not applicable even though it may on its face appear to affect the privacy rights of an individual.

3.21 Accordingly, where there is no collection of personal data in the sense that there is no compilation of information about an individual identified or intended to be identified, there is no issue of "information privacy" affecting that individual and the matter falls outside the scope of the Ordinance.

3.22 Indeed, from a practical point of view, defining the meaning of the word "*collect*" provides clarity to the regulatory remit. This is because, given the very wide definition of "*personal data*" in section 2(1), the application of the requirements of the Ordinance in a mechanical manner could lead to unexpected practical difficulties, not to mention anomalies in relation to activities where the handling of personal data is not in issue.

3.23 Since the *Eastweek* case, the tests laid down therein have become useful guidance in facilitating the Commissioner to discharge his regulatory functions to determine and to form views on whether "*collection*" of personal data takes place in any particular case when complaints or enquiries come before him.

Information privacy and other privacy interests

3.24 Another important point to note from the judgment given by Ribeiro JA in the *Eastweek* case is that he has made clear the scope of privacy interests covered by the Ordinance to be as follows (95I to 96E):

"Personal data protection and not a general right to privacy

Mr. Griffiths stressed the limited protection to privacy afforded by the Ordinance. As its long title states, it is 'an ordinance to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith.' It is therefore not intended to establish general privacy rights against all possible forms of intrusion into an individual's private sphere or, as an American judge succinctly put it in an early textbook, a general right 'to be let alone' (Judge Cooley in Cooley on Torts, (2nd ed.) p.29, cited in Warren & Brandeis, 'The Right to Privacy' (1890) 4 Harv LR 193).

The distinction between other interests in privacy and the protection of personal data is well recognized. Thus, the Law Reform Commission of Hong Kong, whose Report on Reform of the Law Relating to the Protection of Personal Data provided the basis for the Ordinance as enacted, cited four privacy "interests" identified by the Australian Law Reform Commission as follows: –

(a) the interest of the person in controlling the information held by others about him, or 'information privacy' (or 'informational self-determination') as it is referred to in Europe;

(b) the interest in controlling entry to the 'personal place' or 'territorial privacy';

(c) the interest in freedom from interference with one's person or 'personal privacy';

(d) the interest in freedom from surveillance and from interception of one's communications, or 'communications and surveillance privacy'.

The Law Reform Commission made it clear that it was only concerned in its Report with 'information privacy'. Protection of that particular interest is plainly also the aim of the Ordinance."

3.25 Confusion is sometimes caused when a complainant, who fears his privacy right has been infringed, for instance, by being followed or watched by someone, lodges a complaint with the Commissioner. Unless it can be shown that information about him has been recorded and collected as a result, e.g. by being photographed or video taped, the infringement of personal as opposed to personal data privacy is a matter outside the jurisdiction of the Ordinance.

3.26 In respect of communications and surveillance privacy, it covers issues such as intrusion (by electronic or other means) into private premises and the interception of communications which sometimes overlap in certain situations. It is however to be noted that surveillance activities though causing interference with the privacy of the individual, do not necessarily involve the collection of "personal information"[15].

3.27 While personal privacy may be interpreted to mean the right to seclusion or solitude, the Hong Kong Law Reform Commission addressed the issue in its *Report on Stalking, October 2000* concerning reform of the law relating to domestic violence. The Commission recommended that when a person who pursues a course of conduct that amounts to harassment of another which he knows or ought to know amounts to harassment of the other, he should be guilty of an offence. In the area of media intrusion upon the privacy of individuals, the Law

[15] Hong Kong Law Reform Commission's Report on *Privacy: Regulating the Interception of Communications,* December 1996, at paragraphs 6 to 9. *The Privacy Guidelines: Monitoring and Personal Data Privacy at Work* issued by the Commissioner in 2004 focuses on the monitoring activities carried out by employers where personal data of employees are collected.

Reform Commission recognized the limitation of the Ordinance as it is not intended to establish general privacy rights against all possible forms of intrusion into an individual's private sphere[16].

3.28 Since the laws as they presently stand do not afford an aggrieved party the general civil remedy for invasion of the different types of privacy interest[17], it would no doubt be helpful if a general tort on invasion of privacy be introduced so as to widen the channel for redress made available to an individual whose privacy right has been intruded upon[18].

[16] The Report on *Privacy and Media Intrusion,* December 2004, at paragraph 9.39.

[17] Section 66 of the Ordinance does provide for a right to claim compensation by an individual who suffers damage which includes injury to feelings by reason of a contravention of a requirement of the Ordinance by a data user.

[18] Law Reform Commission's Report on *Civil Liability for Invasion of Privacy* issued in December 2004. In the Law Reform Commission's report issued in March 2006 on *Privacy: The Regulation of Covert Surveillance*, two criminal offences were proposed, making it an offence in respect of the "*entering and remaining on private premises as a trespasser with intent to observe, overhear or obtain personal information*" and also an offence for a person "*to place, use, service or remove a sense-enhancing, transmitting or recording device (whether inside or outside private premises) with the intention of obtaining personal information relating to individuals inside the private premises in circumstances where those individuals would be considered to have a reasonable expectation of privacy*."

Chapter 4

Meaning of "Data User"

The main questions:

- What is the meaning of the term "data user"?
- What is the relevance of the *Eastweek* case to such meaning and how such meaning was applied in AAB cases?
- How is such meaning affected by section 2(12)?
- How does the term "data user" apply to an individual and to the government?
- Can two or more persons be jointly accountable as data users?
- How does section 4 operate to affect the obligations and liabilities of the data user?

The questions discussed in this chapter concerning the meaning of *"data user"* are selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

Meaning of "data user" with reference to the *Eastweek* case

4.1 The term "**data user**" is defined in **section 2(1)** of the Ordinance as follows:

> *" 'Data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data."*

4.2 A person who satisfies the definition of a "*data user*" is obliged to observe and comply with the relevant provisions and requirements of the Ordinance. As mentioned in Chapter 3, the Court of Appeal judicially defined the meaning of the word "*collect*" in the *Eastweek* case. Thus, it could be inferred that a person who passes the tests laid down in the *Eastweek* case is a "*data user*" falling within the definition under section 2(1) as a person who *". . . controls the collection . . . of the data"*.

4.3 A common example is found in the purchase of newspapers or magazines by an individual. He might have physically collected or held the personal data of persons mentioned in the newspapers or magazines through the act of a purchase, however it would be artificial to thereby treat him as assuming the role of a "*data user*" with the attendant duties and obligations. In *AAB No. 22/1997*, the AAB ruled that a secretary who was merely responsible for transmitting the document passed to her by another staff member of the company did not fall within the definition of a "*data user*" as she did not *"control the collection, holding or processing of the data contained in the document"* and there was no evidence to show a breach of DPP4 when the document was found lost in transit.

4.4 The situation quoted above might be different if the reader of the newspaper or magazine intends to compile information about an identified individual, for example, a celebrity or public figure for the purpose of, say, the later publishing of a dossier about that person. It might then be argued that the reader has become a data user through his act of collection of the personal data in question.

4.5 While *Eastweek* is the landmark case which judicially defines the word "*collect*" and therefore has an important bearing on the meaning of the term "*data user*", there was an earlier AAB decision on the issue of the meaning of "*data user*". The AAB came to a conclusion consistent with the subsequent *Eastweek* case, although the reasoning was not set out as fully. It is the case of *AAB No. 4/1997* which was an appeal that resulted from a decision by the Commissioner not to investigate further a complaint brought to him. The complaint was made by a hospital employee concerning an incident in which three hospitals had permitted to be posted on their notice boards an open letter written by another employee, which contained the personal data of the complainant. In the appeal, the AAB upheld the Commissioner's decision not to investigate the case further. In this connection, the AAB observed:

"*Even if the hospitals had allowed or given consent for such posting, the hospitals could not be taken as data users, since they only permitted the posting of the letters but they had no control on the content or data mentioned in the open letter.*"

4.6 If one were to apply the *Eastweek* rationale to this AAB case, it might be argued that by not having compiled information about the complainant, the hospitals did not "*collect*" the complainant's personal data in the *Eastweek* sense, which as a result, did not render the hospitals "*data users*" vis-à-vis the personal data in question.

Meaning of "data user" with reference to recent AAB cases

4.7 In the case of *AAB No. 55/2006*, an individual on behalf of an organization wrote two letters to a regulatory body concerning a complaint against a company. The regulatory body forwarded the two letters to the company for their reply to the individual directly. The individual asked the company for copies of those two letters together with the covering letter from the regulatory body, but the company refused to do so. The individual complained to the Commissioner that, in contravention of section 19 of the Ordinance, the company had failed to provide him with copies of the requested letters within 40 days of his request. The Commissioner found that (1) the company had received those two letters for the purpose of dealing with the complaint the organization made to the statutory body against the company; (2) the correspondence between the company and the regulatory body was about the complaint and did not concern the individual personally; (3) there was no collection of personal data about the complainant by the company and therefore the Ordinance did not apply; and (4) no investigation or further investigation was necessary. On appeal, the AAB upheld the Commissioner's decision and ruled that:

"A person who does not collect, hold, process or use the personal data is not a data user in relation to that data. He is not obliged to comply with a data access request in relation to that data."

4.8 In the case of *AAB No. 3/2005*, a student complained against a school for failing to comply with his data access request. The school denied that it was the data user because it did not hold or control the requested data. The school then diverted the request to a closely connected college, which was the data user, for processing the request. The complainant insisted that it should be the school, not the college, to comply with his request. The AAB ruled that the school and the college were separate legal entities. Although the school was closely connected to the college in that it had control over the college on policy matters, the school was not the data user of the requested personal data in that it did not control the collection, holding, processing or use of the requested data. The college collected the personal data for its own use. There was no evidence that the college had ever transferred

the requested data to the school or that the school had control over the requested data.

4.9 In the case of *AAB No. 16/2007*, the AAB considered the question whether a data user's control over personal data could have been "vitiated" when the data user was compelled by the operation of PRC law to disclose the personal data. The AAB decided that the data user still retained control over the personal data, and the fact that disclosure of the relevant information in order to comply with local laws does not affect whether the data user was in control of the information or its disclosure.

Section 2(12)

4.10 Another point worth noting regarding the meaning of "*data user*" is the exclusion under **section 2(12)**, which provides:

> *"(12) A person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes."*

4.11 To understand the meaning of section 2(12), one has to examine what is meant by data being held, processed or used "*solely on behalf of another person*" and not for one's "*own purposes*".

4.12 Take the example of a garbage collector retained for providing the service of regularly disposing of garbage. Unless it can be shown that he has his own purpose in collecting the personal data that might be found in the garbage, he is generally not viewed to have satisfied the definition of a data user. He simply holds and processes the materials collected for the sole purpose of garbage disposal and without any of his own purpose to serve, with respect to the personal data that might be contained in the garbage. Another example is found in the case of the internet service provider ("the ISP") that by merely providing the means of internet linkage it does not thereby render the ISP a data user especially when it does not control the collection, holding, using or processing of the personal data of individuals accessing and using such online functions as, for example, chat rooms to disseminate and communicate with other users. The ISP is thus to that extent not a data user as excluded under section 2(12).

Meaning of "person" in the context of data user

4.13 Although one would expect that the mischief the Ordinance primarily seeks to prevent is the abuse of personal data by institutional data users, there is nothing

in the definition of *"data user"* to confine its meaning to institutions alone. Accordingly, insofar as an individual "*controls the collection, holding, processing or use*" of personal data, the individual is a data user in relation to the personal data and will consequently be subject to the full force of the requirements of the Ordinance.

4.14 Another point to note in the interpretation of "*data user*" and the word "*person*" is in relation to the government. In this connection, the word "**person**" is defined in **section 3** of **the Interpretation and General Clauses Ordinance (Cap. 1)** as follows:

> *"'person' includes any public body and any body of persons, corporate or unincorporate, and this definition shall apply notwithstanding that the word 'person' occurs in a provision creating or relating to an offence or for the recovery of any fine or compensation."*

4.15 The term "**public body**" is, in turn, defined in **section 3** of Cap. 1 as follows:

> *"'public body' includes –*
>
> *(a) the Executive Council;*
>
> *(b) the Legislative Council;*
>
> *. . .*
>
> *(c) any District Council;*
>
> *. . .*
>
> *(d) any other urban, rural or municipal council;*
>
> *(e) any department of the Government; and*
>
> *(f) any undertaking by or of the Government."*

4.16 The government as a whole, is in possession of a very large amount of personal data in relation to the citizens of Hong Kong. Such data have been collected and are retained by different government bureaux and departments, according to their respective functions, such as law enforcement, tax, social welfare, etc.

4.17 In the light of the definitions of the terms "*data user*", "*person*" and "*public body*", one could in theory choose to interpret such terms to refer to either individual government bureaux and departments as separate data users, or, the entire government (being a body of persons) collectively as one single data user. However, in view of the vast array of functions the government performs in relation to individual citizens which involve the collection and use of personal

data, the latter approach would effectively empower the government to collect, virtually without limitation as to scope, the personal data relating to those citizens, and to exchange such data freely among its various bureaux and departments. This would create an anomalous result that runs contrary to one of the principal tenets of the Ordinance, namely, to protect the personal data privacy of individuals by reference to a linkage between the purpose of collection of data and their intended use by the data user in relation to that purpose.

4.18 Hence, so far as the relationship between the government and citizens is concerned, the operational stance taken by the Commissioner is to interpret such terms to refer to each individual government bureau and department as a separate data user[19]. In accordance with this, under DPP1(1), a government department is not allowed to collect personal data in excess of those required for its own function and activity (as opposed to those of other government departments). Furthermore, the transfer of citizens' data between departments is subject to the relevant restrictions under DPP3. For a more comprehensive discussion of DPP1(1)(c) and DPP3, the reader is referred to paragraphs 5.1 to 5.14 in Chapter 5 and Chapter 7.

Joint data users

4.19 The definition of the term "*data user*" extends to apply where more than one person is found to be in control of the collection, holding, processing or use of the data, in which case they are jointly regarded as data users who are obliged to observe and comply with the provisions and requirements of the Ordinance.

4.20 An example is found in the case in which two or more persons who jointly or in common hold the legal title of real property leased out to a tenant for rental profits. They may have collected the tenant's personal data in such circumstances that they jointly control the holding, processing or use of such data. Thus, when a dispute arises or a complaint is lodged by the tenant regarding the improper handling of his personal data, all of the owners who satisfy the definition of "*data user*" will be jointly held accountable for the act or practice in question.

4.21 Another common situation in which more than one person may qualify as a data user is found in cross-marketing activities whereby the personal data of customers held by company "A" (the transferor company) are transferred to another company "B" (the partner company) for the purpose of conducting activities in the nature of a "joint marketing campaign". The joint marketing campaign may involve the marketing of products or services of A or B or both to customers of A and/or B.

[19] There may, however, be certain exceptions to this general rule, including, for example, the case of a civil servant who is posted to different departments from time to time. In this situation, the government as a whole may be regarded as the data user of personal data about the civil servant relating to his employment.

When both A and B jointly control the collection, holding, processing or use of the data, they will be regarded as joint data users under the Ordinance[20].

4.22 When direct or cross-marketing activities are carried out whereby a potential customer's personal data are first used for marketing purposes, the data user is obliged under section 34(1) of the Ordinance to inform him or her of his or her right to "opt-out" of such marketing activities. If the data user continues to use personal data about the individual for direct marketing after receiving his opt-out request, this may give rise to an offence. In order to effectively comply with the statutory requirements under section 34(1), it has been the view of the Commissioner that the data user shall keep and maintain an opt-out list of individuals who have chosen not to receive further marketing approaches. If direct marketing activities are carried out by the partner company and a customer exercises his opt-out right, the partner company should inform the transferor company about the request made by the customer. The partner company, as well as the transferor company, shall maintain the opt-out list. Thus, both the transferor company and the partner company as data users shall not make any further marketing approaches to those customers who "opted-out" [21] from the direct marketing activities in question.

Section 4

4.23 When a person falls within the definition of "*data user*", the Ordinance applies to govern his act and conduct since **section 4** provides that:

> *"(4) A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance."*

4.24 Concerning the acts and practices that are required under the Ordinance, the six data protection principles laid down in Part I of the Ordinance are of vital importance to guide one's act or practice in handling personal data[22]. It is for this reason that they are selected in the subsequent chapters as topics for discussion[23]. Although non-compliance with any of the data protection principles does not *per*

---

[20] Even if the joint marketing campaign does not involve transfer of customers' personal data, A and B may still be considered as joint data users as long as they jointly control the collecting, holding, processing or use of the data.

[21] The Commissioner issued a Guidance Note on cross-marketing activities which provides a summary of the salient points to be observed and noted by data users when carrying out such activities. The Guidance Note can be downloaded from the Commissioner's website, *http://www.pcpd.org.hk/english/publications/files/cross_marketing_e.pdf*.

[22] A chart illustrating the relationship of the data protection principles in the personal data handling cycle is found in Appendix II of this Book for easy reference.

[23] A checklist for data users in ensuring compliance with the requirements of the Ordinance is found in Appendix III of this Book. The remedies that a data subject may resort to if his personal data privacy interest is infringed are summarized in Appendix IV.

se attract criminal sanction, when coupled with provisions in the Ordinance that are relevant to the application of the data protection principles, the wrongful act or practice may constitute an offence under the Ordinance. For instance, section 19 of the Ordinance obliges the data user to comply with the data access request and it is regarded as a statutory requirement in relation to compliance with DPP6. Similarly, section 26 provides for the erasure of personal data no longer required and it is also a statutory requirement applicable to compliance with DPP2(2). Under section 64(10), the contravention of a requirement of the Ordinance, other than the data protection principles, is an offence liable on conviction to a fine at level 3.

4.25 As for acts that are permitted under the Ordinance which would otherwise render the act in question contravention of the data protection principles, the exemption provisions in Part VIII of the Ordinance are of particular relevance and the application of these exemption provisions are discussed in more detail in Chapter 12.

Chapter 5
Data Protection Principle 1

The main questions:

- What are the general requirements under DPP1(1)?
- In particular, for the purpose of DPP1(1)(a), how is the "function and activity" of a data user ascertained?
- What are the general requirements under DPP1(2)?
- What are the common examples of collection of personal data by unfair means?
- What are the general requirements under DPP1(3)?
- When do such requirements apply to the collection of personal data, and how?
- What should be considered in attempting to collect biometric data?

The questions of the purpose and manner of collection of personal data discussed in this chapter concerning DPP1 have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

DPP1(1)

5.1 **Data Protection Principle 1(1)** in Schedule 1 of the Ordinance provides as follows:

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

5.2 The wording used in DPP1(1) allows considerable flexibility in interpretation. In applying this, the Commissioner will take into account all relevant factors according to the circumstances[24] and is mindful about the proper application of the rules of interpretation stated in paragraphs 1.6 to 1.8 in Chapter 1.

5.3 For the purpose of paragraph (a), in the case of a government bureau or department or a public body being the data user, the Commissioner will generally regard the "*function and activity*" of the data user as being restricted to its generally recognized functions, whether conferred on it by statute or otherwise. Hence, a government department should not collect personal data for the sole purpose of assisting another department, where such collection is directly related to the function and activity of the other department, but not to that of its own[25].

5.4 The same approach is adopted in the case of data users that are private organizations, but perhaps with greater difficulty. The function or activity of a private organization may change in response to changes in the business environment, making it harder to define its scope of business precisely.

5.5 Indeed, given the advent of low cost – high performance technology for information storage, an organization may easily be tempted to collect from a variety of sources and hoard personal data (especially those of prospective customers or clients) just in case such data may become useful at some future date. Insofar as there is an intention on the part of the data user to compile information about these identified or identifiable

---

[24] For enquiries made to the Commissioner concerning the application of DPP1(1) to the collection of personal data in particular situations, the reader may refer to relevant cases in the Complaint and Enquiry Case Notes Section on the Commissioner's website, *http://www.pcpd.org.hk/english/casenotes/case.html*.

[25] For a discussion of the treatment of different government bureaux and departments as separate data users, the reader may refer to paragraphs 4.16 to 4.18 in Chapter 4.

individuals in the *Eastweek* sense[26], the personal data of these data subjects are treated as having been collected. The indiscriminate collection of personal data, in particular, if it involves sensitive personal data, is likely to be viewed by the Commissioner as a contravention of DPP1(1), in that it may be considered not directly related to, or even excessive for, the organization's function and activity.

5.6 In a case that came before the Commissioner, a job seeker sought the service of an employment agency and the employment agency requested the deposit of a copy of the job applicant's HKID on the ground that it would guarantee the payment of commission by the employer on successful placement of jobs. The Commissioner found the act and practice of collecting a copy of the HKID excessive having regard to the fact that the payment of commission is a contractual agreement with the employment agency and the prospective employer. In collecting personal data from job applicants, a prospective employer should be mindful of the need to demonstrate that the personal data to be collected are directly relevant to the purpose of identifying suitable candidates. For example, these may include work experience, job skills, competencies, academic or professional qualifications, good character and other attributes required for the job.

5.7 Three codes of practice have so far been issued by the Commissioner under section 12(1) of the Ordinance which provide useful references setting out the scope of personal data that, in the opinion of the Commissioner, may be collected under DPP1(1) in respect of the relevant industries and/or fields of activity[27]. The collection of personal data by a data user in excess of that expressly permitted under the relevant code of practice will give rise to a presumption of contravention of DPP1(1) under section 13 of the Ordinance in proceedings brought before a magistrate, a court or the AAB.

5.8 In the case of collection of HKID numbers by a management company of drivers who visited the car park of a commercial building open to public, the Commissioner found, in a complaint case brought before him, contravention by the management company of DPP1(1) and Clause 2.3 of the *Code of Practice on the Identity Card Number and other Personal Identifiers* when such collection was not shown to be necessary for the prevention of crime as alleged. The management company appealed against the enforcement notice issued by the Commissioner. The appeal was dismissed by the AAB in *AAB No. 41/2004* and the decision of the Commissioner upheld.

---

[26] See Chapter 3 on the *Eastweek* case and the meaning of "*collect*".

[27] See Appendix I of this Book on a brief description of the following Codes of Practice issued by the Commissioner:
a. Code of Practice on the Identity Card Number and Other Personal Identifiers;
b. Code of Practice on Consumer Credit Data; and
c. Code of Practice on Human Resource Management.
Full versions of the above Codes can be downloaded at http://www.pcpd.org.hk/english/publications/code_pra_ex.html.

5.9 In other situations where there is no applicable code of practice to refer to for ensuring compliance with DPP1(1), a data user should nonetheless, before the collection of any personal data, give due consideration to relevant factors such as:

- the particular function or activity to which the collection of the data concerned is considered directly related;
- the degree of sensitivity of such data;
- the legitimate purposes to be served in collecting the personal data and the adverse impact on personal data privacy;
- whether there is a real need (i.e. the degree of likelihood of such need arising) for the data to be collected in order to carry out that function or activity;
- whether there is any realistic and less privacy intrusive alternative for attaining the purpose of collection.

5.10 Collection of certain personal data in marketing activities may contravene DPP1(1) if there is no actual need to collect those data. For the purpose of marketing, collection of name and contact information may be allowed if it is necessary to use those data to contact the relevant persons. While collection of background information of the relevant individuals, such as age, sex, income and occupation, may provide valuable information for the purpose of enhancing the chance of successful promotion, such collection is only allowed if the same purpose cannot be achieved by less intrusive alternative. For instance, data user shall not collect age and income when information about age group and income group are already adequate for assessing the background of the relevant persons.

5.11 Collection of HKID number should be more cautious. Other than the necessity to comply with the general requirements of DPP1, data users should be aware of the restrictions imposed by clause 2.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers.

5.12 In a complaint handled by the Commissioner, a food company required purchasers of its food products who wished to be registered for a lucky draw to provide it with the purchasers' names, contact information, HKID numbers and dates of birth. Prizes of the lucky draws included credit card free spending credit and gift vouchers worth of several thousand dollars. Upon investigation, the Commissioner found that there were two categories of lucky draw tickets, namely tickets placed inside the products all bearing the same lucky draw number, and tickets that were attached to the package boxes of other products with unique lucky draw numbers. The Commissioner decided that if participants were issued with unique lucky draw numbers, the company should be able to identify the winners by checking the lucky draw numbers together with the names and addresses of the winners. As such, collection of HKID numbers of those participants was excessive and in contravention of DPP1(1). As for those participants holding the same lucky draw

numbers, the Commissioner considered that collection of their HKID numbers was to avoid damage or loss which was more than trivial in the circumstances permitted under clause 2.3.3.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers. The Commissioner also considered that it was unnecessary for the company to collect the participants' date of birth for the purpose of contacting them and verifying their identities[28].

5.13 In another case, a credit company sent letters without naming the recipients, inviting the recipients to supply to it "simple information" about four individuals in the household and upon verification, the individuals would receive a supermarket gift coupon of $20. The "simple information" required by the credit company included HKID numbers of the individuals. The credit company claimed that the HKID numbers of the individuals were for identification purpose to prevent those individuals from redeeming more than one coupon by multiple submissions. The Commissioner considered that since the possible loss was only $20, the collection of the HKID numbers of the individuals was not the one permitted under clause 2.3.3.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers.[29]

5.14 In relation to the collection of copy of HKID, clause 3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers has prescribed situations under which such collection is allowed. Clause 3.3.1 made clear that no collection of copy of HKID should be allowed merely to safeguard against clerical error in recording name or HKID number of the individual. There was a complaint against a government department for taking photograph of the complainant's HKID for the purpose of verifying the complainant's identity as a witness. The Commissioner opined that such act was contrary to the relevant DPP and the Code. The government department agreed that collection of the photographed image of the complainant's HKID was unnecessary and deleted the image.

DPP1(2)

5.15 **Data Protection Principle 1(2)** in Schedule 1 of the Ordinance provides as follows:

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

[28] Details of the Commissioner's findings are contained in the Investigation Report Number R09-3658, which can be downloaded from http://www.pcpd.org.hk/english/publications/files/Food_company_Report_e.pdf.

[29] Details of the Commissioner's findings are contained in the Investigation Report Number R07-6168, which can be downloaded from http://www.pcpd.org.hk/english/publications/files/R07-6168_e.pdf.

5.16 The wording used in DPP1(2), especially paragraph (b), allows considerable flexibility in interpretation. To the Commissioner, an obvious example of data being obtained by unfair and perhaps also unlawful means is personal data being obtained through deception or coercion – for instance, the offering of free gifts on the street by a survey conductor to attract passers-by to complete a questionnaire and to provide his or her personal data when the true purpose is to collect and amass personal data for sale in bulk to direct marketing companies for profits.

5.17 A similar, but perhaps less clear, situation in which the issue of DPP1(2)(b) may arise, relates to capturing and recording the visual image of an individual by means of a camera, video recorder or other device[30]. One illustration of the Commissioner's position in this regard may be found in the investigation report published[31] in respect of the covert video taping of the activities of a female hostel inmate of a university by her friend using a hidden camera installed in her room without her knowledge. The Commissioner found that the manner of collecting the complainant's personal data was highly privacy intrusive and that the means adopted without the knowledge and consent of the complainant was unfair in the circumstances of the case, in breach of DPP1(2).

5.18 In a case concerning secret recording of conversation, the Commissioner considered that the collection was by unfair means. The conversations were secretly recorded in a lunch between a teacher and his supervisor. The purpose of the lunch was to discuss the teacher's performance and to offer the teacher some counseling. The recording was made without the knowledge of the supervisor and the recorded conversations were subsequently uploaded onto a website accessible by the public. In the appeal *AAB No. 46/2006*, the AAB opined that the subsequent use of the recorded conversations indicated that the recording was not made with the bona fide intention of keeping a record of the meeting. The AAB agreed that the means of collection of the personal data contained in the recorded conversations was unfair contrary to DPP1(2).

5.19 Fairness of means of collection was considered extensively in a case concerning collection by an airline of past medical data of its cabin crew members. The airline required its cabin crew members who took long or frequent sick leave to consent

---

[30] For collection of employees' personal data through telephone, email, internet or video monitoring carried out by an employer, the Commissioner has, in the exercise of his powers under section 8(5) of the Ordinance, issued a *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* in December 2004 which gives practical guidance for employer's consideration. The 3 A's concept was introduced, i.e. assessment, alternatives and accountability for the employer to take into account before deciding whether to engage in any employee monitoring activity.

[31] Report No. R97-1948 issued by the Commissioner on 13 October 1997 under section 48(2) of the Ordinance. See also Report No. R05-7230 issued by the Commissioner on 8 December 2005 in respect of the collection of employees' personal data by an employer for a suspected crime of theft through the installation of pinhole cameras. The employer was found to have contravened DPP1(2) in collecting employees' personal data by unfair means in the circumstances of the case. The Report can be viewed at *http://www.pcpd.org.hk/english/infocentre/files/R05-7230_e.pdf*.

to the release of their medical data for the previous 12 months which related to the causes of their absences. The Commissioner found that there was an element of threat in the manner the airline expressed its requirement especially through its newsletter in which it was indicated that failure to provide consent would be treated as a disciplinary and grievance matter. To that extent, the Commissioner decided that the airline's means of collection of the past medical data was unfair in the circumstances. On appeal in *AAB No. 3/2007*, the AAB upheld the decision of the Commissioner.

5.20 The airline applied to the Court of First Instance of the High Court for a judicial review of the decisions made by both the Commissioner and the AAB[32]. The High Court decided that in circumstances when disclosure of personal data is properly rendered mandatory, it is necessary for the airline to advise the cabin crew of the adverse consequence of failing to make disclosure, hence, the advice given by the airline to its cabin crew members did not of itself constitute a threat or the exertion of undue influence to the latter. The Court quashed the decisions of the Commissioner and the AAB.

5.21 The learned judges commented that the disquiet expressed by the Commissioner and the AAB, "*was to a material degree, based on the blunt and brusque manner in which certain of the information concerning the failure to consent to deliver up medical records under the [airline's relevant policy] was conveyed to cabin crew members*" and the "*threatening or oppressive tone of relevant literature*". In the learned judges' views, "*fairness is a broad principle and, as to the manner in which personal data is to be collected, is capable of encompassing the form in which relevant information is conveyed as well as the substance of that information*".

5.22 The Commissioner is of the view that, given that the airline was under a duty to comply with Directive 360 of the Civil Aviation Directives in ensuring that cabin crew members remain medically fit to discharge the duties specified in the operations manual, application of the High Court decision should be confined to its own facts and circumstances. The Commissioner considers that the case does not affect the principles that collection of past medical records of employees by the employer must be justified on the ground that such collection is necessary, adequate and not excessive and are collected by means that are fair in the circumstances under DPP1.

5.23 Another example of collecting personal data by unfair means is the resort to the use of blind advertisements published without disclosing the identity of the data user where job applicants are lulled into sending in resumes to an unknown party[33]. The situation is even worse where there is in fact no recruitment exercise

[32] HCAL 50/2008

[33] See clause 2.3.3 of the *Code of Practice on Human Resource Management*.

being conducted and the advertisement is placed solely as a pretext to collect personal data for use in conjunction with other purposes, such as the compilation of a list of individuals for carrying out direct marketing activities.

5.24 The concept of fairness can also be illustrated by collection of consumer credit data pursuant to the Code of Practice on Consumer Credit Data issued by the Commissioner. Pursuant to clause 2.11 of the Code, for every access to the database of a credit reference agency by a credit provider, the credit provider shall confirm the purpose of access to the data in order to prevent arbitrary or indiscriminate access to these sensitive personal data.

5.25 The means of collection is unlawful if it is prohibited under any law[34]. The theft of one's credit card or bank account information is a typical example of collection by unlawful means.

DPP1(3)

5.26 **Data Protection Principle 1(3)** in Schedule 1 of the Ordinance provides as follows:

> *"(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that –*
>
> *(a) he is explicitly or implicitly informed, on or before collecting the data, of –*
>
> *(i) whether it is obligatory or voluntary for him to supply the data; and*
>
> *(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and*
>
> *(b) he is explicitly informed –*
>
> *(i) on or before collecting the data, of –*
>
> *(A) the purpose (in general or specific terms) for which the data are to be used; and*
>
> *(B) the classes of persons to whom the data may be transferred; and*

[34] The interception of the communications of individuals by law enforcement agencies carried out under section 33 of the Telecommunications Ordinance, Cap. 106 was ruled in the case of *Leung Kwok Hung and another v HKSAR* [2006] HKCU 230 to be inconsistent with Articles 30 and 39 of the Basic Law and hence unconstitutional. With the introduction of the Interception of Communications and Surveillance Ordinance, Cap. 586 in 2006, personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of the Ordinance, including the requirements under DPP1.

> *(ii) on or before first use of the data for the purpose for which they were collected, of –*
>
> *(A) his rights to request access to and to request the correction of the data; and*
>
> *(B) the name and address of the individual to whom any such request may be made,*
>
> *unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6."*

5.27 DPP1(3) requires a data user to inform the data subject of the prescribed information on or before collection of his personal data. Such requirement is however applicable only to collection of personal data directly from the data subject. It implies that personal data may be collected from a third party in the absence of the data subject's consent or even knowledge without contravening DPP1(3). The AAB in *AAB No.64/2005* expressed their concern that in such circumstances the privacy of the data subject would not be well protected because the data subject would not have any redress against the data collector, albeit the disclosure of personal data by the third party has to be in compliance with DPP3.

When does DPP1(3) apply?

5.28 Given the wording used in DPP1(3), i.e. *"from whom personal data are or are to be collected is the data subject"*, the duty to inform the data subject of the matters prescribed thereunder is taken to arise in situations when the data in question are collected directly from the data subject. Hence, the notification requirement under this principle is generally considered by the Commissioner not to be applicable where the personal data in question are:

- collected from a third party;
- unsolicited and supplied by the data subject; or
- generated by the data user itself (this is possible because the definition of "*data*", as referred to in paragraph 2.1 of Chapter 2, includes an expression of opinion in a document).

5.29 The notification obligation under DPP1(3) arises in commonly encountered situations of collection of personal data, such as when:

- an individual is asked to provide written information about himself (e.g. by filling in a form);
- the individual is asked to provide oral information to be recorded (e.g. making a statement to the Police);
- personal data are generated by the data user in the course of its conduct with the data subject (e.g. entering into employment or banking transactions); or
- personal data about the individual are obtained through automatic or scientific devices (e.g. recording a telephone conversation, conducting a medical checkup, etc.)

Obligation not absolute – "all practicable steps"

5.30 In situations where the condition is satisfied, DPP1(3) requires "a*ll practicable steps*" to be taken to ensure that the data subject is informed of the matters mentioned therein on or before the collection of the data. As mentioned previously, the word "*practicable*" is defined under section 2(1) as meaning "*reasonably practicable*".

5.31 Accordingly, the requirement under DPP1(3) does not apply in those situations where it is not reasonably practicable to inform the data subject, examples of which may include the following:

- Law enforcement – where it is required in the course of law enforcement to collect the personal data of an individual without prior notification.
- Employment – where personal data were collected as evidence of an employee's dereliction of his duty, e.g. video images showing that an employee was sleeping while on duty (*AAB No. 23/2008*).
- Receiving unsolicited data from the data subject – the term "unsolicited data" is used here to denote data received without having been requested. In relation to such data, it is impractical in most cases to expect the recipient to give notice pursuant to DPP1(3) to the sender, for example, the voluntary sending of a job resume or name card to a company to seek employment or solicit business.
- Subsequent "collection" in the *Eastweek* sense – even if the recipient does "*collect*" the data in the sense of the *Eastweek* case (according to that case, there would be collection of personal data if, having received the unsolicited data, the recipient subsequently compiles information about the data subject).

5.32 In situations where a data user is required to inform the data subject from whom personal data are collected about the matters mentioned in DPP1(3), the next question to ask is whether the effort made to inform the data subject sufficiently constitutes "*all reasonably practicable steps*" as required under DPP1(3). For

example, where a notice has been posted up, matters such as the prominence of the notice, whether and the manner by which the data subject has been told about the existence of the notice are relevant for consideration. Where direct communication with the data subject is not possible, whether there may be other practical alternatives to bring the notice to the attention of the data subject, are also matters that need to be taken into account in deciding whether "*all reasonably practicable steps*" have been taken in compliance with DPP1(3). In *AAB No. 25/1999,* the AAB found the hospital was in breach of DPP1(3) by having failed to take all reasonably practicable steps in bringing the PICS to the attention of its private patients as the notice displayed in the waiting room was not prominent enough.

Matters to be informed

5.33 Turning then to the specific matters of which an individual needs to be informed under DPP1(3), these fall under either paragraph (a) or paragraph (b). For those matters falling under paragraph (a), it is required that the individual be "**explicitly or implicitly**" informed of such matters. Accordingly, the Commissioner takes the view that explicit notification of those matters will not be required where it is obvious from the circumstances. For example, where there is an invitation to submit contact data for inclusion in a mailing list for a product promotion, it is not necessary to state explicitly that provision of data is purely voluntary, which is obvious from the circumstances. Another example is where a policeman, in discharging his duties, asks a man in the street to provide his name and address in which the obligatory nature of such request is also obvious from the circumstances. However, in situations where a data subject is given an option to decide whether to supply voluntarily his personal data for use by the data user for a number of different purposes, it is good practice for the data user to give clear indication of the choice to be given to the data subject to avoid misunderstanding.

5.34 In contrast, under paragraph (b) a data user is required to take all reasonably practicable steps to ensure the individual is "**explicitly**" informed of the matters mentioned therein. Accordingly, notification is necessary even if it may appear to be stating the obvious. There is however no requirement for the notification to be in writing, although the Commissioner would consider it to be good practice to follow, especially for organizational data users. It is common practice for the notifications required under DPP1(3) to be conveniently included in one written statement, generally referred to as a **Personal Information Collection Statement** or, in short, "**PICS**".

5.35 Under DPP1(3)(b)(i), the individual is to be explicitly informed of "*(A) the purpose (in general or specific terms) for which the data are to be used, and (B) the classes of persons to whom the data may be transferred*", on or before the collection of the data.

5.36 Of the various kinds of information of which an individual has to be informed under DPP1(3), the above item (A) is perhaps the most important. This is because many of the requirements of the Ordinance (including, for example, those under DPP1(1), DPP2, DPP3, DPP5 and section 26, as well as some of the exemptions under Part VIII) apply by reference to the "*purpose*" of the collection of the data. Hence, a data user should make sure that such purpose is reflected correctly and adequately in the PICS. It is noteworthy that the purpose as stated in the PICS is one of the relevant factors, though not necessarily the sole factor, that the Commissioner will look at in determining whether there is contravention of any of the provisions of the Ordinance. For a more complete discussion of those other factors that are also considered relevant in ascertaining the permitted purpose of use, the reader is referred to Chapter 7.

5.37 In the experience of the Commissioner, paragraph (B) of DPP1(3)(b)(i), which concerns the classes of persons to whom the data may be transferred, is also very often the bone of contention between the data user and the data subject. This is so especially because many ordinary transactions in modern society are in fact procedurally more complicated than they appear. Hence, a transaction involving the collection of personal data from an individual may entail the further transfer of such data to a third party beyond the expectation of the individual. In this connection, a well drafted "transferee clause" in a PICS will help to avoid any unpleasant surprise or dispute. A common example is found in the case of the transfer of personal data of the debtor by a credit provider to a debt collection agent for the purpose of debt recovery.

5.38 It is also important to note that the word "**use**", in relation to personal data, is defined in section 2(1) of the Ordinance as including to "**disclose**" or "**transfer**" the data. In other words, "*transfer*" is one type of "*use*". On this basis, the Commissioner takes the view that paragraph (B) in DPP1(3)(b)(i) should be read always subject to paragraph (A), in the sense that the transfer of data to a third party coming within paragraph (B) may happen only where the purpose for such transfer comes within paragraph (A), but not otherwise.

5.39 Regarding the matters to be notified to a data subject under DPP1(3)(b)(ii), it should be noted that they differ from those under DPP1(3)(b)(i) in that the notification is required to be given "*on or before **first use** of the data for the purpose for which they were collected*". It is therefore strictly permissible under DPP1(3)(b) for a data user first, on or before the collection of personal data, to give to the data subject notification under DPP1(3)(b)(i), and later, on or before first using such data, to give a separate notification under DPP1(3)(b)(ii). However, save in exceptional situations, there would seem to be little advantage in adopting a two-step process. Instead, it would be more sensible and practicable for a data user to give a comprehensive PICS in compliance with both sets of requirements at the same time.

5.40 Similar to DPP1(3)(b)(i), DPP1(3)(b)(ii) also consists of two paragraphs (A) and (B). The requirement under paragraph (B), however, may appear somewhat unusual in that it requires a data user to notify the data subject of "*the **name** and address of the individual to whom any (data access or correction) request may be made*".

5.41 The "*individual*" referred to in DPP1(3)(b)(ii)(B) will, in most cases, be a designated officer in an organization. Given that the relevant officer named in a PICS is subject to personnel changes, it is not entirely clear why the name, instead of his position or title, is required to be stated in the PICS. Whilst an organization may issue a further notice following change of personnel, such notification will have been given after "first use".

5.42 As a pragmatic approach, therefore, the Commissioner is inclined to accept as sufficient a PICS that, in giving notification under DPP1(3)(b)(ii)(B), refers to the person in question by position or title. The proposal to allow data user to give the post title of the person to whom a data access or correction request may be made has been included by the Administration in the Consultation Document on Review of the Personal Data (Privacy) Ordinance released in August 2009.

5.43 It should be noted that there is an express exemption under DPP1(3) in that compliance with that subsection is unnecessary where such compliance *"would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6"*. The practical effect of this is that, in many of the situations in which personal data are exempted from DPP6 under one of the relevant exemptions provided for in Part VIII of the Ordinance, there is also likely to be exemption from DPP1(3). In *AAB No. 23/2008*, the AAB considered that the purpose of recording the video image of an employee sleeping while on duty was for the determination of the suitability for continuance in employment under section 55 of the Ordinance, it would not be necessary for the employer to comply with DPP1(3) on or before making the recording. An even more obvious example is where the police collect evidence from a targeted person, the police would not be required to notify the person before collection of evidence.

Collection of biometric data

5.44 Given the sensitive nature of biometric data, collection of such data should be handled with extra care and caution. In seeking to collect biometric data from data subjects, one should consider providing an option to the data subjects who are unwilling to supply such data. Where the data subjects are willing to supply their biometric data, their genuine consent to do so should be obtained. This is particularly so where the data subjects are considered to be vulnerable, e.g. a

minor. It is relevant to note that the consent may be given out of pressure and the disparity of bargaining power, or that the data subjects may not even possess the full capacity to fully understand the privacy impact. In such cases, the collection may be viewed as collection without genuine consent and thus in breach of DPP1(2) for being unfair or unlawful.

5.45 In a complaint case in which an employer collected fingerprint data to record staff attendance, the Commissioner considered that the goal of collecting staff's attendance record effectively and accurately was not a sufficient ground for collection of fingerprint data. Since the employer had also installed surveillance cameras to monitor staff attendance and the system that collected fingerprint data also offered the option of using passwords for identification, the goal could also be achieved by those means without collecting the staff's fingerprint data. The Commissioner therefore decided that the collection of fingerprint data by the employer was unnecessary and excessive. The Commissioner also found on the facts that the employer might dismiss the staff who did not cooperate in using the fingerprint attendance system, and the employer had not provided that staff with sufficient information to enable the staff to make an informed decision on whether to supply the data to the employer. In the circumstances, the Commissioner found that the employer's means of collecting the fingerprint data was unfair under DPP1(2)(b)[35].

5.46 Despite the advantages of using biometric data, from the perspective of data privacy protection, it is advisable for data users to resort to less privacy intrusive but equally effective alternatives.

[35] Details of the Commissioner's findings in the investigation can be found in the Report Number R09-7884, which can be downloaded from http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf.

Chapter 6

Data Protection Principle 2

The main questions:

- What are the general requirements for accuracy of personal data under DPP2(1), and how do they apply?
- What are the general requirements for retention of personal data under DPP2(2) and section 26, and how do they apply?

The questions of accuracy and duration of retention of personal data discussed in this chapter concerning DPP2 and section 26 have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

DPP2(1)

6.1 **Data Protection Principle 2(1)** in Schedule 1 of the Ordinance provides as follows:

> ***"Principle 2 – accuracy and duration of retention of personal data***
>
> *(1) All practicable steps shall be taken to ensure that –*
>
> *(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;*
>
> *(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used –*
>
> *(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or*
>
> *(ii) the data are erased;*
>
> *(c) where it is practicable in all the circumstances of the case to know that –*
>
> *(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and*
>
> *(ii) that data were inaccurate at the time of such disclosure, that the third party –*
>
> *(A) is informed that the data are inaccurate; and*
>
> *(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose."*

6.2 The first point to note about the requirement under DPP2(1) is that the requirement is not absolute. In particular, as mentioned in the previous chapters, the word "*practicable*" as used throughout the Ordinance is defined in section 2(1) to mean "*reasonably practicable*". It follows that the duty of a data user under DPP2(1) is to take all **reasonably practicable steps** in ensuring (as opposed to, say, guaranteeing) the accuracy of all personal data held by it. Indeed, the fact that DPP2(1) does not impose an absolute standard is understandable, given the inevitability of human error. In an appeal lodged by a customer of a telecommunications company, the AAB ruled in *AAB No. 19/1999* that the obligation under DPP2(1) is not an absolute one. The AAB in this case was

satisfied that the company in maintaining accuracy of personal data of its customers had in place a sound system of recording and updating instructions given by customers. The AAB upheld the Commissioner's decision and the appeal was dismissed owing to lack of evidence to prove a breach of DPP2(1) by the company.

6.3 As for the meaning of the word "**accurate**", this can be inferred from the definition of "*inaccurate*" in section 2(1) which, in relation to personal data, means the data is "*incorrect, misleading, incomplete or obsolete*".

6.4 In this connection, however, it is also relevant to note that DPP2(1)(a) speaks of personal data being accurate *"having regard to the purpose for which (they) are to be used"*. The Commissioner is fully cognizant of the fact that the standard of accuracy varies according to the circumstances and there is no hard and fast rule to be universally applied. For instance, a greater degree of care would need to be taken to ensure the accuracy of such data the inaccuracy of which may involve serious consequences, as opposed to data concerning trivial matters.

6.5 The mere fact that the personal data kept by a data user are found to be inaccurate by the data subject does not necessarily result in a breach of DPP2(1)(a). In *AAB No. 12/2008*, the AAB considered that "*[The requirement of DPP2(1)(a)] does not mean that data held by the data user must be correct in all respects. The requirement is this : provided that the data user has taken all practicable steps to ensure the personal data kept by him are accurate, it is no breach of this requirement if the data are subsequently found to be incorrect by the data subject. If that happens, the data subject may pursuant to section 22 of the Ordinance ask the data user to correct the inaccuracies. Thus, there is no contravention of a requirement of the Ordinance where the personal data kept by the data user are inaccurate but it would be in contravention if the data user refused to correct the inaccuracies when the data subject lodged a data correction request with him*."

6.6 If the result of an investigation reveals that error committed is attributable to some identifiable defect in the data handling system or procedures of the data user, the Commissioner is likely to form the view that there is contravention of DPP2(1) and that it is likely that the contravention will continue or be repeated. By way of remedial action, the Commissioner will normally require the data user to take appropriate steps to improve its data handling system or procedures, with a view to preventing repetition of similar inaccuracy in the future.

6.7 In contrast, complaints may be lodged with the Commissioner by an individual against another which typically involve an ongoing dispute about the accuracy of the allegations, sometimes defamatory in nature, made by one party against the other. Since the allegations may in some cases technically constitute the personal data of the complainant, he will invariably contest their accuracy.

6.8 Not surprisingly, the complainant may seek to complain to the Commissioner about the "*inaccuracy*" of the data on the ground of contravention of DPP2(1) by the other party. The Commissioner would, in general, decline to investigate such a case, insofar as the true essence of it lies in the resolution of the parties' dispute, and not so much in the inaccuracy of personal data held. In such a situation, it is the court or tribunal of competent jurisdiction, rather than the Commissioner, that is the appropriate forum for adjudicating such a dispute. The same applies in a similar situation where the individual, having taken the further step of making a data correction request to the other party, complains to the Commissioner about the latter's refusal to "*correct*" the data in the way he wants. Comments contained in a dismissal letter are inherently contentious and the appellant in *AAB No. 22/2000* sought to correct the comments by making a data correction request. The AAB dismissed the appeal and ruled that the proper channel for redressing the dispute was to commence proceedings in the Labour Tribunal, not by way of a data correction request. (For further discussion on data correction request, the reader is referred to paragraphs 11.15 to 11.20 in Chapter 11).

DPP2(2) and section 26

6.9 **Data Protection Principle 2(2)** provides as follows:

> *"(2) Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used."*

6.10 Unlike DPP2(1), the application of DPP2(2) is not confined to the taking of what is a "*(reasonably) practicable*" step. Similarly, no such confinement is found in **section 26(1)** concerning erasure of personal data no longer required, which provides as follows:

> *"(1) A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless –*
>
> *(a) any such erasure is prohibited under any law; or*
>
> *(b) it is in the public interest (including historical interest) for the data not to be erased."*

6.11 In connection with the penalty that attaches for contravening section 26(1), it is relevant to take note of **section 64(10)** of the Ordinance which provides as follows:

> *"(10) A data user who, without reasonable excuse, contravenes any requirement under this Ordinance (other than a contravention of a data protection principle) for which no other penalty is specified in this section commits an offence and is liable on conviction to a fine at level 3."*

6.12 Since section 26(1) is not a DPP, it follows that a contravention of section 26(1) without reasonable excuse constitutes an offence under section 64(10). Thus, DPP2(2), backed up by section 26(1), seems to be imposing a more stringent obligation on the data user than the other DPPs (except for DPP6, which is backed up by parallel provisions in Part V of the Ordinance, as discussed in Chapters 10 and 11).

6.13 It is apparent that the central concept, by reference to which both DPP2(2) and section 26(1) operate, is the **purpose** for which the data in question were, or are to be, used. Indeed, the concept of purpose is important not only for the operation of DPP2(2) and section 26(1), but also for the operation of other requirements of the Ordinance. How the permitted purposes of use are to be ascertained will be discussed in detail in paragraphs 7.5 to 7.35 in Chapter 7.

6.14 In the absence of any statutory requirements or strong evidence supporting a genuine need for a data user to do so, the Commissioner is unlikely to accept retention of personal data indefinitely. In a case handled by the Commissioner in 2008, a former insurance agent abandoned copies of a huge amount of documents containing personal data of the agent's former clients collected more than four years before. The former insurance agent was prosecuted for contravention of section 26(1) of the Ordinance, and was fined accordingly. In a complaint case investigated by the Commissioner in 2007, an unsuccessful insurance applicant complained to the Commissioner against an insurance company for retaining the applicant's personal data. During investigation, it was revealed that the insurance company did not have a specific retention policy and would retain personal data of unsuccessful applicant indefinitely. The Commissioner found that the insurance company was in breach of DPP2(2). The Commissioner was of the view that the optimal period for retention of personal data for unsuccessful insurance applications with and without money transaction involved should be no more than seven and two years respectively.

6.15 The Commissioner is of the view that, for prudent business and good privacy practice, data users should devise a clear privacy policy and practice to ensure compliance with DPP2(2) to erase those personal data when the purpose of collection is fulfilled.

6.16 Sometimes, personal data may be kept longer than usual in compliance with specific requirements provided by statutes, code of practices or guidelines applicable to a particular trade or industry. For example, in cases where there are

suspected money laundering activities, the banks are required to comply with the Guidelines on Prevention of Money Laundering issued by the Monetary Authority to combat money laundering and retain records for that purpose[36]. Some statutes[37], codes of practices[38] or guidelines may provide for the prescribed period of retention of documents containing personal data in which case the data user may be obliged to comply.

6.17 Practical difficulty may arise in a situation where personal data are collected at different times for various purposes. The strict compliance with DPP2(1) and section 26(1) may entail the data user in tediously going through the items of personal data held and deleting those that have outlived their purposes on a regular basis. In this respect, a clearly promulgated retention policy may facilitate the data users, especially organizational ones, in implementing appropriate measures, such as the installation of automatic verification software to ensure those unnecessary data are properly erased. Without confining the obligation to the taking of "*all (reasonably) practicable steps*", the duty imposed on the data users under DPP2(2) and section 26(1) appears to be a harsh one to discharge. The Commissioner has thus proposed to the Administration to limit the extent of liability under section 26 and DPP2(2) so that a data user's duty is discharged insofar as it has taken all reasonably practicable steps to comply with the said requirements on retention and erasure of personal data. The proposal has been included by the Administration in the Consultation Document on Review of the Personal Data (Privacy) Ordinance released in August 2009.

6.18 Setting aside the practical difficulty mentioned above, in considering the application of DPP2(2) and section 26, it is also relevant to give due regard to the

---

[36] Sections 7.3 to 7.5 of *Prevention of Money Laundering: Guidelines issued by the Monetary Authority under section 7(3) of the Banking Ordinance*.

[37] For instance, in complying with section 51C of the Inland Revenue Ordinance, Cap 112 on keeping business records for not less than 7 years, personal data contained in such records shall be so retained. Under s.59(3) of the Police Force Ordinance, Cap. 232, the police who arrested a person and took identifying particulars of the arrested person, such as photographs and fingerprints, may retain the identifying particulars if the arrested person had been previously convicted of any offence or was the subject of a removal order under the Immigration Ordinance, Cap. 115. The retention period of the identifying particulars was specified in the Hong Kong Police Force Procedures Manual as 12 months. Another example is found in the three pieces of anti-discrimination legislation, namely, the Disability Discrimination Ordinance, Cap 487, the Family Status Discrimination Ordinance, Cap 527 and the Sex Discrimination Ordinance, Cap 480 which permit an individual to make a claim to the District Court against another person for an act of discrimination against him before the end of the period of 2 years beginning (a) when the act complained of was done; or (b) if there is a relevant report in relation to the act, the day on which the report is published or made available for inspection. The relevant documents containing personal data may therefore be kept for responding to a possible claim brought by the employee or ex-employee.

[38] Clause 1.3.3 of the *Code of Practice on Human Resource Management* issued by the Commissioner provides that personal data in respect of recruitment-related data held about job applicants be retained for not longer than 2 years and that personal data in respect of employment-related data about an employee be kept for not longer than 7 years. Clause 3.3 of the Code of Practice on Consumer Credit Data issued by the Commissioner provides that credit reference agency may retain account repayment data revealing material default (i.e. default in payment for a period in excess of 60 days) for 5 years either from the date of final settlement or from the date of the individual's discharge from bankruptcy, whichever is the earlier.

decision of the *Eastweek* case which is authority that where there has been no collection of personal data by a data user (as the term "*collect*" is defined in the case), the data protection principles will not be engaged. On that basis, it seems a person needs not worry about accidental contravention of DPP2(2) or section 26(1) in respect of any information that happens to be in his physical possession, unless he has "*collected*" such personal data in the sense that he compiled information about the relevant individual whom he has identified or intends or seeks to identify. To give a simple illustration, a newspaper may publish an article about a named individual which, in a technical sense, constitutes that individual's personal data. According to the *Eastweek* case, a person who merely holds a copy of the newspaper need not worry about compliance with DPP2(2) or section 26(1), but the situation may change if the newspaper clippings are retained and filed by that person as part of his compilation of information about that data subject mentioned in the clippings.[39]

6.19 Finally, according to section 26(1), it is to be noted that the erasure of personal data is not required under two alternative conditions, namely: (a) where the erasure of the data is prohibited under any law[40], or (b) where it is in the public interest (including historical interest) for the data not to be erased[41]. Hence, in a case where one of the two conditions mentioned in section 26(1) is satisfied, the data in question may be retained under DPP2(2) despite fulfilment of the purpose of use, because without infringing section 4, a data user may perform an act or engage in a practice contrary to a DPP if this is required or permitted under the Ordinance.

---

[39] For enquiries made to the Commissioner concerning whether the proposed retention of personal data in particular situations is likely to be consistent with DPP2(2) and section 26, the reader may refer to relevant cases in the Complaint and Enquiry Case Notes Section on the Commissioner's website, *http://www.pcpd.org.hk/english/casenotes/case.html*.

[40] For example, under section 56(3) of the Employment Ordinance, Cap 57, an employment agency shall retain records of all job applicants for a period of not less than 12 months after expiration of each accounting year of the employment agency concerned.

[41] For example, the Government Records Service of Hong Kong manages and records information for the HKSAR Government through its Public Records Office by developing a record-keeping programme that enables bureaux and departments to manage information resources appropriate to their purpose. The public can access Hong Kong's archives through documents, movies, photographs, posters or other records kept by it.

Chapter 7
Data Protection Principle 3

The main questions:

- What are the general requirements under DPP3?
- How is the original purpose of collection ascertained?
- What constitutes the use of personal data for a purpose directly related to the original purpose of collection?
- What constitutes "prescribed consent" of the data subject?

The questions of use of personal data discussed in this chapter concerning DPP3 have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

Importance of DPP3

7.1 **Data Protection Principle 3** provides as follows:

> ***"Principle 3 – use of personal data***
>
> *Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than –*
>
> *(a) the purpose for which the data were to be used at the time of the collection of the data, or*
>
> *(b) a purpose directly related to the purpose referred to in paragraph (a)."*

7.2 The word "**use**", in relation to personal data, is defined in section 2(1) as including the **disclosure** or **transfer** of data.

7.3 Among the six data protection principles, DPP3 is the one that governs the use of personal data, and as such, is probably of the greatest practical importance and concern to both data users and data subjects. Apart from using personal data for its own purposes, a data user may sometimes be asked to disclose the data to a third party, which disclosure also amounts to "*use*". Any improper use, disclosure or transfer of the personal data by the data user may contravene the requirements under DPP3. The ascertaining of the lawful and permitted purpose of use is therefore relevant not only for the application of DPP3, but also for the application of other purposes – related provisions of the Ordinance, such as, DPP1(3), DPP2(2), DPP5 and section 26.

7.4 In essence, the use of personal data, in order not to contravene under DPP3, must be for a purpose:

- that is the same as the purpose for which the data were to be used at the time of their original collection by the data user;
- directly related to the original purpose of collection; or
- to which the prescribed consent[42] of the data subject has been obtained.

The original purpose of collection

7.5 Paragraph (a) of DPP3 allows the use of personal data for the purpose for which the data were originally collected. In ascertaining the original purpose of collection, the following factors are relevant for consideration:

[42] For a discussion of the meaning of "*prescribed consent*", the reader is referred to paragraphs 7.36 to 7.44 below.

- the explicit purposes stated in the PICS given under DPP1(3);
- the function or activity of the data user;
- the restrictions of use imposed by the data subject or the transferor of the data;
- personal data collected in the public domain; and
- compliance with legal[43] or statutory requirements

7.6 It was mentioned in Chapter 5 that DPP1(3) requires a data user, on or before the collection of personal data from a data subject, to take all reasonably practicable steps to ensure that the data subject is informed, amongst others, of the purpose for which his data are to be used. The informed purpose obviously reflects the data user's then expectation regarding the use of the data collected. However, the question is to what extent does this also reflect the expectation of the data subject.

7.7 Apparently, insofar as the data subject allows the collection of data from him with the knowledge of the informed purpose on or before such collection, he is treated to have implicitly agreed to the use of his personal data for such informed purpose and therefore to be bound by it. The simplicity of this argument notwithstanding, the Commissioner will also take into account the following considerations in assessing the purposes of use.

7.8 First, in most, if not all, cases of data collection, the PICS tends to be an imposition by one party rather than a result of negotiation by both. This is especially so where the activity giving rise to the collection of data is one involving the provision of an essential service (e.g. educational, medical or other social service, public utility or banking service), or is otherwise important to the data subject (e.g. concerning his employment), or even compulsory in nature (e.g. the collection of data at an immigration check-point). In all these situations, it would be unrealistic to expect the data subject to refrain from such activity solely on account of his dissatisfaction with the PICS.

7.9 It is also common to find the purposes stated in the PICS couched in highly legalistic language, appearing in fine print among other lengthy and complicated standard terms and conditions of contract. Some data users may have a tendency to frame the intended purposes in terms as general and as wide as possible (which is arguably permitted under DPP1(3)(b)(i)(A) which allows the purposes to be stated "*in general or specific terms*") for the sake of flexibility. It would render the protection of personal data intended under DPP3 virtually meaningless if the data user were allowed to unilaterally dictate the purposes of collection as would

[43] In *AAB No. 40/2004*, the AAB recognized the prosecution's common law duty of disclosure on evidence collected though not used by it for prosecution. The common law principles of fair trial and open justice require disclosure of the "unused materials" categorized by the prosecution to the defendants of the action and was viewed by the AAB to be used for a purpose consistent with the original purpose of collection, not contravening DPP3.

exceed its lawful function and activities and the reasonable expectation of the data subject. To take a hypothetical example, where an individual applies for the opening of an account for a particular service, the account opening form may contain the following statement:

"Any information provided in this application may be transferred by the Company to any other companies inside or outside Hong Kong for such purpose as the Company may in its absolute discretion deem fit."

7.10 It would seem to fall within the literal meaning of the stated purpose if the Company decided, say, to sell its customer database to a third party for profit. However, having regard to the data subject's reasonable expectation that his data provided to the Company were to be used only for purposes directly related to his application for service (including, for example, application processing, service provision, billing and debt recovery, etc.) but not for any other unrelated purpose, the sale of the data by the Company to third parties would be likely to be construed as a change in purpose of use inconsistent with the original purpose of collection.

7.11 As prescribed in DPP1(1), personal data shall be collected for a lawful purpose directly related to the data user's function or activity. Thus, the lawful function and activity of the data user is a prime factor in deciding whether the use is proper in particular in situations where no PICS was given or where the wording of the PICS is ambiguous. For example, where personal data of job applicants are received in a recruitment exercise by Company A (not being an employment agency), the referral by it of such job applications to unrelated parties or other prospective employers without the job applicants' consent may exceed its normal functions and activities and thus constitute a change in purpose of use.

7.12 However, sometimes the function or activity of the data user may entail the disclosing of personal data to a party to the complaint. In one complaint case that came before the Commissioner, a flat owner A repeatedly complained to the management company about water dripping from the flat owned by B. As a result of the complaint, the management company collected the personal data of A and upon the request of B, the personal data collected were disclosed to B who subsequently commenced civil proceedings against A. On appeal in *AAB No. 66/2003*, the AAB upheld the Commissioner's finding that since A's personal data collected was for the purpose of handling and following up on the dispute in question, the disclosure of A's personal data by the management company to B was for a purpose consistent with the original purpose of collection and hence no prescribed consent from A was required prior to the disclosure.

7.13 It can be seen from the examples provided that the function and activity of a data user is of particular relevance in ascertaining the lawful purpose of use of personal data especially in relation to unsolicited data or data collected from third parties. On the other hand, there may be occasions where, upon provision by a person of

his personal data, he may have chosen to make an express stipulation regarding particular ways in which the data may or may not be used. Generally speaking, if the recipient has no intention to compile information about the individual in the *Eastweek* sense, such restrictions on use, if any, imposed might not have a part to play and the Ordinance has no application as the recipient did not "*collect*" the personal data in question. However, if the recipient subsequently compiled information about the individual whom it has identified or intends to or seeks to identify, the restrictions on use imposed may then become a relevant factor for consideration.

7.14 The way in which such express stipulation is viewed by the Commissioner is illustrated in this case: a bank customer, in providing his data to a bank officer in making an application for a particular service, requested his data to be handled only by that particular bank officer. Subsequently, in accordance with the bank's normal procedures, the bank officer transferred the data to other bank officers for further processing, in order to provide the customer with the service applied for. Such passing on of the data within the bank contrary to the data subject's request (which may, however, be considered to be unreasonable) was considered by the Commissioner not to amount to use of the data contrary to DPP3.

7.15 Another example is found in cases where complainants, upon lodging complaints to various authorities, requested non-disclosure of their identities to the parties complained against. In some of these cases, such anonymity may not affect the effective and fair handling of the complaint in question. When this is the case, the request may, in the Commissioner's view, have the effect of limiting the purposes of use for which the identity data in question were collected, so that their disclosure to the party complained against might amount to contravention of DPP3. The Commissioner's view on the matter could well be different, however, in other cases where a request for non-disclosure of the complainant's identity is not made, in which case, there will not be any contravention of DPP3 if disclosure of the complainant's identity is for the purpose of handling the complaint. Generally, when a data subject has imposed a condition to keep his personal data confidential, the more prudent practice is to obtain his prior consent before disclosing his personal data to a third party.

7.16 It is worth noting that the potential opportunity for a data subject to define, through the making of an express stipulation as mentioned above, the purposes of use in relation to personal data collected, exists only **on or before** the collection of the data. In other words, the Commissioner considers that it is not open for a data subject, whose personal data have already been collected or even used by a data user, to unilaterally introduce **thereafter** any restriction on or modification to the purposes of use.

7.17 For personal data that are intended by the data subject to be held confidentially, the mere fact that there might exist a duty of confidentiality does not thereby

necessarily render the disclosure by the data user a breach of DPP3. The tenet is to look at the purpose of disclosure. A complainant in his complaint to the Commissioner alleged that his employer wrongfully disclosed the fact that he was subject to disciplinary proceedings (which he claimed to be a confidential matter) to his visiting doctor in requesting a medical certificate as to his mental and physical fitness to attend the proceedings. The evidence supplied showed that the disciplinary proceedings had been postponed several times as a result of the excuse of sick leave by the complainant. The Commissioner found that personal data collected for the disciplinary proceedings was for the purpose of deciding the employment matter of the complainant and the disclosure of this fact to his visiting doctor to certify his fitness to attend the proceedings was, in the circumstances of the case, proper as being for the same or directly related purpose under DPP3 and this view was upheld by the AAB in *AAB No. 26/2004* on appeal by the complainant.

7.18 Sometimes when personal data are transferred by a data user ("the transferor") to another data user ("the recipient"), the transferor may specify the purpose for providing such data in order to prevent the risk of data abuse. Once so specified, this may be regarded as the purpose by reference to which any future use of the data by the recipient will be restricted under DPP3. However, there may be cases where the transferor did not stipulate any purpose of use. Must the recipient make enquiries into the purpose of use for which the data were originally acquired by the transferor (or even, where the data have gone through a chain of transfers, the purpose for which the data were originally collected by the first data user in the chain), so as to be bound by such purpose under DPP3? The Commissioner finds no support for the existence of such a duty in the language of DPP3, which duty (if existing at all) would be difficult to comply with or to enforce. The better view appears to be that where no restrictions of use were imposed, the recipient should only use the personal data for the purposes for which such data were collected by it or the directly related purposes. In case of doubt, the prudent practice is to seek the prescribed consent of the data subject before making further use of the personal data.

7.19 In the case of *AAB No. 41/2006*, the complainant lodged a complaint against the management company for disclosing her personal data, including her name, address and contact telephone number, to a law enforcement agency without her consent and contrary to prior agreement not to do so for investigation of a complaint of nuisance. Accepting the complainant's evidence that the management company had promised not to disclose her personal data to the law enforcement agency, the AAB ruled that when the management company provided the complainant's personal data to the law enforcement agency upon their request, the management company was using them for a purpose which was directly related to the purpose for which her data was collected in the first place (i.e. for investigation of the complaint of foul smell). Accordingly, the AAB found there was no contravention of DPP3.

7.20 Where personal data are collected in the public domain, for example, from the public register or where the personal data are being publicly made known, is the data user then free to use such data for whatever purpose as he wishes? It should be noted that the Ordinance does not differentiate or exempt from its application personal data collected in the public domain. Certain public records may expressly restrict the purposes for which the information, including the personal data, contained in the records may be used. Where the lawful perimeters for making further use of the data so obtained are defined or inferred, the subsequent data user is still liable and accountable for any abusive or improper use by it of the personal data. For instance, in a case that came before the Commissioner, a data user had subscribed from a public registry an online bulk service for public records containing personal data of third parties, and the subscription contract contained provisions stipulating that the information obtained should not be sold for the purpose of commercial gain. The data user subsequently developed and explored new search engines enabling name searches to be undertaken by subscribers to the services provided by the data user and the act was viewed as a change in purpose of use, contravening DPP3. Sometimes the purpose of use is spelt out in the enabling legislation[44] and sanctions may be imposed for improper use of the personal data[45]. The purpose statement may serve to define or limit the scope of lawful uses to be applied by the data user to the personal data obtained from the public registry.

7.21 Where there is a mandatory requirement under statute or common law for a data user to use personal data held by it in a particular way[46], the Commissioner would generally regard this to be a consistent purpose of use permitted under DPP3. This may, for example, be in the form of a statutory obligation to disclose information to a relevant authority, or in the form of a court order to disclose information to another party during litigation.

7.22 However, in the case of *AAB No. 16/2007*, the AAB did not agree with the Commissioner's view and considered that disclosure by a webmail service provider to public prosecution authorities in compliance with statutory requirement could not be considered as a use of the information intended by the parties when the

---

[44] For example, section 136(4) of the Securities and Futures Ordinance, Cap 571 stipulates that the purposes of the register of licensed persons and registered institutions available for public inspection are to enable members of the public to ascertain whether he is dealing with a licensed person or a registered institution in matters connected with any regulated activity, etc.

[45] See, for example, section 22(3) of the Electoral Affairs Commission (Registration of Electors)(Legislative Council Geographical Constituencies)(District Council Constituencies) Regulation, Cap. 541A for sanctions imposed for improper use of information obtained from the voters' register.

[46] For example, section 5 of the Registration of Persons Ordinance, Cap 177 confers on a public officer the power to require a registered person in all dealings with the government to furnish his identity card number and, so far as he is able, the identity card number of any other person whose particulars he is required by law to furnish. Section 56 of the Employment Ordinance, Cap 57 also requires a licensed employment agency to maintain a record of all job applicants containing name, address, identity card number or passport number available for inspection by the Commissioner of Labour.

information was collected. The AAB nevertheless concluded that the webmail service provider was not in breach of DPP3 because the Terms of Services agreed between the data subject and the service provider contained a provision whereby the service provider was authorized to make disclosure "in accordance with legal procedure". The AAB considered that the data subject had thereby given his prescribed consent to the relevant disclosure.

7.23 The rationale for treating compliance with the lawful requirements on use of personal data as being consistent with the original purpose of use is that it is commonly and generally understood by society that all law abiding citizens shall observe and comply with lawful requirements in discharging their civic duties.

7.24 That said, even where the use of personal data is permitted or required under statute or common law, unless the scope of personal data are clearly and sufficiently laid down, care should nonetheless be taken to ensure that irrelevant or excessive personal data not contemplated by statute or common law are not used. For example, where there is relevant statutory provision empowering the data user to publish a report consequent upon, say, the completion of an investigation conducted by it, it should take steps to ensure that only necessary and relevant personal data in compliance with the statutory provision are used and that where appropriate, certain editing, erasure or omission be carried out in respect of the unnecessary personal data. In case of doubt, the obtaining of the prior prescribed consent of the data subject is viewed as prudent practice.

Purposes directly related to the original purpose of collection

7.25 Paragraph (b) of DPP3 allows personal data to be used for a purpose directly related to the original purpose of collection. This makes sense as in many cases not all purposes of use of personal data can be definitively stated on or before the collection of the personal data by the data user. The concept of "**directly related purpose**" is of great practical significance, without which the use of personal data for various ordinary and innocuous purposes by the data user may be hampered.

7.26 In assessing whether the act in question is done for a "*directly related purpose*" and thus covered by DPP3(b), the Commissioner will take into account factors such as:

- the nature of the transaction giving rise to the need for using the personal data; and
- the reasonable expectation of the data subject.

7.27 The need of the transaction in question is regarded as relevant because one would expect that a data subject provides his personal data in order to enable or facilitate the transaction with the data user. It would therefore be within the reasonable

contemplation of the data subject that the use of his personal data shall consist of all such uses as would be necessary to effect the intended transaction.

7.28 In commercial transactions, such as the hire purchase or credit sale of goods, the provision of banking or financial services, the provision of utility or telecommunications services, etc., service providers have a legitimate interest to ensure the full and prompt settlement of all sums due and owed by the party to the transactions for services rendered. Hence, it is generally viewed that debt collection is a directly related purpose for the provision of the paid services and the creditor may transfer the personal data of the debtor to the debt collection agent or its solicitors to take recovery action[47]. In transferring personal data for the debt collection purpose, the creditor should nonetheless note that only necessary or sufficient personal data should be disclosed, lest it be challenged as a change in purpose of use.

7.29 In a complaint case handled by the Commissioner, the complainant complained against a credit provider for having transferred his personal data to a debt collector, who subsequently disclosed the personal data in a public place in the course of collecting a debt owed by the son of the complainant. The Commissioner found that the personal data of the complainant were provided to the credit provider in a loan application form as a family member of the son when the son applied for a loan from the credit provider. The credit provider explained to the Commissioner that the application form was prepared by its agent and it did not require the personal data of the family members of a loan applicant at all. When it passed the loan application form to the debt collector for recovery of the son's debt, the complainant's personal data were not intended to be used by the debt collector. The Commissioner was of the opinion that the credit provider should have withheld the personal data of the complainant from the debt collector since they were not intended to be used by the debt collector for the purpose of recovering the son's debt. As the credit provider had disclosed the complainant's personal data to the debt collector, the credit provider had contravened DPP3.

7.30 In the field of human resources management, the personal data of the employees are collected for human resources purposes, such as promotion or renewal of contracts or discontinuation of employment, etc. which are generally viewed as for a directly related purpose. Other examples of the use of employees' personal data by employers for directly related purposes are: the disclosure to Mandatory Provident Fund providers for the administering of the MPF scheme; the use of data for integrity checking owing to the inherent nature of the job; the inclusion in a medical insurance plan taken out by an employer; conducting of disciplinary proceedings or compiling performance appraisal reports about an employee in

[47] In *AAB No. 19/1999*, the AAB decided that there was no change of purpose of use in the passing of the appellant's personal data by the telecommunications company to a debt collecting agent to pursue a debt owed by the appellant, being its customer.

question. In a complaint case that came before the Commissioner, the complainant alleged that her employer was wrong in disclosing her medical records to the medical board convened for the purpose of determining her fitness for employment. The Commissioner found that the disclosure of her medical records was necessary for the purpose of the hearing and for a purpose directly related to her employment, permitted under DPP3. Not satisfied with the finding of no contravention, the complainant appealed to the AAB which appeal was subsequently dismissed[48].

7.31 There are cases in which the use of the personal data of the job applicants or employees may be viewed as being used for a non-related purpose. For instance, in a case that came before the Commissioner, a job applicant complained that the prospective employer used his personal data for making a direct marketing approach to him after the job interview which act was found by the Commissioner in the circumstances of the case to have exceeded the original purpose of collecting the job applicant's personal data, namely, for human resources purposes only. In another case, the employer engaged in a credit card promotion campaign with a credit card company by offering special terms and conditions for its employees. The employer should not, in such a case, use the employees' personal data and pass them to the credit card company for marketing of the card without first obtaining the prescribed consent of the employees as such act might amount to a change in purpose of use, contravening DPP3.

7.32 Notwithstanding that the use of the personal data can be shown to be for a purpose directly related to its original purpose of collection, care should be taken to ensure that the amount and kind of personal data disclosed are necessary for attaining that related purpose of use. For instance, where a PICS provides for the transfer of customers' personal data to the data user's associated company for direct marketing purposes, it is generally taken by the Commissioner that the transfer of contact data, such as name, telephone number or address would be sufficient for such purpose and any further disclosure of personal data might, depending on the circumstances of the case, be viewed as excessive and thus amount to a change in purpose of use. Similarly, in some of the cases involving the posting of debtors' identity cards in public by debt collection agents for debt recovery action, the Commissioner found that the transfer of the copy of the identity card of the debtor by the creditor to the debt collection agents was not necessary for the purpose of debt recovery and as such a contravention of the requirements of DPP3. Location or contact data would generally suffice for such purpose.

[48] *AAB No. 17/2002*. In the course of hearing evidence it emerged that the complainant did in fact give her written consent to the disclosure of her medical records to the Medical Board. In another AAB case, *AAB No. 11/2004*, the educational institution's disclosure of the evaluation questionnaire completed by students by submitting them to an academic committee for a staff assessment review was held to be for a directly related purpose in the circumstances of the case.

7.33 Any excessive disclosure of personal data not necessary for the purpose of use will run the risk of being accused by the data subject as a change in purpose of use. In particular where such personal data will be made public, the damage that is likely to occur to a data subject on wrongful disclosure may be significant having regard to the nature and type of personal data involved. Sometimes the extent of disclosure may exceed the reasonable expectation of the data subject, and thus might become the subject of potential dispute.

7.34 This is illustrated in a complaint case handled by the Commissioner. A government department collected a witness statement for the purpose of prosecuting an offender and the standard form witness statement contained personal particulars of the witness, such as his name, address, HKID number, date of birth, place of employment, etc. The department furnished the whole unedited version of the witness statement to the defendant. While it was accepted that the disclosure of the contents of the statement made by the witness to the defendant was necessary for the defendant to answer the charge, the disclosure of such personal particulars of the witness, such as HKID number, address, date of birth and place of employment, was not justified in the circumstances of the case to be necessary. Based upon the findings of the Commissioner, the government department agreed to revise its working manual such that unnecessary personal particulars of the witness were edited out before supplying it to other parties to the proceedings.

7.35 In the case of *AAB No. 46/2006*, an employee secretly recorded his conversation with his supervisor during a lunch meeting and then uploaded the recorded conversation onto the websites and internet discussion forum inviting downloading. The Commissioner found the mode, magnitude and extent of disclosure of personal data via the borderless world of the Internet privacy intrusive, exceeding the original purpose of collection (i.e. for handling personal affairs) and hence in contravention of DPP3.

Prescribed consent

7.36 When the use of personal data collected does not fall within the original purpose of collection or its directly related purpose or where the data user is uncertain as to the proper use of the personal data, the prescribed consent obtained from the data subject is of particular relevance in ensuring compliance with DPP3 unless otherwise exempted under Part VIII of the Ordinance[49]. The term "**prescribed consent**" is defined under **section 2(3)** of the Ordinance:

[49] For discussion of the Part VIII exemptions, reader may refer to Chapter 12.

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

7.37 There are two important points to note regarding paragraph (a) of the above definition. First, prescribed consent has to be **express**. In other words, no such consent is to be implied from conduct or omission by the data subject. Subject to this, however, there is no requirement for such consent to be in writing, which means that it may be given orally. For evidentiary reasons, it would certainly be advantageous if prescribed consent in writing were obtained.

7.38 Consent should not be deemed given merely by the fact that the data subject does not respond or object to the giving of such consent. In one complaint case, an estate agent notified its client that he would automatically become a member of a club operated by the estate agent's related company (which offered multifarious services other than estate agency services) if he failed to object. The client did not respond and as a result the estate agent transferred his personal data to the club. Since such transfer was not for a directly related purpose, the prescribed consent of the data subject was needed. The Commissioner found that the non response could in no way be construed as consent expressly given within the meaning of "*prescribed consent*".

7.39 The other important point to note from paragraph (a) is that prescribed consent must be "*given voluntarily*". What this means exactly, however, may be open to some doubt, as discussed below.

7.40 As the true meaning of the word suggests, "*consent*" obtained by misrepresentation or duress is no consent at all and thus cannot possibly amount to "*prescribed consent*". This arguably is already the case even without the reference to voluntariness in paragraph (a). By including the element of voluntariness, therefore, it seems possible that the legislature's intention was to impose a higher standard than merely the absence of misrepresentation or duress.

7.41 With this in mind, in ascertaining whether the consent is voluntarily given under paragraph (a) of section 2(3), the Commissioner would give due regard to such factors as whether the data subject is in fact free to choose between giving and withholding consent, **without fear of any adverse consequence** either way. In this connection, "*adverse consequence*" may include, for example, the denial to the data subject of any benefit or any service (especially essential service) by the data user, if the data subject were to withhold his consent.

7.42 Hence, in negating the giving of consent with the free will of the data subject, a data subject may adduce contrary evidence to prove that any consent purportedly given was not voluntarily made. The Commissioner will look at all the relevant evidence and circumstances of the case before deciding whether prescribed consent was indeed given by the data subject.

7.43 According to section 2(3)(b), prescribed consent does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent had been given. However, for avoidance of doubt, acts done pursuant to the consent before the notice withdrawing such consent is served are not affected. Hence, it is noted that although prescribed consent is not statutorily required to be given in writing, written as opposed to verbal notice in withdrawing the consent is required under this provision in the interest of clarity which may also serve as evidence to avoid any misunderstanding on the part of data users.

7.44 It is controversial whether minors and persons under disability are able to give valid consent. Sometimes the data subject does not have a sufficient understanding of what is proposed to him for consent owing to age or mental incapacity. In cases involving minors and persons under disability, consideration should be given as to whether the person has a "sufficient understanding and intelligence" to enable him/her to fully understand what is proposed to him/her. This is a test derived from a UK court decision in *Gillick v West Norfolk and Wisbech Area Health Authority and Another* [1986] AC 112.

When Part VIII exemption applies

7.45 There are situations where use of personal data for other purposes unrelated to the original purpose of collection is necessary and the prescribed consent of the data subject is neither forthcoming nor could it be practicably obtained, such as, for instance, the reporting of evidence of crime to the law enforcement agencies. Part VIII of the Ordinance contains relevant provisions exempting personal data from the application of DPP3 where use of the personal data is for certain exempted purpose(s) and the data user has reasonable grounds to believe that failure to so use the personal data would prejudice the exempted purpose(s). The ones that are commonly raised are found in section 58(1) (a) and (d) where personal data are used for the prevention or detection of crime or the prevention, preclusion or remedying of unlawful or seriously improper conduct, etc.

7.46 The Part VIII exemption provisions, however, do not have the force of compelling or requiring the data user to disclose or use the personal data for exempted purposes. Rather, it is only to be invoked by the data user to justify his use of personal data as "**permitted**" under section 4 of the Ordinance. For more details on how Part VIII exemptions can be properly invoked to exempt personal data from the application of DPP3, the reader is referred to Chapter 12.

Chapter 8
Data Protection Principle 4

The main questions:

- What are the general requirements on security of personal data under DPP4, and how do they apply?
- What are the specific steps the Commissioner has advised or directed data users to take in particular situations?

The questions of security of personal data discussed in this chapter concerning DPP4 have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

The general requirements of DPP4

8.1 **Data Protection Principle 4** provides as follows:

> ***"Principle 4 – security of personal data***
>
> *All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to –*
>
> *(a) the kind of data and the harm that could result if any of those things should occur;*
>
> *(b) the physical location where the data are stored;*
>
> *(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;*
>
> *(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data, and*
>
> *(e) any measures taken for ensuring the secure transmission of the data."*

8.2 As mentioned previously, the word "*practicable*" is defined in section 2(1) as meaning "*reasonably practicable*". It follows that DPP4 does not require a data user to provide an absolute guarantee for the security of personal data held by it, but rather, only to take such steps as may be reasonably practicable in the circumstances, having regard to the matters mentioned in paragraphs (a) to (e).

8.3 Of the said paragraphs (a) to (e), the "harm test" covered by paragraph (a) is an important consideration. In determining the appropriate security measures to be undertaken by the data user with respect to the data held, they should be proportionate to the degree of sensitivity of the data and harm that will result from accidental or unauthorized access to such data. Take for example the personal data held by a bank about its customers: DPP4 would require a higher degree of care in handling personal data such as the bank statements of its customers as opposed to direct marketing or promotional materials sent to customers.

8.4 In a complaint about the loss of credit card application forms and HKID copies collected by bank staff in an outdoor marketing campaign who accidentally left these sensitive data on a public light bus while carrying them home, the Commissioner found the bank did not have in place adequate security measures to guard against the loss of these sensitive personal data. As a result of the investigation, the bank revised the working procedures and personal data

collected in the course of outdoor marketing campaigns shall be transmitted to the nearby branch and the staff are not allowed to carry these sensitive personal data home.

8.5 With the common and widespread use of online services to gain access to essential services, such as telecommunications, e-banking and e-shopping, service providers should take extra care to attend to the technological pitfalls so that their customers' personal data are stored and transmitted in a safe manner so as to prevent unauthorized or accidental access of these data by, for example, computer hackers or unintended users.

8.6 In some cases handled by the Commissioner, it was found that when applying for network services, service providers collected customers' personal data such as name, identification document number, address and contact telephone number for the purpose of processing the application. In the welcome letter advising the online registration, the activation of the account usually entails the typing in of the login ID and the password of the user. The service providers would in some cases provide the customers with a default password by using the customer's HKID number. In a complaint case handled by the Commissioner, the complainant's creditor successfully gained access to the electronic telephone bills of the complainant by typing in his HKID number as the password for online access which as a result enabled the creditor to collect the telephone records of the complainant and to use them for making nuisance calls to his friends. The telecommunications company in question was found to have contravened DPP4 in failing to take all reasonably practicable steps to safeguard the customers' personal data. In the enforcement notice served by the Commissioner, the company was required to cease the practice of using HKID numbers as default passwords. Given the easy guess for the passwords and the likelihood of manipulation, service providers were advised to take steps to protect the security of the customers' personal data by provision, for example, of randomly selected passwords.

8.7 Also, it is important to note that DPP4 concerns only the way in which personal data are kept or transmitted, but not the way they are used (which is governed under DPP3). This distinction is illustrated clearly in the AAB's decision in the case of *AAB No. 5/1999*.

8.8 In that case, the Commissioner received a complaint from an individual against a newspaper for publishing his name and name of the street to which he moved in a news report. The report related to an assault case in which the complainant's father was injured by a former neighbour. The publishing of the address data of the complainant was considered likely to cause risk of serious harm to him and his family, since the assailant, who remained at large, was known to be a dangerous individual suspected to be of unsound mind, and had previously already committed a series of assaults on the complainant and his family. In fact, it was because of

those previous attacks that the complainant and his family had moved to their current address which was exposed in the news report.

8.9 Despite the harm likely to be caused to the data subject by disclosure of his personal data in the news report, the AAB reversed the Commissioner's original finding of contravention of DPP4 against the newspaper publisher. In particular, the AAB observed that a newspaper uses personal data in publishing them. Once published, the public will inevitably gain access to such data. Accordingly, any access by the assailant to the address data of the complainant in the case would not have been "*unauthorized or accidental*" within the meaning of DPP4[50]. According to the AAB, therefore, the relevance of DPP4 is confined only to security in the storage and transmission of the data. Since this decision, the Commissioner has become mindful of the distinction, sometimes a fine one, between the **use**, especially the disclosure to public or third parties of the personal data of the data subject which might involve a change in purpose of use (of which DPP3 is the subject of concern) and the security requirements on **transit and storage** of personal data to prevent unauthorized or accidental access to the personal data (which is a DPP4 issue).

8.10 In the case of outsourcing work to contractor, data users should take extra care where the contractor would be entrusted to handle the personal data in the course of performing services. For instance, if a contractor is retained to develop, enhance or maintain computer system for processing database which contains personal data, and it is necessary to entrust the personal data to the contractor for handling, the data user should ensure that the personal data are accessible by the contractor only. In order to minimize the risk of unauthorized or accidental disclosure of personal data, e.g. leakage of data from computer database through the Internet, data users should avoid using real personal data, even for the purpose of test running the computer system.

8.11 If personal data are accessible by the contractor, it is essential for the data user to take measures to prohibit the contractor from conveying the data to third parties, especially when the data user has no control over these third parties on how the personal data are handled. In this regard, the Commissioner is of the view that the data user in the circumstance should ensure the inclusion of a prohibition clause in the service contract with the contractor. Data users should also consider the possibility of arranging all handling of the personal data to be performed within the premises of the data users, in order to minimize the risk of data loss[51].

---

[50] Whether the publication of the address data by the newspaper publisher could have been regarded as giving rise to any requirement in the Ordinance other than DPP4 (e.g. DPP3) was not raised, hence not decided upon by the AAB.

[51] The Commissioner has made detailed findings and recommendations in an investigation. The relevant investigation report no. R06-2599, can be downloaded from http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf.

8.12 Internet and telecommunication services providers are usually in possession of voluminous personal data of their customers. Thus, it should be a prime concern of them to ensure data security in order to avoid any leakage of data. Customers sometimes may have forgotten the passwords to their e-mail account(s) or telephone call records. In such circumstances, services providers must be cautious in verifying the identity of the customer before rendering any assistance that could facilitate the access to any information of that customer's account. The Commissioner received a complaint in which the Internet service provider reset a customer's password upon the request of a person who knew the name and HKID number of that customer, even though the caller was not the customer and the customer was not aware of the request. Such practice of the service provider was held as not meeting the standard of DPP4 in ensuring data security.

8.13 Universal Serial Bus (USB) flash drives have been widely used for their advantages of portability and high storage capacity. However, their mobility and compact sizes have also increased the risk of data loss as the USB flash drives containing the data may be misplaced or lost without the notice of the users. In 2008, repeated incidents of loss of patients' personal data contained in USB flash drives caused the public concern on the use of USB flash drives. As a result, the Commissioner carried out an inspection for the first time of the personal data system of the Hospital Authority[52]. If portable storage devices like the USB flash drives are to be used, all reasonably practicable steps shall be taken to prevent such devices from being obtained and accessed by unauthorised persons and clear policy and guidance should be devised governing the use of such portable storage devices.

Specific situations

8.14 Given the flexibility of the meaning of the phrase *"all reasonably practicable steps"*, it should not be surprising that the steps thus required of a data user may vary widely from situation to situation. Nevertheless, from the experience acquired by the Commissioner in handling cases on the application of DPP4, the following precautionary steps (without in anyway limiting or affecting the Commissioner's exercise of his powers according to the particular circumstances of each case) are generally accepted to be examples of the appropriate measures to be taken by data user in the situations cited below (some suggestions originated from: http://www.getsafeonline.org/):

[52] The relevant inspection report no. R08-4232 can be downloaded from http://www.pcpd.org.hk/english/publications/files/HA_inspection_report_e.pdf. See also the investigation report no. R08-1935 in relation to a complaint against a hospital for loss of a USB flash drive containing the complainant's personal data. The report can be downloaded from http://www.pcpd.org.hk/english/publications/files/UCH_investigation_report_e.pdf.

Situation	Appropriate steps
Storage of data in paper files	– files under lock and key or in a secure area – access by authorized personnel on a need-to-know basis – shred the paper files – have a 'clear-desk' policy requiring employees to lock up sensitive papers when they are not working on them
Transmission of data by mail	– the use of sealed envelopes – making sure no sensitive data (e.g. HKID number) are visible through envelope window – mail marked "private and confidential" if intended for the eyes of the addressee only – making sure dedicated fax machine, if available, is used at the receiving end – advance notification to the recipient of incoming fax – checking the accuracy of the fax number before dialing
Electronic storage and transmission	– the use of encryption – "confidential mail boxes" – automatic routing to a dedicated computer directory – passwords for access – restriction against indiscriminate uploading or downloading of data via web enabling public access through search engines
Portable electronic storage device	– the use of password protected device, e.g. password protected USB flash drives – The use of encryption
Account data accessible by account holder via the Internet	– service providers avoid setting "obvious" default passwords, such as data subject's HKID number – reminder to data subject to change password regularly
Service of legal processes	– documents contained in sealed envelopes except where personal service is to be effected directly on the individual
Server security	– Keep servers and network switch boards in a locked room and control access to it – Unplug unused network extensions – Consider hiring a knowledgeable IT manager or outsourcing the work to a trusted supplier – Restrict the number of administrator passwords – As with desktop personal computers, servers need a firewall, regular updates and anti-virus software – Do not use a server as an employee's workstation – Read server reports, such as security logs, and monitor for changes and irregularities

Situation	Appropriate steps
	– A rapid response maintenance contract for any servers. – Treat server backups as if they were complete copies of all the information on the server (which they are) and make sure that they are also kept under lock and key and only available to authorized personnel
Accessing database	– Regularly review who has access to information and change access privileges as necessary – Limit the number and scope of administrative users – For consistency, allocate access on the basis of an individual's role, not on a person-by-person basis. For example, employees in the accounts department may need access to the book keeping system and the human resources managers and finance managers may need access to personnel records. – Each employee should have his own user ID. They should be treated like office keys and not shared or compromised in any way. – Make sure that all computers attached to the network require a secure log in and that they are all set to log out automatically if left unattended for more than a few minutes. – Delete users' access privileges once they stop working for the company. – A secure network, including an effective firewall to keep out unwanted connections. – Delete remote access privileges once they are not needed. For example, do not let any departed employees retain access to your network. – Review firewall and other server logs to monitor remote access. Watch for unusual activity. – Keeping firewall and VPN software up-to-date to protect against evolving threats. – Many remote desktop programs rely on installing a client program on an office computer. This creates a tunnel through the firewall. Do not allow employees to do this on their own initiative. Control which programs are used and how they are installed.

Chapter 9

Data Protection Principle 5

The main questions:

- What are the general requirements under DPP5?
- How can privacy policy and practices be made generally available?

The questions of making information generally available by a data user discussed in this chapter concerning DPP5 have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

The general requirement of DPP5

9.1 **Data Protection Principle 5** provides as follows:

> ***"Principle 5 – information to be generally available***
>
> *All practicable steps shall be taken to ensure that a person can –*
>
> *(a) ascertain a data user's policies and practices in relation to personal data;*
>
> *(b) be informed of the kind of personal data held by a data user;*
>
> *(c) be informed of the main purposes for which personal data held by a data user are or are to be used."*

9.2 Although the obligation imposed under DPP5 is not an absolute one insofar as it only requires a data user to take all reasonably practicable steps to comply with it, the Commissioner regards it as important for a data user who engages in regular acts or practices that involve the collection of substantial amount of personal data in the course of its business or performance of its activities or functions, to make known and be transparent about its personal data policies and practices. Good governance dictates that organizational data users, such as government departments or corporations take heed of increasing public concern to ensure that data subjects' personal data privacy is properly protected by following a set of privacy policies or practices that is made generally available. In *AAB No. 15/2000*, the Commissioner's decision to issue an enforcement notice on implementing a privacy policy statement in compliance with DPP5 against a regulatory body whose daily operation involves the collection of sensitive personal data from general public was upheld by the AAB.

9.3 DPP5 does not require the data user's policies or practices to be produced in writing. However, in order to effectively communicate its data management policies and practices and for avoidance of doubt, it is proper and prudent to have a written privacy policy statement, which is commonly known as a **Privacy Policy Statement**, or in short, "**PPS**", implemented incorporating such essential matters as the kind of personal data held and the main purposes for which personal data held by a data user are or are to be used. An effective PPS may also include other useful information which might affect the data subjects' personal data privacy, such as the retention period for the data collected, the security measures in place and the proper mechanism for erasure or destruction of records, etc. When the actual practice on data management changes in response to business needs, the data user should review or revise its PPS so that current acts or practices of personal data collection accord with its published PPS.

9.4 The PPS once in place has to be effectively communicated to the persons affected and some of the common ways of dissemination are by putting up conspicuous

notices displaying the PPS publicly, playing a pre-recorded PPS if personal data are collected through telephone conversation[53], or incorporating it in relevant documents when personal data are collected or uploading the PPS onto the data user's website, etc. A data user may explore other effective and appropriate means of keeping data subjects informed of its personal data policies and practices taking into account its nature of business.

9.5 The complainant in *AAB No. 35/2003* alleged that a library failed to comply with DPP5 in making known its privacy policies and practices in respect of personal data collected by the library's prescribed forms. The appeal was dismissed and the AAB in upholding the Commissioner's decision not to investigate the complaint decided that the publication via the library's website of its privacy policy statement was sufficient compliance with DPP5.

9.6 The principle of transparency has assumed increasing importance not only in relation to dealing with personal data in the business-to-customer market segment, but also in respect of employees' personal data privacy rights. This is particularly so when an employer intends to carry out monitoring activities in the workplace where personal data of employers are collected via telephone, email, internet or video monitoring. Owing to its privacy intrusive nature, the employer should as far as practicable, formulate and disseminate its monitoring policy in order to keep employees informed of the extent, scope and manner in which such activities are carried out and how their personal data would be subsequently used and transferred and the possible adverse or disciplinary action that may ensue. Employers shall also ensure that new employees are aware of the existing PPS. In an AAB's decision[54], the AAB opined that an employer who failed to draw the attention of an employee employed in 2004 to an existing PPS issued in 2000 could be in breach of DPP5.

9.7 In facilitating compliance with the requirements of the Ordinance by employer as data user and in exercise of the Commissioner's powers under section 8(5) of the Ordinance, the Commissioner issued in December 2004 the *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* indicating the manner in which the Commissioner proposes to perform his functions and powers in relation to employee monitoring[55]. Where employee monitoring is justified for legitimate business purposes, an employer should take practicable steps to formulate and

---

[53] See the inquiry case note no. 2007106, which can be downloaded from http://www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=275&casetype=O&cid=17.

[54] *AAB No. 14/06.*

[55] In the Guidelines, the 3A's concept (i.e. Assessment, Alternatives and Accountability) in assessing the appropriateness of employee monitoring and the 3C's approach (i.e. Clarity, Communication and Control) were introduced in relation to the handling of personal data collected during monitoring. The DPP5 requirements were expounded in the Clarity and Communication concepts in devising and making known a Monitoring Policy. Employers are encouraged to follow the recommended good practices mentioned in the Guidelines.

make known its monitoring policy and due regard should be given to the legitimate expectation of the employees of personal data privacy. It has been generally accepted that by entering into employment relationships, the employees though submitting themselves to the lawful instructions to be given by the employer, do not thereby forsake all their rights to personal data privacy, their legitimate expectation of privacy would extend to cover such matters as abhorrence of the installation of CCTV in toilets or changing rooms, the indiscriminate collection of the contents of their personal emails or the taping of private calls without proper justification. The transparency of actions expressed through a clearly written and communicated PPS is conducive to building mutual trust between employers and employees.

9.8 In a complaint case that came before the Commissioner, a public organization was found to have installed covert pinhole cameras for detecting the theft of its property believed to be committed by its staff. Upon investigation, it was found that the use of pinhole cameras was extensive and out of proportion in relation to the objective of gathering evidence of crime and the means adopted was unfair. Also, the organization did not have in place a monitoring policy which, in view of the activities carried out by the organization and the number of employees affected, was found not to have taken reasonably practicable steps to comply with DPP5[56].

[56] A report on this complaint case was published pursuant to section 48 of the Ordinance and readers may refer to the report at the Commissioner's website, *http://www.pcpd.org.hk/english/infocentre/files/R05-7230_e.pdf.*

Chapter 10

Data Protection Principle 6(a) to (d) and the Data Access Provisions in Part V

The main questions:

- What constitutes a data access request?
- Who may make a data access request?
- How can a data access request be made?
- How can a data user comply with a data access request?
- What charge may a data user levy for complying with a data access request?
- When shall a data user refuse to comply with a data access request?
- When may a data user refuse to comply with a data access request?
- What steps must a data user take in refusing to comply with a data access request?

The questions discussed in this chapter concerning data access requests and DPP6 and Part V of the Ordinance have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

The basis of a data access request

10.1 The right of a data subject to access his personal data held by the data user is provided for under paragraphs (a) to (d) of **Data Protection Principle 6**:

> ***"Principle 6 – access to personal data***
>
> *A data subject shall be entitled to –*
>
> *(a) ascertain whether a data user holds personal data of which he is the data subject;*
>
> *(b) request access to personal data –*
>
> *(i) within a reasonable time;*
>
> *(ii) at a fee, if any, that is not excessive;*
>
> *(iii) in a reasonable manner; and*
>
> *(iv) in a form that is intelligible;*
>
> *(c) be given reasons if a request referred to in paragraph (b) is refused;*
>
> *(d) object to a refusal referred to in paragraph (c); . . ."*

10.2 In addition, Part V of the Ordinance contains detailed provisions and procedural requirements regarding how a data subject may make, and how a data user complies with, a data access request. Apart from reliance on some valid grounds provided under Part V that the data user shall or may refuse to comply with a data access request, there are exemption provisions in Part VIII of the Ordinance which, when properly invoked, may exempt the data user from compliance with a data access request.

10.3 Generally speaking, there are stringent provisions relating to compliance with a data access request that a data user shall carefully observe. Thus, when a data access request is received, the data user shall properly handle it by examining the relevant provisions under Parts V and VIII of the Ordinance in complying with or refusing to comply with, the data access request.

10.4 To facilitate understanding, the salient points to the making of a data access request by a data subject or his relevant person, and to the handling and responding to such request by the data user are set out below.

What constitutes a data access request?

10.5 The first question relevant to considering the data access provisions of the Ordinance is what constitutes a data access request? In this connection, the term "**data access request**" is defined in section 2(1) as *"a request under section 18"*.

10.6 **Section 18(1)** provides as follows:

> *"(1) An individual, or a relevant person on behalf of an individual, may make a request –*
>
> *(a) to be informed by a data user whether the data user holds personal data of which the individual is the data subject;*
>
> *(b) if the data user holds such data, to be supplied by the data user with a copy of such data."*

10.7 The first thing to note from the definition in section 18(1) is that neither the word "*and*" nor the word "*or*" appears between paragraphs (a) and (b). Taking the grammatical meaning that it bears, and in applying the rule of literal interpretation, paragraphs (a) and (b) could be construed to be two distinct categories of request. The Commissioner adopts the view that the two paragraphs are not conjunctive in character and should be construed to cover two separate categories of request that a requestor, in making a data access request, is entitled to express his choice. In other words, a data access request may consist of only a request under paragraph (a), or only a request under paragraph (b), or both.

10.8 However, when a data access request purportedly made under section 18(1)(a) is received, section 18(3) provides that the data user may, in the absence of evidence to the contrary, treat the data access request as one made under both section 18(1)(a) and (b) and in addition to simply responding to the request made under section 18(1)(a), supply also the copy of the personal data to the requestor pursuant to section 18(1)(b) of the Ordinance. The reverse situation (i.e. a request purportedly made under section 18(1)(b)) however is not provided for in the Ordinance, it is therefore doubtful whether the same rationale applies. The Commissioner takes the view that each case should be determined according to its own set of facts and relevant evidence in ascertaining the scope of the data access request made by a requestor.

10.9 It should also be noted that in reading paragraph (a) alone, it is not clear whether the term *"personal data"* appearing therein refers to personal data in general or any specific item of personal data. The Commissioner takes the view that the meaning of that term includes both. In other words, in a data access request under paragraph (a), the requestor may choose to ask a data user, "*Do you hold any of my personal data?*" or, alternatively, "*Do you hold Item X?*" (X being a description of one or more items believed to constitute or contain the requestor's personal data).

10.10 Insofar as paragraph (b) is concerned, the reference to *"a copy of such data"* must necessarily mean the data referred to in paragraph (a). It should be noted, however, that no reference is made in paragraph (a) or (b) of a description or list of data (if any) being held. Accordingly, where a data access request is

phrased in terms such as: "*give me a list of all my data held by you*", the Commissioner is inclined to the view that this does not strictly constitute a data access request within the meaning of section 18(1) obligating compliance by the data user under the Ordinance. It has been confirmed in the case of *AAB No. 24/2001* (discussed in paragraphs 10.29 to 10.32 below) that a data subject has no right to demand an exhaustive list of all his data held by a data user. A data user, however, may sometimes choose to provide such a list to facilitate its handling of a data access request, especially a request under section 18(1)(b).

10.11 Similarly, the Commissioner has received complaints about alleged failure to comply with requests worded like: "*give me in writing the reason for (my dismissal, your rejecting my application, etc.)*." In this connection, it is important to remember that the term "*data*" is defined in section 2(1) as meaning the representation of information in a document. Hence, unless the reason or explanation being sought **already exists** in such a document (which in most cases means in writing), the Commissioner takes the view that the data user has **no** obligation, upon receiving the request, then to reduce to writing the reason or explanation being sought, i.e. to **create** data for the sake of complying with the data access request.

Who may make a data access request?

10.12 Having considered what constitutes a data access request, the next question to consider is who may make such a request. In this connection, section 18(1) provides for the making of a data access request by "*an individual, or a relevant person on behalf of an individual*". The term "***relevant person***" is defined in **section 2(1)** as follows:

> *"'relevant person', in relation to an individual (howsoever the individual is described), means –*
>
> *(a) where the individual is a minor, a person who has parental responsibility for the minor;*
>
> *(b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;*
>
> *(c) in any other case, a person authorized in writing by the individual to make a data access request, a data correction request, or both such requests, on behalf of the individual."*

10.13 The provisions of the Ordinance give no indication, however, of the kind of situation in which a data access request made by a relevant person is to be regarded as being so made "*on behalf of*" the individual. Doubt may arise as to

whether a data access request is properly made by one of the parents as a relevant person on behalf of a minor in the two situations illustrated: first, where the parent is physically separated from the minor, so that one may suspect the data access request is in fact made by the parent for his/her own purposes such as to enable himself or herself to locate the minor or the other parent of the minor rather than on behalf of the minor; secondly, where the minor could well be disinclined, if asked, to have his data released to the parent (e.g. youths receiving help from social workers).

10.14 The Commissioner has encountered cases where a parent who was denied physical access to his or her child by the custodian parent, lodged a data access request under the Ordinance in the name of the child's relevant person, with parties such as the school that the child attended or the social welfare organization that provides welfare services to the child seeking access to the location data (e.g. the address) of the child. It is obvious from the subject matter raised in the request that the child has actual knowledge of the location data requested and is therefore apparent that the requestor parent has his or her own rather than his or her child's interest to serve in tracing the whereabouts of the child. In situations like this, the Commissioner will incline to the view that the request is not one made "*on behalf of*" the child and does not therefore satisfy the requirements under section 18(1) of the Ordinance.

How to make a data access request?

10.15 Having considered who may make a data access request, the next question is how such a request can be made.

10.16 The Ordinance does not prescribe any particular form or mode in which a data access request must be made, except that under section 20(3)(a), if a data access request is not made "*in writing in the Chinese or English language*", this will constitute valid grounds on which the request may be refused. Even so, the data user is still bound to comply with the requirements applicable to such a refusal, as will be discussed in paragraphs 10.54 to 10.63 below.

10.17 In early cases handled by the Commissioner, the absence of any prescribed form for a data access request would often cause confusion. In particular, a data user receiving such a request could easily be unaware of it being a data access request, hence its obligation to respond to it in strict compliance with the Ordinance. This had significant impact on data users such as any public or private organization that its regular dealings with individuals and it is not unusual for it to have to handle data access requests from time to time. Even if a request is not meant to be made pursuant to the Ordinance (for example, a request made to a government department pursuant to the Code of Access to Information), the requested information may happen to contain the requestor's personal data.

10.18 The Commissioner took the view that for a data access request intended to be made under the Ordinance (whether under section 18(1)(a), 18(1)(b) or both), the requestor should at least refer to terms such as "*personal data*", "*Personal Data (Privacy) Ordinance*", "*Cap. 486*", "*data access request*", etc. In order to prevent or reduce the risk of misunderstanding, the Commissioner has, since December 1999, pursuant to his power to specify forms under section 67(1) of the Ordinance, specified a Data Access Request Form[57] in which data access requests are to be made. The consequence for making a data access request **not** in the specified form is provided for in **section 20(3)(e)** as follows:

> *"(3) A data user may refuse to comply with a data access request if –*
>
> *. . .*
>
> *(e) the form in which the request shall be made has been specified under section 67 and the request is not made in that form; . . ."*

10.19 The Data Access Request Form has been designed to make clear, both to the party using it to make a data access request and to the party receiving it, the following essential matters:

- the fact that a data access request is being made under the Ordinance;
- the particular provision(s) under which such request is being made (i.e. paragraph (a) or (b) of section 18(1), or both);
- the precise scope of the data to which the request relates (in this regard, the data subject is guided through to frame his request as specific as possible);
- the way of handling (including the time for compliance with) such a request, and possible consequences of failure to do so.

10.20 It is to be noted that failure to use the Data Access Request Form does not of itself render the data access request invalid nor does it exonerate the data user from responding to it in a manner prescribed by the Ordinance though it may afford the data user a ground under section 20(3)(e) to refuse compliance with it as mentioned in paragraph 10.18 above.

10.21 The benefit derived from the introduction of the prescribed Data Access Request Form is seen in the significant reduction of the number of complaint cases received by the Commissioner concerning disputes as to whether a data access request is made under the Ordinance.

[57] Form OPS003.

How to comply with a data access request?

10.22 A data user, upon receiving a data access request, may decide to comply with such a request. A relevant point to note, then, is how this may be done.

10.23 First, it should be noted that a data access request under section 18(1)(a) is a request to *"be informed by a data user"* whether any personal data of the data subject are being held. To comply with the request, there is no express requirement under the Ordinance for the requested information to be provided in writing. Nevertheless, this would be highly desirable for the sake of avoiding disputes.

10.24 On the other hand, a data access request under section 18(1)(b) is a request to be supplied with a copy of the data held, if any. In this connection, it may be noted that **section 19(3)(a)** provides, *inter alia*, as follows:

> *"(3) A copy of the personal data to be supplied by a data user in compliance with a data access request shall –*
>
> *(a) be supplied by reference to the data at the time when the request is received except that the copy may take account of –*
>
> *(i) any processing of the data –*
>
> *(A) made between that time and the time when the copy is supplied; and*
>
> *(B) that would have been made irrespective of the receipt of the request; . . ."*

10.25 Thus, it can be seen that the relevant point in time by reference to which personal data are said to be held by the data user is the time when the request is received by the data user and not any subsequent time when further personal data might be collected. That said, the data user may, but is not obliged to, take into account any processing of the data that would in any event take place prior to compliance with the data access request. The latter duty is however not a strict one imposed upon the data user.

10.26 The operation of section 19(3)(a) may lead to the interesting question being asked as to the application of the other provisions relating to compliance or non-compliance with the data access request. For instance, if a data user invokes the application of any of the Part VIII exemptions in refusing to comply with the data access request, does it also mean that the exempting circumstances can only be ascertained at the time when the request was received and no account shall be taken of any exempting circumstances that exist after receipt but before compliance with the data access request? The better view adopted by the Commissioner is that section 19(3)(a) concerns only the technical aspect of drawing the time line for the obligation of the data user to supply copies of the

personal data. The right to refuse compliance, as provided under section 20 of the Ordinance, does not contain provisions that restrict or confine its application insofar as they are properly invoked with reasons stated and the requestor is notified in accordance with section 21.

10.27 Sometimes, a data access request may be framed in such a way that it contains a **subjective** element (e.g. "*all data that affect my reputation*"). In complaints arising from this, the Commissioner has generally taken the view that a data subject who chooses to make his request in an unspecific manner will have to rely on the judgment of the data user in selecting the relevant data that need to be provided (if any).

10.28 Even more commonly, a data subject may, in the data access request, ask for copies of "*all personal data*" relating to him or her held by the data user. This, however, may create serious practical difficulty for the data user, especially where there has been extensive dealings between the parties, during which a large amount of personal data may have been created, e.g. where the data subject is or used to be employed by the data user for many years.

10.29 Such, indeed, was the situation in the case of *AAB No. 24/2001*. In that case, the appellant institution was found by the Commissioner to have failed to comply fully with data access requests by a former staff member by omitting to provide her with some of her personal data. In her data access requests, she asked for "*all of my personal data*" held by the appellant, including but not limited to certain named categories. Despite repeated requests for clarification from the appellant, the requestor refused to narrow the scope of her data access requests in any way. In his enforcement notice issued against the appellant under section 50 of the Ordinance, therefore, as one of the remedial measures to be taken, the Commissioner directed the appellant to conduct a "*thorough search*" for the data as requested.

10.30 Upon appeal by the appellant against the enforcement notice issued against it by the Commissioner, AAB upheld the appeal and observed that such a direction was contrary to **section 20(3)(b)** of the Ordinance, which provides that:

> *"(3)* A *data user may refuse to comply with a data access request if –*
>
> . . .
>
> *(b) the data user is not supplied with such information as the data user may reasonably require to locate the personal data to which the request relates; . . .".*

10.31 According to the AAB's decision, therefore, it appears that the said provision of section 20(3)(b), in addition to constituting grounds upon which a data user may make a formal refusal under section 21 to a data access request, may also,

even where no such formal refusal is made, operate to limit the scope of data which the data user is obliged to provide in compliance with the request. In particular, it seems that where the data access request is of a general nature, and in the absence of any information from the requestor to specify or to otherwise assist in the location of the data requested, the data user's duty of compliance may only extend to such data as it may reasonably and practicably be expected to provide (even if this may not necessarily be exhaustive of all data held by the data user that fall under the description of the data requested)[58].

10.32 Indeed, in so ruling, the AAB seems to have made compliance with a data access request somewhat less onerous than it otherwise might have been in some situations. To a certain extent, the view expressed in the following extracted passage from the AAB's decision may be seen to be relevant to the AAB's adoption of a pragmatic approach:

"The Board wish to make it known that we deprecate any attempt by persons to use the Board as a forum for the pursuit of personal vendetta or to vent their anger. The Ordinance must be interpreted and applied sensibly, reasonably and practicably so that it is not used as a tool of oppression or revenge."

10.33 In the case of *CACV351/2006* (in relation to *AAB No. 61/2005*), the Court of Appeal held that a person making the data access request has a duty to make clear what personal data are requested under the data access request and also to supply further information to clarify if so requested by the data user. Furthermore, the AAB has also decided in *AAB No. 16/2008* that where the data user reasonably requires the data requestor to supply information to enable him to locate the relevant personal data, unless and until such information has been supplied, there is no valid data access request for the data user to comply with. Whether the request for information by the data user is reasonably made is a question of fact depending upon the circumstances and the facts of each case.

10.34 It is also important to note that the data requester is entitled to a copy of his personal data only, not every document which refers to him. This view is confirmed by the AAB in *AAB No. 27/2006* and the Court of First Instance in *Wu Kit Ping v Administrative Appeals Board [2007] 5 HKC 450*. The Court considered that "*If in a document, the maker of the document expresses an opinion about a data subject, that opinion will constitute personal data to which the data subject will be entitled to access. However, an opinion expressed in the same document, by the maker of the document, about the maker of the document himself, unless relating*

[58] Indeed, in a situation where the data access request is framed so widely that the type and scope of the data requested is obviously unclear so that further clarification is required before it can be complied with, the AAB in *AAB No. 17/2004* took the view that the data access request may be regarded as unclear and should not have been accepted for processing and the time to comply with the data access request does not start to operate until a properly completed data access request is received.

indirectly to the data subject, will not constitute the personal data of the data subject".

10.35 Regarding compliance with a data access request, one last important point to note is the time requirement for compliance with a data access request provided for in **sections 19(1)** and **(2)** of the Ordinance, as follows:

> *"(1) Subject to subsection (2) and sections 20 and 28(5), a data user shall comply with a data access request not later than 40 days after receiving the request.*
>
> *(2) A data user who is unable to comply with a data access request within the period specified in subsection (1) shall –*
>
> *(a) before the expiration of that period –*
>
> *(i) by notice in writing inform the requestor that the data user is so unable and of the reasons why the data user is so unable; and*
>
> *(ii) comply with the request to the extent, if any, that the data user is able to comply with the request; and*
>
> *(b) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with the request."*

10.36 As seen from section 19(1) above, the normal time period for complying with a data access request is 40 days after the receipt of such request. This, however, is subject to sections 19(2), 20 and 28(5). In this connection, the application of sections 20 and 28(5), which relate respectively to a data user's refusal to comply with, and imposition of a fee for compliance with, a data access request, will be dealt with in paragraphs 10.38 to 10.53 below.

10.37 As for section 19(2), that provision does not lay down the precise situations in which a data user may legitimately claim to be "*unable*" to comply with a data access request within the prescribed period. In previous complaint cases, the Commissioner has accepted as valid a data user's claim that before complying, it needed to obtain legal advice, or clarification from the requestor on the scope of the request. It is however important to still observe the time limit imposed under section 19(2) to respond and give reasons for being unable to comply with the whole or part of the request within 40 days. *AAB No. 17/2004* concerned a data access request made by a patient for medical records kept by a hospital. The hospital charged for the expenses for making copies of the requested data which was paid by the requestor near to the expiration of the 40 days. The hospital supplied the copies some 60 days after receipt of the request and was ruled by the AAB to have breached section 19(2) in failing to respond within 40 days after receipt of the data access request.

Charge for complying with a data access request

10.38 For compliance with a data access request, a data user may levy a charge on the requestor in accordance with the following provisions in **section 28** of the Ordinance:

> *"(1) A data user shall not impose a fee for complying or refusing to comply with a data access request or data correction request unless the imposition of the fee is expressly permitted by this section.*
>
> *(2) Subject to subsections (3) and (4), a data user may impose a fee for complying with a data access request.*
>
> *(3) No fee imposed for complying with a data access request shall be excessive.*
>
> *. . .*
>
> *(5) A data user may refuse to comply with a data access request unless and until any fee imposed by the data user for complying with the request has been paid. . . ."*

10.39 While section 28(3) prohibits the imposition of an "*excessive*" fee for complying with a data access request, that word is not defined. In determining whether the fee imposed by the data user is excessive, the Commissioner regards it as important that the fee, if any, charged should not be set with a view to generate profit, or worse, to deter the data subject from exercising his data access right under the Ordinance. In cases handled by the Commissioner, the charging for the actual out-of-pocket expenses, such as the photocopying fee and postage incurred by the data user are not regarded as excessive. A data user may be asked to justify the basis of calculation of the fee in determining whether the fee charged is excessive in the circumstances of the case. In a complaint case, a parent complained against the school for imposing an excessive fee for complying with his data access request made on behalf of his son. In determining whether the fee was excessive, a data user may be allowed to recover only the labour costs and actual out-of-pocket expenses involved in the process of complying with a data access request insofar as they relate to the location, retrieval or reproduction of the data requested. The labour costs should only refer to the normal salary of a clerical or administrative staff who is to handle the location, retrieval or reproduction work. No charge for the sum incurred for legal advice or the time spent in redacting data or deciding which personal data should be disclosed or refused to be disclosed. The fee imposed by the school in this case based upon an average hourly salary comprising those of the headmaster, principal, and other senior staff was excessive and contrary to section 28(3) of the Ordinance.

10.40 Section 28(5) entitles a data user to refuse to comply with a data access request unless and until the fee imposed has been paid. However, there is no provision in the Ordinance to entitle a data user to charge for the work done (e.g. in retrieving and quantifying the data) for compliance with the data access request if the requestor finally refuses to pay for the fee imposed.

When shall a data user refuse to comply with a data access request?

10.41 The obligation under section 19(1) for a data user to comply with a data access request is subject to sections 19(2), 20 and 28(5). The provisions of sections 19(2) and 28(5) have already been discussed. Section 20(1) and (3) provide respectively for a variety of situations in which the data user shall, or may, refuse to comply with a data access request. The following discussion deals with the situations under section 20(1).

10.42 **Section 20(1)** provides as follows:

> *"(1) A data user shall refuse to comply with a data access request –*
>
> *(a) if the data user is not supplied with such information as the data user may reasonably require –*
>
> *(i) in order to satisfy the data user as to the identity of the requestor;*
>
> *(ii) where the requestor purports to be a relevant person, in order to satisfy the data user –*
>
> *(A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and*
>
> *(B) that the requestor is such a person in relation to that individual;*
>
> *(b) subject to subsection (2), if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the data user is satisfied that the other individual has consented to the disclosure of the data to the requestor; or*
>
> *(c) in any other case, if compliance with the request is for the time being prohibited under this Ordinance."*

10.43 Of the situations mentioned in section 20(1), the difficult one is that provided for under paragraph (b), i.e. where personal data requested by a data subject or his relevant person contain also the personal data of another individual. This is therefore discussed first.

10.44 It should be noted that when applying the definition of "*personal data*" under section 2(1), it is possible for an item of information to constitute simultaneously the personal data of two or more individuals. Take, for example, a statement contained in a letter which says, *"John Doe is a distant cousin of Mary Doe."* Obviously, the statement constitutes the personal data of John Doe and, at the same time, that of Mary Doe, and it is impossible to separate one from the other. In other words, compliance with a data access request from one of the individuals may involve the disclosure of the personal data of the other.

10.45 In this situation, section 20(1)(b) requires that the data access request be refused unless the other data subject has consented to the disclosure of the data to the requestor. Such requirement, however, is subject to section 20(2).

10.46 Regarding consent from the other data subject, it is important to note that section 20(1)(b) does not contain any express provision as to who (as between the data user and the data subject) may have the responsibility for asking the third party for consent. However, in most situations, insofar as it is likely to be the data user who has contact information about the third party, and insofar as it is the data user who is seeking to rely on section 20(1)(b) to justify its refusal to comply with the data access request, the better view, therefore, seems to be that the responsibility should lie with the data user.

10.47 To make the situation regarding the handling of third party data even more complicated, section 20(1)(b) is expressly provided to be read subject to **section 20(2)**, which provides as follows:

> *"(2) Subsection (1)(b) shall not operate –*
>
> *(a) so that the reference in that subsection to personal data of which any other individual is the data subject includes a reference to information identifying that individual as the source of the personal data to which the data access request concerned relates unless that information names or otherwise explicitly identifies that individual;*
>
> *(b) so as to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise."*

10.48 Section 20(1)(b) and section 20(2) together make difficult reading. In a nutshell, their overall effect, gathered from experience in handling cases that came before the Commissioner, has been taken to be as follows:

10.48.1 Where the information requested under a data access request contains personal data about another individual (whether as the provider of the information or otherwise) whose consent for the release of such data

to the requestor has not been obtained[59], the data user, in complying with the request, shall erase from the data released the name or other explicit identification of the other individual;

10.48.2 It is **not** the data user's concern, however, whether such erasure may be effective in preventing the requestor from knowing the identity of the individual whose name or other explicit identification has been so erased. To impose otherwise an additional duty on the data user to ascertain the subjective knowledge of the requestor in relation to the identity of such third party, notwithstanding the erasure of the name or other explicit identification prior to compliance with the data access request, would be too onerous a burden to discharge and not in accordance with the letter and spirit of section 20(2). For example, where in the data access request the requestor asks for written comments on himself made by a specified third party, the fact that the requestor already knows the identity of the third party does not, in the Commissioner's view, give the data user any justification for refusing to comply with the data access request, for the sake of protecting the privacy of the third party involved. All the data user needs to ensure is that the data as released do not contain the name or other identifying information of the third party. This view has been confirmed in *Wu Kit Ping v Administrative Appeals Board [2007] 5 HKC 450*, in which the learned judge considered that "*. . . by s.20(2)(a), the restriction on the disclosure of personal data of one data subject, which might disclose the personal data of other data subject, operates only where the maker of the report, that is the source of the personal data to which the data access request is concerned, is named or explicitly identified. If the person who examined diagnosed and treated Ms Wu is not named in the report, it is likely that by deduction or inference Ms Wu will know the name of that person, if it had been given to her, for example, at the time of treatment. The fact that that deduction or inference may be made is not a barrier to the disclosure of Ms Wu's personal data . . . But unless the data names or otherwise explicitly identifies the complainant, the fact that the complainant's identity might be determined by deduction or inference is not a barrier to the disclosure of the data . . . The effect of s.20(2)(b) is that if the data user can supply to the data subject his personal data, without the disclosure of the identity of the source of the information, then a means to supply the data must be found.*"

10.49 Of the other situations covered by section 20(1), it is worth mentioning that under paragraph (c), a data user shall refuse to comply with a data access request where such compliance is "*for the time being prohibited*" under the Ordinance.

[59] For discussion of the question of whose responsibility it is to seek such consent, see paragraph 10.46 above.

There are few situations in which compliance with a data access request is expressly prohibited under the Ordinance, one of them is found in a situation in which a data access request is made to the Commissioner himself for personal data collected by the Commissioner in the course of his investigation under Part VII of the Ordinance. With regard to such data, section 46(1) imposes on the Commissioner and officers of the Commissioner a duty to maintain secrecy, subject to certain exceptions provided for in section 46(2) and (3), and unless any of these exceptions applies, the Commissioner is obliged to refuse the data access request according to section 20(1)(c).

When may a data user refuse to comply with a data access request?

10.50 Having considered the provisions in the Ordinance which oblige a data user to refuse to comply with a data access request, we turn to other situations where such refusal may be exercised by the data user. These are provided for in **section 20(3)** as follows:

> *"(3) A data user may refuse to comply with a data access request if –*
>
> *(a) the request is not in writing in the Chinese or English language;*
>
> *(b) the data user is not supplied with such information as the data user may reasonably require to locate the personal data to which the request relates;*
>
> *(c) the request follows 2 or more similar requests made by –*
>
> *(i) the individual who is the data subject in respect of the personal data to which the request relates;*
>
> *(ii) one or more relevant persons on behalf of that individual; or*
>
> *(iii) any combination of that individual and those relevant persons, and it is unreasonable in all the circumstances for the data user to comply with the request;*
>
> *(d) subject to subsection (4), any other data user controls the use of the data in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with the request;*
>
> *(e) the form in which the request shall be made has been specified under section 67 and the request is not made in that form; or*
>
> *(f) in any other case, compliance with the request may for the time being be refused under this Ordinance, whether by virtue of an exemption under Part VIII or otherwise."*

10.51 Of the various grounds of refusal provided for above, the one under paragraph (f) is the broadest. In particular, Part VIII of the Ordinance provides for many situations in which personal data are exempted from access by the data subject[60]. When a data user is uncertain whether any of the exemption provisions applies to a particular case, the more prudent practice is to seek independent legal advice before relying upon the exemption to comply with a data access request. This is important particularly because the Commissioner takes the view that refusal of a data access request on invalid grounds (which the data user innocently believed to be valid) technically constitutes contravention of section 19(1) by the data user.

10.52 Of the remaining provisions in section 20(3), paragraph (d) also deserves mentioning. In fact, this paragraph needs to be read in conjunction with sections 21(1) and 18(4), which provide as follows:

Section 21(1) –

> *"(1) Subject to subsection (2), a data user who pursuant to section 20 refuses to comply with a data access request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor –*
>
> *(a) of the refusal;*
>
> *. . .*
>
> *(c) where section 20(3)(d) is applicable, of the name and address of the other data user concerned."*

Section 18(4) –

> *"(4) A data user who, in relation to personal data –*
>
> *(a) does not hold the data; but*
>
> *(b) controls the use of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with a data access request which relates to the data,*
>
> *shall be deemed to hold those data, and the provisions of this Ordinance (including this section) shall be construed accordingly."*

10.53 In other words, where a data access request has been refused based on section 20(3)(d), there is an alternative channel for the requestor to make a request to

[60] For discussion of some of these exemptions, see Chapter 12.

the party that ultimately controls the use of the data (even if it does not physically hold such data). An example is where the data user owes a legal duty of confidentiality to a third party in respect of the personal data held by it and thus is refrained from complying with the data access request. In such a situation, the data access request may be made to the third party as notified to the requestor.

Steps to take in refusing to comply with a data access request

10.54 Where a data user is entitled, on one of the grounds provided for in section 20, to refuse to comply with a data access request, this does not mean that the data user can thereby ignore the request altogether. Rather, there are two steps which the data user is required to take in relation to such refusal to comply, namely, putting a relevant entry in its log book as required under section 27(2), and notifying the requestor in accordance with section 21(1).

10.55 Regarding the requirement to notify the requestor, **section 21(1)** provides as follows:

> *"(1) Subject to subsection (2), a data user who pursuant to section 20 refuses to comply with a data access request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor –*
>
> *(a) of the refusal;*
>
> *(b) subject to subsection (2), of the reasons for the refusal; and*
>
> *(c) where section 20(3)(d) is applicable, of the name and address of the other data user concerned."*

10.56 It is important to note that even though a data user may be legally entitled to refuse to comply with a data access request, it is still obliged to give to the requestor written notification of the prescribed matters **within 40 days of receiving the request**. Failure to comply with this requirement will result in contravention of section 21(1).

10.57 Pursuant to section 21(1)(a) and (b), a data user who refuses to comply shall by notice in writing inform the requestor of the **refusal** and the **reason** for such refusal. Presumably, the intention behind such a requirement on the part of the data user is to give a dissatisfied requestor a fair chance to challenge the refusal without undue delay.

10.58 In this connection, it is important also to note that where, in response to a data access request, a data user releases to the requestor only **part** of the data held, then regarding the **remainder** of the data being withheld, the data user is in effect **refusing** to comply with the data access request. The notification requirements

under section 21(1) also apply to that part of the data that are withheld. In other words, in compliance with paragraph (a), the data user is obliged to notify the requestor, with reasons, for withholding of certain requested data, otherwise the requestor might be given the impression that the copy data provided to him constitutes all that are being held, which might not be true.

10.59 In relation to notification under paragraph (b), one question is how specific the reasons should be. In this regard, the notification given should at least be specific enough to enable the requestor, if he so wishes, to challenge the refusal. In previous cases handled, the Commissioner has considered the notification given by a data user to be sufficient where it mentioned the grounds relied on (e.g. "*legal professional privilege*") or, alternatively, the exact section number of the relevant exemption provision (in the example just quoted, "*section 60*").

10.60 However, where the data user has failed to notify the requestor of the grounds relied upon under section 20(1) and (3) to refuse compliance with the data access request, even where valid grounds do exist to justify refusal, the data user is still regarded as having breached section 19(1) in complying with a data access request. Care should thus be taken to ensure that where proper grounds of refusal are relied upon in refusing compliance with a data access request, they should be clearly notified in accordance with section 21 of the Ordinance.

10.61 Prior to giving notification to the requestor, a data user refusing a data access request is required to keep a log entry of any refusal. In particular, **section 27(1), (2)(a)** and **(3)(a)** provide as follows:

> *"(1) A data user shall keep and maintain a log book –*
>
> *(a) for the purposes of this Part;*
>
> *(b) in the Chinese or English language; . . .*
>
> *(2) A data user shall in accordance with subsection (3) enter in the log book –*
>
> *(a) where pursuant to section 20 the data user refuses to comply with a data access request, particulars of the reasons for the refusal; . . ."*
>
> *(3) The particulars required by subsection (2) to be entered by a data user in the log book shall be so entered –*
>
> *(a) in the case of particulars referred to in paragraph (a) of that subsection, on or before the notice under section 21(1) is served in respect of the refusal to which those particulars relate; . . ."*

10.62 In this connection, it should be noted that "*log book*" is not defined in the Ordinance. One may therefore question whether, besides a bound book which

is a generally accepted form of a "*log book*", records kept in different forms, e.g. by electronic means would also suffice as constituting a "*log book*" for the purposes of section 27(1)? There is nothing in the Ordinance to prevent the giving of a liberal meaning to "log book" to include one existing in electronic format so long as the procedures prescribed under section 27(1) are followed and the Commissioner is not hindered from exercising his powers under section 27(4) to inspect and copy the log book at any reasonable time.

10.63 The question also arises as to whether section 27 actually requires every data user always to have ready a blank log book for the purpose of that section, even **before** it refuses any data access request, i.e. before there is anything to record. The Commissioner takes the view that this would not be necessary so long as the refusal to comply with a data access request is properly recorded in accordance with section 27.

Proper exercise of the right to access personal data

10.64 It should be emphasized that the data access right conferred upon a data subject under section 18 of the Ordinance is not to be abused nor should it be exercised to substitute or replace other proper channels for discovery of documents readily available to the data subject. The Commissioner is vigilant in examining all relevant circumstances of the case in ensuring that such right is not being abused so as to become an instrument of harassment against the party to the request which goes against the legislative intent of the Ordinance.

10.65 Use of data access request shall not supplement the rights of discovery in legal proceedings. In the case of *Wu Kit Ping v Administrative Appeals Board [2007] 5 HKC 450* (in relation to *AAB No. 27/2006*), it was held that the right of an individual to obtain data is limited to that individual's personal data and the entitlement of a data subject is to know what "personal data" the data user holds. The learned judge took the view that the data subject's entitlement is to a copy of the data, not to "*see every document which refers to a data subject*". Furthermore, "*It is not the purpose of the Ordinance to supplement rights of discovery in legal proceedings, nor to add any wider action for discovery for the purpose of discovering the identity of a wrongdoer*" under the third party Norwich Pharmacal discovery principle. The purpose of the Ordinance "*is not to enable a data subject to locate information for other purposes, such as litigation*".

10.66 To illustrate this point, in a complaint lodged by a dismissed employee against his former employer, he claimed that the employer failed to comply with a series of his data access requests for various internal minutes, letters and records on incidents which concerned him by omitting or deleting data which he believed to belong to him. After examining the reply and documents supplied, the Commissioner took the view that the former employer had complied with his requests. It was also noted that the complainant had separately commenced legal

action against his ex-employer for unlawful dismissal. The way and manner that the complainant conducted his complaint led the Commissioner to conclude that the complaint was frivolous or vexatious or was not made in good faith under section 39(2)(c) of the Ordinance. Dissatisfied with the Commissioner's finding, the complainant applied to the Court of First Instance for a judicial review.

10.67 The Judge[61] dismissed the application and ruled that since it transpired that the complainant had already obtained or would be able to obtain the documents he requested for in the process of legal discovery in the separate lawsuits, the attempt to obtain his personal data by lodging data access requests against his ex-employer under section 18 of the Ordinance had become meaningless. In *AAB No. 46/2004*, the AAB accepted the fact that the complainant had obtained a copy of the document she requested in her data access request through other legal proceedings is a relevant factor for the Commissioner to consider in exercising his discretion to refuse to carry out any or further investigation under section 39(2)(d).

10.68 It is also to be noted that when a data access request is made against judicial officers in exercise of their judicial function, for example, request for notes written by judges at the hearing, the Commissioner took the view that section 18 of the Ordinance has no application to such a situation. The rationale being that the independence of judiciary is inviolable and protected under the Basic Law of the HKSAR, pursuant to which, members of the judiciary shall be immune from legal action in the performance of their judicial functions[62]. All laws previously in force including the Ordinance shall not contravene the Basic Law[63] and therefore the data access right shall not apply to inhibit or infringe upon the independence of the judiciary in performance of judicial acts.

10.69 This view has been endorsed by the AAB in *AAB No. 39/2004* concerning the disclosure of a sickness certificate belonging to the complainant by a Tribunal to the other party to the proceedings. Although the case concerns the proper use of the personal data and not a data access request, the AAB ruled that the Ordinance does not apply to judicial acts and any error of laws or impropriety of procedures should be dealt with by appeal procedures and are not subject to the regulatory remit of the Ordinance. This provides certainty to the scope of application of the data access right.

---

[61] Cheung J. in judgment given in *Tsui Koon Wai v Privacy Commissioner for Personal Data* [2004] 2 HKLRD 840.

[62] Article 85 of the Basic Law provides, *"The Courts of the Hong Kong Special Administrative Region shall exercise judicial power independently, free from any interference. Members of the judiciary shall be immune from legal action in the performance of their judicial functions."*

[63] Section 2A(1) of the Interpretation and General Clauses Ordinance, Cap 1 has made it clear that *"All laws previously in force shall be construed with such modifications, adaptations, limitations and exceptions as may be necessary so as not to contravene the Basic Law and to bring them into conformity with the status of Hong Kong as a Special Administrative Region of the People's Republic of China."*

Chapter 11

Data Protection Principle 6(e) to (g) and the Data Correction Provisions in Part V

The main questions:

- What is the relationship between a data correction request and a data access request?
- How can a data user comply with a data correction request?
- When shall, or may, a data user refuse to comply with a data correction request?
- What steps must a data user take in refusing to comply with a data correction request?

The questions discussed in this chapter concerning data correction requests, DPP6 and Part V of the Ordinance have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

Relationship between data correction request and data access request

11.1 **Data Protection Principle 6**, after providing for an individual's data access rights under paragraphs (a) to (d), proceeds to provide for his data correction rights under paragraphs (e) to (g) as follows:

> ***"Principle 6 – access to personal data***
>
> *A data subject shall be entitled to –*
>
> *. . .*
>
> *(e) request the correction of personal data;*
>
> *(f) be given reasons if a request referred to in paragraph (e) is refused; and*
>
> *(g) object to a refusal referred to in paragraph (f)."*

11.2 More specifically, the term "**data correction request**" is defined in section 2(1) as "*a request under section 22(1)*", and **section 22(1)** provides as follows:

> *"(1) Subject to subsection (2), where –*
>
> *(a) a copy of personal data has been supplied by a data user in compliance with a data access request; and*
>
> *(b) the individual, or a relevant person on behalf of the individual, who is the data subject considers that the data are inaccurate,*
>
> *then that individual or relevant person, as the case may be, may make a request that the data user make the necessary correction to the data."*

11.3 From the above, it should be noted that a data correction request applies only to personal data a copy of which has been provided to the requestor pursuant to an earlier data access request. In other words, a data correction request must be preceded by a data access request.

11.4 It also follows that where a data access request has been properly refused by a data user (for example, pursuant to an applicable exemption under Part VIII of the Ordinance), there can be no subsequent data correction request made in respect of the data in question. In this sense, the exemptions under Part VIII that apply to data access could be interpreted as applying equally to data correction.

11.5 In terms similar to those applicable to a data access request, section 22(1) allows a data correction request to be made by a data subject or by "*a relevant person on behalf of*" the data subject. The issues concerning the meaning of this phrase

have already been discussed in paragraphs 10.12 to 10.14 in Chapter 10, to which the reader may refer.

11.6 As in the case of a data access request, although section 24(3)(a) allows a data user to refuse to comply with a data correction request not made "*in writing in the Chinese or English language*", the non-fulfilment of this condition does not, strictly speaking, prevent the request from being a data correction request (albeit one that may be legitimately refused). An important consequence of this is that the data user refusing the request on such ground will still be required to comply with the requirements applicable to such refusal, as will be discussed in paragraphs 11.22 to 11.28 below. In any case the AAB has considered in *AAB No. 12/2008* that a data correction request cannot be made verbally.

11.7 Similarly, neither section 22(1) nor any other provision in the Ordinance provides for any particular way in which a data correction request must be framed. However, since a data correction request must be preceded by a data access request, by the time the data user receives the data correction request, he should be aware of its nature as such.

Compliance with a data correction request

11.8 **Section 23(1)** of the Ordinance, which deals with compliance with a data correction request, provides as follows:

> *"(1) Subject to subsection (2) and section 24, a data user who is satisfied that personal data to which a data correction request relates are inaccurate shall, not later than 40 days after receiving the request –*
>
> *(a) make the necessary correction to those data;*
>
> *(b) supply the requestor with a copy of those data as so corrected; and*
>
> *(c) subject to subsection (3), if –*
>
> *(i) those data have been disclosed to a third party during the 12 months immediately preceding the day on which the correction is made; and*
>
> *(ii) the data user has no reason to believe that the third party has ceased using those data for the purpose (including any directly related purpose) for which the data were disclosed to the third party,*
>
> *take all practicable steps to supply the third party with a copy of those data as so corrected accompanied by a notice in writing stating the reasons for the correction."*

11.9 The first point to note from the above is that, a data user is obliged to comply with a data correction request only if it is "*satisfied that the personal data to which the data correction request relates are inaccurate*". Where the data user is not satisfied that is so, the data user may refuse to comply with the data correction request in accordance with section 24(3)(b), as discussed in paragraphs 11.17 to 11.21 below.

11.10 Another point to note is that "**correction**", in relation to personal data, is defined in section 2(1) as meaning "*rectification, erasure or completion*". How this has been applied by the Commissioner is illustrated in a complaint case, in which the complainant made a data correction request to a government bureau in relation to a file minutes kept by the bureau. The minutes, being the record of an interview with a third person, contained certain information provided by the third person in the interview about the complainant, information which later proved to be inaccurate. The complainant therefore requested the deletion of his data contained in the minutes.

11.11 Rather than deleting the data, the government bureau created a note in the same file clearly pointing out the inaccuracy of the information contained in the minutes. A copy of the file note was provided to the complainant. Also, a marker was added to the relevant file to refer the reader to the new file note.

11.12 Although the complainant was dissatisfied with the manner in which his request had been complied with, the Commissioner took the view that what the government bureau had done was in effect "*rectification*" or "*completion*" of the relevant data, and as such, amounted to adequate compliance with section 23(1). This is because the manner of compliance was regarded as more appropriate than simply deleting the data as suggested by the complainant so as to preserve a true record of what the third person had actually said in the interview, despite the accuracy of the information spoken about.

11.13 Finally, insofar as compliance with a data correction request involves, *inter alia*, providing a copy of the corrected data to the requestor, it is to be noted that **section 28(1)** provides as follows:

> *"(1) A data user shall not impose a fee for complying or refusing to comply with a data access request or data correction request unless the imposition of the fee is expressly permitted by this section."*

11.14 While section 28(2) expressly permits imposing a fee for compliance with a data access request, section 28 contains no similar provision for a data correction request. It follows therefore that a data user cannot impose any fee for compliance with a data correction request.

Circumstances in which a data user shall or may refuse to comply with a data correction request

11.15 The circumstances in which a data user shall refuse to comply with a data correction request are given under **section 24(1)**, which provides as follows:

> *"(1) Subject to subsection (2), a data user shall refuse to comply with section 23(1) in relation to a data correction request if the data user is not supplied with such information as the data user may reasonably require –*
>
> *(a) in order to satisfy the data user as to the identity of the requestor;*
>
> *(b) where the requestor purports to be a relevant person, in order to satisfy the data user –*
>
> *(i) as to the identity of the individual in relation to whom the requestor purports to be such a person; and*
>
> *(ii) that the requestor is such a person in relation to that individual."*

11.16 It can be seen that these circumstances are similar to those provided for in section 20(1), in which a data user receiving a data access request is obliged to refuse to comply with the request.

11.17 Regarding the circumstances in which a data user receiving a data correction request may refuse to comply with the request, these are given under **section 24(3)**, which provides as follows:

> *"(3) A data user may refuse to comply with section 23(1) in relation to a data correction request if –*
>
> *(a) the request is not in writing in the Chinese or English language;*
>
> *(b) the data user is not satisfied that the personal data to which the request relates are inaccurate;*
>
> *(c) the data user is not supplied with such information as the data user may reasonably require to ascertain in what way the personal data to which the request relates are inaccurate;*
>
> *(d) the data user is not satisfied that the correction which is the subject of the request is accurate; or*
>
> *(e) subject to subsection (4), any other data user controls the processing of the personal data to which the request relates in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with that section."*

11.18 Again, most of the circumstances provided for in section 24(3) are largely similar to those provided for in section 20(3), under which a data user receiving a data access request may refuse to comply with such request. In addition, it is a ground for refusal, under paragraph (b), when the data user is not satisfied that the personal data to which the request relates are inaccurate.

11.19 In this regard, the Ordinance does not lay down any standard for determining whether a data user is justified in claiming that the data user is not "*satisfied*" that the personal data to which a data correction request relates are inaccurate. However, it has already been explained in paragraphs 6.7 and 6.8 in Chapter 6, in relation to the requirement for data accuracy under DPP2(1), that where the true essence of any allegation by an individual of an inaccuracy in data held lies in the dispute between two parties on matters that should be appropriately decided by a court or tribunal of competent jurisdiction, the parties should not turn to the Commissioner for deciding the dispute. Thus, the Commissioner will only intervene when a data user refuses to correct an obvious inaccuracy in the personal data it holds. In the case of *AAB No. 22/2000*, the complainant made a data correction request to his ex-employer regarding allegations made against him in his letter of termination. The Commissioner took the view that in refusing to amend the letter of termination as requested, the employer was not in breach of section 23(1). On appeal to the AAB, the AAB upheld the Commissioner's view that the Ordinance was inapplicable to the case. In particular, according to the AAB, if an employee is dissatisfied with the grounds for termination, he should seek to resolve the dispute through other legal channels, such as taking the case to the Labour Tribunal. In this respect, the Commissioner cannot assume the role of a presiding officer of the Tribunal in deciding the validity of the grounds for termination.

11.20 It is perhaps worth mentioning here that in many of the complaint cases that came before the Commissioner, aggrieved employees often seek to rely upon their data correction rights under the Ordinance in attempting to "*correct*" the opinions or comments expressed in appraisal reports or letters of dismissal issued by employers or supervisors. Save for an obvious mistake or omission committed by the data user, it is beyond the jurisdiction of the Commissioner to assume the role of an adjudicator or arbitrator to resolve any dispute between these antagonistic parties. Such disputes should be more appropriately dealt with through other proper legal channels. A recent example is *AAB No. 12/2008*, in which an employee complained to her employer alleging that she had been receiving unfair treatment by her supervisor. Upon investigation, the employer found that the employee's complaint was not substantiated. The employee subsequently made a data access request to the employer for copy of all her personal records and the employer complied with the request. After receiving the documents from her employer, the employee complained to the Commissioner against the employer, alleging that there were 16 items of "incorrect facts" she found in the documents. The Commissioner considered that the alleged "incorrect

facts" concerned essentially employment disputes on unfair treatment and discrimination, it was not for the Commissioner to resolve disputes on errors of facts. The Commissioner decided not to carry out an investigation. On appeal, the AAB agreed that the Commissioner was not empowered to investigate such matters relating to the employee's employment.

11.21 It is common that the data subjects and the data users may have contradictory views on the correctness of opinion data. For instance, a patient would disagree with a doctor's diagnosis of mental illness. Pursuant to section 24(3), a data user may refuse to comply with a data correct request if the data user is not satisfied that the personal data to which the request relates are inaccurate. In respect of medical opinion, for instance, the Commissioner would not be in a position to comment on the accuracy or otherwise of an opinion made by a medical professional. In *AAB No. 42/2006*, the AAB stated in its decision: ". . . *[the AAB] is not in a position to find any error in the Commissioner's view that he would not be in a position to determine whether the opinions concerning the mental condition of the Appellant contained in the Forms were accurate or not. That is clearly something beyond the scope of the Commissioner's duty.*"

Steps to take in refusing to comply with a data correction request

11.22 Usually, where a data user refuses to comply with a data correction request, two basic steps should be taken: first, to put a relevant entry in its log book as required under section 27(2)(c) and (3)(c), and secondly, to notify the requestor in accordance with section 25(1).

11.23 In this connection, **section 27(2)(c)** and **(3)(c)** provide as follows:

> *"(2) A data user shall in accordance with subsection (3) enter in the log book –*
>
> *. . .*
>
> *(c) where pursuant to section 24 the data user refuses to comply with section 23(1) in relation to a data correction request, particulars of the reasons for the refusal;*
>
> *. . .*
>
> *(3) The particulars required by subsection (2) to be entered by a data user in the log book shall be so entered –*
>
> *. . .*
>
> *(c) in the case of the particulars referred to in paragraph (c) of that subsection, on or before the notice under section 25(1) is served in respect of the refusal to which those particulars relate; . . ."*

11.24 **Section 25(1)** provides as follows:

> *"(1) A data user who pursuant to section 24 refuses to comply with section 23(1) in relation to a data correction request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor –*
>
> *(a) of the refusal and the reasons for the refusal . . ."*

11.25 The above requirements to enter into a log book the refusal to comply with a data access request, and to give notification of such refusal to the requestor, are similar to the corresponding requirements in relation to a data access request. Regarding the requirement for a data user to keep a log book under section 27(1), the reader is referred to the discussion in paragraphs 10.61 to 10.63 in Chapter 10.

11.26 Finally, where the data correction request relates to data that constitute an "**expression of opinion**", there are additional requirements for the data user to comply with. These are provided for in **section 25(2)** and **(3)**, as follows:

> *"(2) Without prejudice to the generality of subsection (1), where –*
>
> *(a) the personal data to which a data correction request relates are an expression of opinion, and*
>
> *(b) the data user concerned is not satisfied that the opinion is inaccurate, then the data user shall –*
>
> *(i) make a note, whether annexed to that data or elsewhere –*
>
> *(A) of the matters in respect of which the opinion is considered by the requestor to be inaccurate; and*
>
> *(B) in such a way that those data cannot be used by a person (including the data user and a third party) without the note being drawn to the attention of, and being available for inspection by, that person; and*
>
> *(ii) attach a copy of the note to the notice referred to in subsection (1) which relates to that request.*
>
> *(3) In this section, "expression of opinion" (意見表達) includes an assertion of fact which –*
>
> *(a) is unverifiable; or*
>
> *(b) in all the circumstances of the case, is not practicable to verify."*

11.27 What amounts to an "*expression of opinion*" hinges on the distinction between factual and evaluative statements and is often a matter of form and difficult to judge. The evaluative statements made by one person against the other, such as, those made in an appraisal report or in a letter of termination of employment, are often the subject of dispute by dissatisfied data subjects. While it is easy to ascertain and correct factual statements, for example, the name, age, address, or identity card number of the data subject, the Ordinance recognizes the difficulty of assessing the *"correctness"* of an evaluative statement. Other courses of action, like a civil claim for defamation or the filing of an employee claim for unlawful dismissal seem to be the more suitable channels for redress.

11.28 As an illustration of how section 25(2)(b)(i)(B) has been applied by the Commissioner, in a complaint brought against an educational institution, it was found that the institution had kept, in two of its departments, the same record of an expression of opinion about a staff member. In response to a data correction request from the staff member, the educational institution had caused a note under section 25(2)(b)(i) to be annexed to the record kept in one department, but had omitted to do the same to the record kept in the other department. As a result of this omission, the educational institution was found to have contravened section 25(2).

Chapter 12

Exemption Provisions in Part VIII

The main questions:

- What are the different categories of exemption provisions contained in Part VIII?
- What is the scope of the "domestic purposes" exemption intended to be covered by section 52?
- When do employment-related exemptions in sections 53 and 54 and the evaluative process exemptions in sections 55 and 56 apply?
- What is the effect of invoking section 57, i.e. security, etc. of Hong Kong in denying a data access request?
- What are the Commissioner's views on the operation of section 58?
- When does legal professional privilege exempted under section 60 arise?
- What constitutes "news activity" exempted under section 61?

The questions discussed in this chapter concerning the exemption provisions in Part VIII of the Ordinance have been selected on the basis of their practical importance in light of the Commissioner's own experience. Before reading this chapter, the reader should read paragraphs 1.6 to 1.11 in *Chapter 1 – Introduction*, which contain important information on using this Book in general.

Exemptions in general

12.1 **Section 51** in Part VIII of the Ordinance provides as follows:

> *"Where any personal data are exempt from any provision of this Ordinance by virtue of this Part, then, in respect of those data and to the extent of that exemption, that provision neither confers any right nor imposes any requirement on any person, and the other provisions of this Ordinance which relate (whether directly or indirectly) to that provision shall be construed accordingly."*

12.2 Accordingly, sections 52 to 63A provide for specific exemptions from all or some of the provisions of the Ordinance. Broadly speaking, the exemption provisions in Part VIII may be divided into the following categories:

- exemption from DPPs, Parts IV and V and sections 36 and 38(b) – section 52
- exemption from DPP6 and section 18(1)(b) for (mainly) employment-related data – sections 53 to 56
- exemption from DPP3, DPP6 and section 18(1)(b) – sections 57 to 59
- exemption from all the provisions of the Ordinance – section 58A
- exemption from DPP6 and section 18(1)(b) of the Ordinance – section 60
- exemption from DPP3, sections 36 and 38(b) and limited exemption from DPP6, sections 18(1)(b) and 38(i) – section 61
- exemption from DPP3 – section 62
- exemption from section 18(1)(a) when compliance with data access request under section 18(1)(b) is exempted by virtue of section 57 or 58 – section 63
- exemption from DPP6 and section 18(1)(b), and further exemption from section 18(1)(a) – section 63A

Section 52 – domestic purposes

12.3 Section 52 is generally taken as one of the broadest exemption provisions found in Part VIII of the Ordinance in that it exempts from application the data protection principles and other provisions of the Ordinance such as the submission of a data user's return and access to or correction of personal data, etc. in respect of personal data held for management of personal, family or household affairs or recreational purposes. A common example would be the holding of an address and telephone list of friends and relatives by an individual for communication purposes and social or recreational activities, such as the sending of Christmas cards.

12.4 To understand its scope of application, **section 52** provides as follows:

> ***"52. Domestic purposes***
>
> *Personal data held by an individual and –*
>
> *(a) concerned only with the management of his personal, family or household affairs; or*
>
> *(b) so held only for recreational purposes,*
>
> *are exempt from the provisions of the data protection principles, Parts IV and V and sections 36 and 38(b)."*

12.5 Although section 52 appears to be a broad exemption in Part VIII, the use of words such as "**held**", "**individual**" and "**only**" in this section necessarily limits its application accordingly. First, as decided by the AAB in *AAB No. 46/2006*, section 52 only applies to data already **held** by an individual and has no application to DPP1 in respect of collection of personal data. Second, section 52 applies to personal data held by an **individual**, as opposed to being held by a corporation. Third, the personal data must be held **only** for the management of personal, family, or household affairs or only for recreational purposes. Thus, if personal data are not held solely for these allowed purposes but for other purposes as well, then section 52 exemption is not be applicable.

12.6 A common example in which section 52 is invoked is found in situations where an individual, without the consent of his relative or friend, uses his or her personal data as a credit referee for a loan or credit application. Subsequently the individual defaults in repayment resulting in the credit provider, or their appointed debt collection agent pursuing the referee to locate the whereabouts of the debtor for recovery of the outstanding loan, causing him or her annoyance and distress. When complaints of this nature are received, the Commissioner will look at the totality of evidence and take into account factors such as whether any actual damage is suffered by the individual concerned, the relationship between the complainant and the party complained against and the purpose for which the personal data were held, processed or used before deciding whether section 52 exemption is applicable to the case in question.

12.7 An interesting point to note in the context of Chinese culture is the close linkage of kinship and the readiness to render mutual assistance. The question to be asked therefore, is whether this traditional concept turns the use of a relative's personal data as a credit reference in the situation mentioned above into a "*directly related purpose*" permitted under DPP3? Conceivably, it may be argued that to use a relative's personal data as a reference in a personal loan application by the individual is for a directly related purpose as the relatives, if asked for such assistance, would in most cases not object to the use. The argument follows

that if it can be established that there is no change of use of the personal data as allowed by DPP3, it would not be necessary to consider further the application of Part VIII exemptions to the act in question. The practice adopted by the Commissioner is to look at the facts of each case independently before any view is formed on the matter.

Sections 53 and 54 – staff planning and employment

12.8 **Section 53** is seen to be a straightforward provision which exempts from application DPP6 and section 18(1)(b) to personal data which consist of information relevant to a staff planning proposal to:

> *"(a) fill any series of positions of employment which are presently, or may become unfilled; or*
>
> *(b) cease any group of individuals' employment. . . ."*

12.9 It is clear that the wording of this section is not intended to apply to any single position occupied by a particular employee but to any series of positions or any group of individuals' employment. It is therefore only in a staff planning situation within the scope contemplated by section 53 that the employer can avail itself of this exemption and refuse to accede to a data access request made by a data subject. Furthermore, the Commissioner takes the view that section 53 should not apply where the data user merely anticipates a possible staff planning in future.

12.10 **Section 54(1)** is a 7-year transitional provision that ceased to be operative since 3 August 2002. The practical effect of section 54(1) was that it exempted from application DPP6 and section 18(1)(b) employment-related personal data held by the employer before 20 December 1996 (i.e. the effective date of the operation of the Ordinance) which were provided by the individual on the implicit or explicit condition that the data subject would not have access to the data. This transitional provision aimed to give employers time to adjust and familiarize themselves with the requirements introduced by the Ordinance without causing them undue hardship.

12.11 In cases previously handled by the Commissioner involving a civil servant making a data access request to a particular government department that he worked under, the Commissioner has formed the view that although a civil servant is generally taken as being employed by the government, the department that he works under also qualifies as a data user as explained in paragraphs 4.16 to 4.18 in Chapter 4. Thus, the word "*employe*r" in the context of it being a data user and appearing in section 54(1)(a)(ii) should be liberally construed to mean the government department for which the data subject is working. The

rationale being that if a civil servant was always regarded as being employed by the government and not the individual department for which he or she worked, then the department, being the data user (yet never the employer of the civil servant), would not be in a position to avail itself of the section 54 exemption.

Section 55 – relevant process

12.12 **Section 55(1)** provides as follows:

> *"(1) Personal data the subject of a relevant process are exempt from the provisions of data protection principle 6 and section 18(1)(b) until the completion of that process."*

12.13 The term "**relevant process**" is in turn defined in sub-section (2) as follows:

> *" 'relevant process' –*
>
> *(a) subject to paragraph (b), means any process whereby personal data are considered by one or more persons for the purpose of determining, or enabling there to be determined –*
>
> *(i) the suitability, eligibility or qualifications of the data subject for –*
>
> *(A) employment or appointment to office;*
>
> *(B) promotion in employment or office or continuance in employment or office;*
>
> *(C) removal from employment or office; or*
>
> *(D) the awarding of contracts, awards (including academic and professional qualifications), scholarships, honours or other benefits;*
>
> *(ii) whether any contract, award (including academic and professional qualifications), scholarship, honour or benefit relating to the data subject should be continued, modified or cancelled; or*
>
> *(iii) whether any disciplinary action should be taken against the data subject for a breach of the terms of his employment or appointment to office;*
>
> *(b) does not include any such process where no appeal, whether under an Ordinance or otherwise, may be made against any such determination."*

12.14 In other words, before the completion, i.e. the making of the determination of the relevant process, the data user may refuse to comply with a data access request by invoking this exemption provision. As soon as the relevant process is completed, the exemption will no longer be available to the data user. However, it should be noted that pursuant to sub-section (2)(b), this exemption does not apply to cases where the data subject has no right to appeal against any such determination.

12.15 The meaning of the word "*appeal*" in section 55(2)(b) was considered in a complaint case in which the employer data user refused to comply with a data access request made by an employee on the grounds that the employee had right to "*appeal*" against the decision made against him in the relevant process. The "*appeal*" referred to was in fact a possible review by the Chief Executive of his own decision. The Commissioner came to the view that neither the type of review mentioned nor the limited form of judicial review (concerned largely with procedure rather than merit) by the courts of the decision made pursuant to completion of the relevant process would constitute an "*appeal*" within the meaning of section 55(2)(b).

Section 56 – personal references

12.16 **Section 56** concerns personal references –

> *"(a) given by an individual other than in the ordinary course of his occupation; and*
>
> *(b) relevant to another individual's suitability or otherwise to fill any position of employment or office which is presently, or may become, unfilled, . . ."*

12.17 In order to ensure that these personal references are given without fear of their being accessed by candidates prior to the determination of the selection process and being disputed as to the accuracy of the contents (which in most cases will comprise subjective personal comments or opinions), section 56 provides for an exemption from the application of DPP6 and section 18(1)(b) unless the person who gave the reference –

> *"(i) . . . has informed the data user in writing that he has no objection to the reference being seen by the individual . . . (or words to the like effect); or*
>
> *(ii) in the case of a reference given on or after the day on which this section comes into operation, until the individual . . . has been informed in writing that he has been accepted or rejected to fill that position or office (or words to the like effect), whichever first occurs."*

12.18 This exemption provision is comparatively easy to understand and apply. The condition (ii) mentioned above is in line with the completion of relevant process mentioned in section 55(2)(a)(i)(A) whereby personal data are considered for the purpose of determining the suitability, eligibility or qualifications of the data subject for employment or appointment to office.

12.19 It is worth noting that after the candidate has been informed in writing of the result of his job application, the data user could not then rely on this exemption provision to deny the data subject the right to make a data access request under section 18(1) of the Ordinance in respect of references given on, or after the coming into effect of, section 56. However, before complying with the provisions of DPP6 and section 18(1)(b), the data user should be careful to check whether the personal references may contain, other than the personal data of the data subject, also the personal data of other individuals, for example, the names or identifying particulars of referees. In complying with the data access request so made, the data user shall, pursuant to section 20(1)(b) and 20(2), give copies of the requested data only after the omission or editing out of the identifying particulars of such third parties unless the data user is satisfied that they have consented to the disclosure of their personal data to the requestor. An analysis of the application of section 20(1)(b) and 20(2) is found in paragraphs 10.41 to 10.49 in Chapter 10.

Section 57 – security, etc. in respect of Hong Kong

12.20 **Section 57** exempts from application the provisions of DPP6, section 18(1)(b) and DPP3 to personal data held or used for the following purposes: –

> *"(1) Personal data held by or on behalf of the Government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to prejudice any of the matters referred to in this subsection.*
>
> *(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which –*
>
> *(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and*
>
> *(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection, . . ."*

12.21 In determining whether exemption under sub-section (1) or (2) of section 57 is, or was at any time applicable to a particular case, the Commissioner will take

into account any certificate signed by the Chief Executive or Chief Secretary for Administration who are empowered under sub-sections (3) and (4) of section 57, as evidence of that fact, to certify that exemption is or was required or that personal data are or have been used for any purposes referred to in sub-section (1). They may also in the certificate direct the Commissioner not to carry out an inspection or investigation and the Commissioner shall comply with that directive.

12.22 This exemption is necessary in safeguarding security, defence or international relations in respect of Hong Kong. So far no appeal has been lodged with the AAB on the applicability of this exemption provision. For cases concerning non-compliance with a data access request, the Commissioner has taken a broad approach in deciding whether compliance with a data access request would jeopardize the purposes covered by sub-section (1).

12.23 The issue was illustrated in one case in which a complaint was lodged against a law enforcement agency for non-compliance with a data access request made under section 18(1). The requestor asked for records and documents in the law enforcement agency's possession that *". . . relate to or assist the [law enforcement agency] to come to the view or conclusion that I am a member of or linked to any triad society"*. The law enforcement agency refused to confirm or deny the existence or non-existence of the data. The reason put forward was that the disclosure of such information, even if it existed at all, would put the lives and well-being of those individuals who contributed the information to the law enforcement agency in jeopardy. Exemptions under sections 57(1), 58(1)(a) (i.e. the prevention or detection of crime) and 58(1)(b) (i.e. the apprehension, prosecution or detention of offenders) were invoked for non-compliance with the data access request. The Commissioner found that there was no contravention of DPP6 on the grounds that the elements of these exemption provisions were satisfactorily proved by the law enforcement agency.

12.24 In coming to the aforesaid conclusion, consideration was given by the Commissioner to the fact that for statements made in confidence by members of the public to the law enforcement agency, the law enforcement agency has a substantial interest to ensure that all statement makers give full and frank disclosure without fear of their statements being used later for another purpose. The candour and frankness of statements given by the public would be inhibited if the statements are liable to be accessed by the individuals mentioned therein.

Section 58 – crime, etc.

12.25 Among the various exemption provisions in Part VIII, **section 58** probably has the widest application, and thus deserves careful study. It covers personal data held for the following purposes:

> *"(1) (a) the prevention or detection of crime;*
>
> *(b) the apprehension, prosecution or detention of offenders;*
>
> *(c) the assessment or collection of any tax or duty;*
>
> *(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;*
>
> *(e) the prevention or preclusion of significant financial loss arising from –*
>
> *(i) any imprudent business practices or activities of persons; or*
>
> *(ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;*
>
> *(f) ascertaining whether the character or activities of the data subject are likely to have a significant adverse impact on any thing –*
>
> *(i) to which the discharge of statutory functions by the data user relates; or*
>
> *(ii) which relates to the discharge of functions to which this paragraph applies by virtue of subsection (3); or*
>
> *(g) discharging functions to which this paragraph applies by virtue of subsection (3), . . ."*

12.26 On the whole, section 58(1) and (2) provide respectively for exemption from DPP6 and section 18(1)(b), and exemption from DPP3. In particular, under section 58(1), exemption from DPP6 and section 18(1)(b) is available for any personal data that satisfy the following criteria:

- the data are **held** for any of the specified purposes (section 58(1)(a) to (g)); and
- the application of DPP6 and section 18(1)(b) to the data would either be **likely to prejudice** any of those purposes, or be **likely to identify** directly or indirectly the person who is the source of the data (section 58(1)(i) and (ii)).

12.27 In contrast, exemption from DPP3 is available under section 58(2) for any personal data that satisfy the following criteria:

- the **use** of the data is for any of the purposes specified in section 58(1) (section 58(2)(a)); and
- the application of DPP3 to such use would be **likely to prejudice** any of those purposes (section 58(2)(b)).

12.28 From the above, it can be seen that the purposes specified in paragraphs (a) to (g) of section 58(1) are important in determining the operation of section 58. The Commissioner takes the view that data users seeking to rely on section 58 have to obtain sufficient evidence to establish that the data are held or used for the specified purposes. Mere or general assertion that the data are held or used for the specified purposes may not be sufficient[64].

12.29 Among the purposes set out in section 58(1), those specified in paragraphs (a), (b) and (c), namely, "*the prevention or detection of crime*", "*the apprehension, prosecution or detention of offenders*" and "*the assessment or collection of any tax or duty*", appear to be relatively straightforward. In deciding on the meaning of the word "crime" under section 58(1)(a), the Commissioner took the view that it only applies to crime under the laws of Hong Kong[65]. Similarly, section 58(1)(b) should only apply to offences under the laws of Hong Kong.

12.30 In comparison, the other purposes specified in paragraphs (d) to (g) appear to be more complicated. Of these, the purposes specified under paragraph (d), namely, *"the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons"*, probably have the greatest practical importance. *AAB No. 26/2004* is an example on dishonesty. In the appeal, the complainant being a member of the disciplinary forces was subjected to disciplinary hearings which had to be repeatedly postponed as a result of the complainant's sickness. With reasonable suspicion, the employer disclosed the fact about the holding of disciplinary hearings to the complainant's doctors in order to obtain a medical certificate regarding his physical and mental fitness to attend the hearing. The AAB held that disclosure in the circumstances of the case met the exempted purpose under section 58(1)(d), i.e. for "*prevention, preclusion or remedying . . . of dishonesty . . .*" in avoiding the proceedings.

12.31 A "deeming" provision for what constitutes "*seriously improper conduct*" is found in section 2(9). It is deemed to be seriously improper conduct when a person who holds any office, profession or occupation and is required by any law or rule to be a fit and proper person to hold such office, profession or occupation, ceases to be a fit and proper person. Section 2(13) also takes it to be seriously improper conduct if such conduct by a person has made him or could have made him a disqualified person or a suspended person under the Rules of Racing and Instructions by the Stewards of the Hong Kong Jockey Club. However, for conduct not otherwise falling within the statutory definitions mentioned, the term "*seriously improper conduct*" has received judicial scrutiny in the cases of *M v M* [1997] HKFamC 2, and *Lily Tse Lai Yin & Others v. The Incorporated Owners of Albert House & Others* [2001] HKCFI 976.

[64] *AAB No. 64/2005*

[65] *AAB No. 16/2007*

12.32 In *M v M*, an ex-wife sought from the Housing Department the current address of her divorced husband, with a view to enforcing her right to maintenance payments pursuant to a court order. The Department refused to disclose such personal data about the husband on the grounds that this might be contrary to DPP3. Saunders, Deputy D.J. (as he then was) ruled, however, that although there is no definition in the Ordinance of the expression *"seriously improper conduct"*, the failure to pay maintenance in breach of the Court Order amounted to a contempt of court and as such was *"seriously improper conduct"* as those words are naturally used and understood in section 58(1)(d). In the circumstances of the case, the application of the provisions of DPP3 to the use of the data would prejudice the wife's taking steps to prevent the husband's seriously improper conduct. Accordingly, the exemption from DPP3 under section 58(2) was available.

12.33 On the application of section 58(2) in general, the judge had the following observations:

"*I accordingly find that where a person is in breach of a Court order and another person, being entitled to the benefit of that order, wishes to enforce the order, then, by virtue of the provisions of s.58(2) of the Data Privacy Ordinance, a data user is exempt from the provisions of data protection principle 3 and may supply the information upon appropriate request.*"

12.34 In contrast, the failure to honour a cheque by a person, without evidence of fraud or dishonesty, might not *per se* amount to "*seriously improper conduct*" to justify invoking the exemption provision under section 58(1)(d) as this view was expressed by the AAB in *AAB No. 14/2004.* The appeal concerned the disclosure by a licence issuing authority to an applicant's employer being a government department the fact that the cheque for payment of the licence fee was not honoured upon presentation. The AAB took the view that the licence issuing authority could not avail itself of the exemption under section 58(1)(d).

12.35 In *Lily Tse Lai Yin*'s case, the plaintiffs claimed damages in respect of an accident involving a collapsed canopy. In an application in chambers, they applied for non-party discovery against the Director of Buildings, the Director of the Urban Services Department and the Commissioner of Police, for the inspection of certain files held by them. It was contended on behalf of the respondents, however, that the disclosure of those files to the plaintiffs would give rise to a contravention of DPP3 in relation to personal data contained therein.

12.36 In his judgment, Suffiad J. ruled that the use of personal data in a civil action for damages resulting from the collapse of the canopy would fall within the meaning of "*the remedying of unlawful conduct*" under section 58(1)(d). He said:

"*Firstly, I note that* (sic) *in section 58(1), the use of the word 'crime' in paragraph (a) and the word 'offender' in paragraph (b). This to my mind suggest* (sic),

therefore, that the use of the words "unlawful or seriously improper conduct" in paragraph (d) extend (sic) *beyond criminal conduct to include civil wrongs. Secondly, the use of the word 'remedying' in paragraph (d) is again suggestive of the same thing. The most natural meaning that can be given to the word 'unlawful' is that it normally describes something which is contrary to some law or enactment or is done without lawful justification or excuse. (See R. v. R. [1991] 4 All ER 481 per Lord Keith of Kinkel at page 484.)*

Since tort is a civil wrong, the bringing of a civil claim for damages in tort amounts to the remedying of unlawful or seriously improper conduct. For these reasons, I have no hesitation in coming to the conclusion that the words contained in section 58(1)(d) of the Personal Data (Privacy) Ordinance is (sic) *sufficiently wide to cover a claim for damages in a personal injuries and/or fatal accident case.*"

12.37 The analysis of Suffiad J. was adopted in *Cinepoly Records Co. Ltd. and Others v Hong Kong Broadband Network Ltd and Others* [2006] HKLRD 255, in which 7 music producers sought discovery from 4 internet service providers the names, identity card numbers and addresses of 22 alleged online copyright infringers. The Court in *Cinepoly* case ruled that the phrase "unlawful and seriously improper conduct" covers copyright infringement, and the music producers' use of the personal data sought was clearly for the purpose of prevention, preclusion (in the form of injunctions) or remedying of the copyright infringements of the producers' musical works.

12.38 Whether a conduct would amount to "*seriously improper conduct*" depends on the fact of each case. A conduct which does not appear to be "seriously improper" in nature, e.g. serious indebtedness, may be "seriously improper" in the circumstances of the data subject. In *AAB No. 5/2006*, the AAB considered that serious indebtedness of an officer of a law enforcement agency was contrary to the disciplinary guidelines of the law enforcement agency and amounted to "seriously improper conduct".

12.39 Even if the data are held or to be used for any of the purposes specified in paragraphs (a) to (g) of section 58(1), the exemption does not apply unless data users can also establish that application of DPP6 and section 18(1)(b), and DPP3, as the case may be, would be likely to prejudice the said purposes. Whether or not the specified purposes would be likely be prejudiced does not depend on the subjective view of the data user. The standard is an objective one[66]. The more enquiries and evidence the data users reasonably make and obtain to establish the prejudice requirement, the more likely that they may satisfy this objective requirement.

12.40 There is usually little or no doubt that the requested data provided to the law enforcement agency would be used in the discharge of the agency's functions (e.g. the prevention or detection of crime, the assessment or collection of any tax or

[66] *AAB No. 5/2006*

duty, etc.), the matter of which would fall within section 58(1). What may be less certain, however, is whether the effect of the failure to use such data in a particular case would indeed be so serious as to be "*likely to prejudice*" any such matters, as required by section 58(2)(b). The view generally taken by the Commissioner is that in case of doubt, it is prudent for the data user to ask the law enforcement agency why the data were considered necessary and, in particular, how the failure to use such data would be likely to prejudice the intended purpose.

12.41 In addition to providing for exemption from DPP3, section 58(2) also creates a defence for a data user who shows, in any proceedings relating to the use of data contrary to DPP3, that he "*had reasonable grounds for believing that failure to so use the data would have been likely to prejudice*" any of the matters mentioned in section 58(1)(a) to (g). Illustration of the potential importance of this defence, and of how the Commissioner has taken his operational stance in applying it, may be found in cases involving requests for information by law enforcement agencies.

12.42 In cases where the information being sought contains personal data, their disclosure by the data user to a law enforcement agency pursuant to a mere request (as opposed to a formal demand in the exercise of a legal or statutory power) is likely to fall outside the purposes for which such data were originally collected. To avoid any contravention of DPP3 in their disclosure by the data user, consideration of the application of exemption under section 58(2) becomes relevant.

12.43 Given the sensitive nature of most law enforcement operations, in so asking, the data user may not perhaps always be able to obtain a reply that contains clear proof that the *"prejudice*" test in section 58(2)(b) has been satisfied. Nevertheless, it is still likely that the law enforcement agency may provide some information, or confirmation of a general nature, on which the data user may reasonably rely. By asking for the supply of more information, the data user is put in a better position to invoke the defence under section 58(2) in any subsequent proceedings or complaint against it for alleged contravention of DPP3 in the disclosure of the data.

Section 58A

12.44 Section 58A contains the broadest exemption in Part VIII. Pursuant to the provisions, any personal data which are or are contained in any communication or material (including their copies) obtained pursuant to the prescribed authorizations given by the panel judges or the authorizing officer for interception and covert surveillance under Interception of Communications and Surveillance Ordinance are exempt from the provisions of the Ordinance. In addition, any personal data system which is used by a data user for the collection, holding, processing or use of the relevant personal data are exempted from the provisions of the Ordinance.

Section 59 – health

12.45 Personal data relating to the physical or mental health of the data subject are generally viewed as confidential and sensitive personal data that should be carefully guarded against unlawful use and access. However, the right to protect these data may have to give way when the harm that it will cause to others (including the data subject himself) outweighs the benefit of strict compliance with DPP3 and DPP6. How this is to be assessed and balanced is exemplified in section 59.

12.46 The criterion laid down in **section 59** exempting physical and mental health data from the provisions of DPP3, DPP6 and section 18(1)(b) is when:

> *". . . the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of –*
>
> *(i) the data subject; or*
>
> *(ii) any other individual."*

12.47 The burden of proof is seen not to be a particularly onerous one for a data user to discharge as he is only required to prove that the application of those provisions of the Ordinance **would be likely** to cause serious harm to the physical or mental health of the data subject or any other individuals. No actual serious harm needs to be proven to have been suffered. Although section 59 does not spell out whether the harm test mentioned therein is a subjective or objective one, in cases brought before the Commissioner, due consideration will be given as to whether a reasonable man in the circumstances of the case would come to the same conclusion as the data user in question. In a complaint case lodged against a Chinese herbal medical practitioner who failed to comply with a data access request by his patient for copies of the medical prescriptions prescribed for him, the medical practitioner relied upon section 59 exemption as grounds for refusal. The Commissioner found that the exemption did not apply in the circumstances of the case as the disclosure would not be likely to cause serious harm to the physical or mental health of the data subject. On the contrary, the refusal to supply the information on the medicines prescribed for the patient would be more likely than not to cause harm to the requestor. It has always been the regulatory philosophy of the Commissioner that in situations where less privacy intrusive alternatives are available to achieve the same result, they should first be explored and resorted to unless there are good reasons for not doing so.

12.48 Illustration of the application of section 59 is found in a case in which an employee expressed suicidal intent to his employer. From the staff records kept by the employer, it was evident that he had been a patient of a psychiatric hospital. Led by the belief that the person might cause serious physical harm to himself, the employer disclosed the information to the psychiatric hospital for

medical follow up. The Commissioner was satisfied that since the life and limb of the data subject was at stake, section 59 was properly invoked to exempt the application of DPP3 to the personal data of that person held by his employer.

12.49 In a complaint case, a mechanic suffered injury from work and required psychological treatment. His employer, a public transport company, referred the mechanic to an organization for such treatment. During the course of the treatment, the mechanic told the psychiatrist and a counselor of the organization that he had planned to bomb the public transport system operated by his employer. Having consulted the mechanic's psychiatrist, the organization informed the mechanic's employer accordingly with a view to warning the employers and protecting the safety of the mechanic himself and the public. The mechanic was subsequently dismissed by the employer. The mechanic complained against the organization for having disclosed information about his health condition to his employer without his prescribed consent, in contravention of DPP3. The Commissioner considered, among others, that the information related to the mental health of the mechanic and should be exempted under section 59. In the circumstances, the organization was not required to comply with DPP3 in disclosing the information to the mechanic's employer. On appeal in *AAB No. 15/2009*, the AAB accepted that the decision of the organization in disclosing the information to the employer was reached upon detailed consideration and proper balance between the interests of the mechanic's data privacy and public safety. The AAB agreed that the personal data disclosed by the organization were exempted under section 59.

12.50 It is however to be noted that section 59 has only a narrow application to physical and mental health data and it does not extend to exempt disclosure of other data such as location data of the data subject.

Section 60 – legal professional privilege

12.51 This exemption reinstates the basic rule of evidence that exempts from discovery proceedings communications between a legal adviser and his or her clients for the purpose of obtaining legal advice or when litigation is contemplated. This legal professional privilege is important so that legal advice may be safely and sufficiently obtained and protected. It is a right recognized by the Basic Law[67] which provides that Hong Kong residents shall have the right to confidential legal advice.

12.52 For this exemption to apply, **section 60** does not require absolute proof of the existence of the privilege but a plausible claim to such privilege will suffice as the wording, "*in respect of which a claim to legal professional privilege* ***could be maintained in law***" suggests. The validity or otherwise of the claim is therefore ultimately, a matter for the court not the Commissioner to decide.

[67] Article 35 of the Basic Law of Hong Kong.

12.53 This exemption therefore operates to exempt personal data from the application of DPP6 and section 18(1)(b) as any data access request for personal data so held would be contrary to the concept of protection of this "*privileged*" information. This is particularly so when a party to litigation might seek to use a data access request to obtain personal data held by the other party's legal adviser about him or her, sometimes motivated by the ulterior intent of fishing for useful information.

12.54 This happened in a complaint case handled by the Commissioner in which a defendant of an ongoing litigation action made a data access request to the plaintiff's solicitors for *"all data held by you in respect of myself and all personal data passed by you to third parties"*. As it turned out, information containing personal data of the defendant was directly or indirectly obtained by the plaintiff's solicitors from their client in the conduct of the litigation and used in the course of legitimate legal enquiries. On the basis that such personal data were held and used by the solicitors in relation to an ongoing litigation case and held in their legal capacity as legal adviser to the plaintiff, the Commissioner came to the view that a claim for legal professional privilege could be maintained in law, hence section 60 exemption was properly invoked to refuse such data access request.

12.55 In another case handled by the Commissioner, an individual sought from his insurer, by means of a data access request under section 18(1)(b), a copy of the loss adjuster's report prepared for his claim for compensation relating to an alleged car accident. The insurer refused to comply with the data access request on the ground that the personal data in the said report were exempted from being accessed by means of legal professional privilege. Despite the fact that the insurer honoured the claim subsequently without going through any litigation, there was evidence to show that the insurer had found the claim suspicious and therefore had the report prepared with the dominant purpose to seek legal advice in relation to the contemplated litigation. The Commissioner came to the view that the report could be protected by legal professional privilege and that section 60 exemption was properly invoked. The same rationale applies in respect of medical reports obtained by an insurance company for the purpose of seeking legal advice in response to an insurance claim lodged by the insured when litigation is contemplated.

12.56 The Commissioner is of the view that section 60 also applies to legal advice given to the data users by their internal legal advisers. In a case handled by the Commissioner, an individual made a complaint to a statutory body and applied for legal assistance from the statutory body in relation to the complaint. The statutory body subsequently turned down the complaint and the application. The individual made a data access request to the statutory body pursuant to section 18(1) for information in relation to her complaint and application. Pursuant to the request, the statutory body provided certain documents to the individual but

refused to disclose certain parts of the documents to the individual by relying on section 60. Since the parts which the statutory body refused to disclose to the individual are legal advice given by the body's internal legal department in relation to the complaint and the application, the Commissioner opined that the exemption under section 60 was available to the statutory body.

Section 61 – news

12.57 In striving to strike a fair balance between upholding the freedom of the press essential to journalists and the protection of the personal data privacy rights of individuals, section 61 is viewed as important in achieving this objective. Section 61 applies to personal data held by a data user who engages in news activity for the sole purpose of that activity and primarily seeks to protect the source of information and to limit the right of access to such information. As this exemption only applies in relation to "*news activity*", it is important to ascertain what kind of activity so qualifies.

12.58 The term "**news activity**" is defined in sub-section (3) to mean any journalistic activity and includes –

> *"(a) the –*
>
> *(i) gathering of news;*
>
> *(ii) preparation or compiling of articles or programmes concerning news; or*
>
> *(iii) observations on news or current affairs,*
>
> *for the purpose of dissemination to the public; or*
>
> *(b) the dissemination to the public of*
>
> *(i) any article or programme of or concerning news; or*
>
> *(ii) observations on news or current affairs."*

12.59 As no further definition is found in respect of the word *"news"*, its natural meaning is adopted to mean information about recent events or happenings, especially as reported by newspapers, periodicals, radio or television. The question as to whether the activity in question amounts to the gathering of news was dealt with in the *Eastweek* case. The Commissioner took the view that since the article in issue was written only as a commentary on dress sense and the criticism of an individual's taste in clothes was based on the random thoughts of the reporter rather than a report on fashion trends, the taking of the complainant's photograph to illustrate such an article, did not amount to news gathering. Though no ruling

was made as to the nature of reporting activities that constitute news gathering, Keith JA, the judge at first instance, concluded that it was open for the Commissioner not to regard the article in question as news gathering.

12.60 Since news activity depends very much on information that is being collected, the journalists are concerned that the source of information is free to disclose information without fear of contravening the requirements of the Ordinance, in particular, DPP3. It is not hard to imagine that the informant who discloses information, in particular, sensitive or "insider" information concerning personal data of another individual to the media will in most cases be committing an act in contravention of DPP3 unless doing so can be justified as a directly related purpose of their collection or with the prescribed consent of the data subject.

12.61 **Section 61(2)** comes in to exempt the source of information from the provisions of DPP3 if the following two criteria set out therein are satisfied, viz.:

> *"(a) the use of the data consists of disclosing the data to a data user referred to in subsection (1); and*
>
> *(b) such disclosure is made by a person who has reasonable grounds to believe (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not they are published or broadcast) is in the public interest."*

12.62 The first criterion is straightforward and easy to apply. What is less clear is the second part on what constitutes "*reasonable belief*" and "*public interest*" as both of these terms are not defined in the Ordinance. The terms as the Commissioner understands and applies them are illustrated in a complaint case concerning the disclosure of the personal data of the complainant (who was on the staff of a college) by the principal of the college contained in an accident investigation report in respect of an employee compensation claim.

12.63 The disclosure was made in circumstances where the principal was confronted by reporters who sought to verify with him the allegation made by the complainant's wife that the college had procrastinated in releasing compensation money to the complainant. In rebutting the allegation, the principal found it necessary to disclose information contained in the investigation report. In response to the complaint later lodged by the complainant with the Commissioner on alleged contravention of DPP3, the college raised section 61 exemption as a defence since the principal had reasonable grounds to believe that disclosure of the personal information in question was in the public interest, i.e. in defending the image of the college and to enable journalists to present a balanced news report. The Commissioner was satisfied that the requirements in section 61(2) were met.

12.64 Dissatisfied with the decision, the complainant appealed to the AAB under *AAB No. 23/1997*. The AAB agreed with the Commissioner's findings but did not give any definitive ruling on what constituted "*public interest*". It was said that each case should be decided on its own facts.

12.65 In handling complaints of this sort, the Commissioner is inclined to take a broad view of what constitutes the "*public interest*" in section 61(2) to mean and include the clear and strong public interest in having access to public information and a free press. The case would be strengthened when the personal data are disclosed to media for the purpose of serious news reporting. The Commissioner would in such cases be more ready to find that reasonable grounds exist to disclose the information in the public interest. Although the term "*public interest*" is not defined, fine distinction may need to be drawn between what the public is interested in knowing and what public interest there exists in disclosing the information.

12.66 As a corollary to exempting the application of DPP3 to the use of personal data in the public interest, Section 61(1) also exempts from application the provisions of DPP6 and section 18(1)(b) in preventing access to personal data unless the data are published or broadcast. This quells the concerns of journalists caused by requests from individuals to access the personal information they have collected in their news gathering activities prior to such data being published or broadcast.

12.67 Section 61(1) also has the effect in circumscribing the Commissioner's powers of inspection and investigation. The Commissioner has no power of inspection of any part of a personal information system that holds such information for the purpose of news activity (section 61(1)(ii)). Also, the Commissioner can only investigate a suspected contravention of the provisions of the Ordinance after the material that is the subject of the complaint has been published or broadcast (section 61(1)(i)) and only when he receives a complaint under section 38(a). In *AAB No. 34/2007*, a data requestor requested a newspaper for copies of emails from a person, who commented on the requestor and whose comments were reported in the newspaper. The data requestor argued that in order to ascertain whether the requested data were published or unpublished, all the contents of the requested data must be disclosed. The AAB rejected the argument and made the following comments: "*We believe this argument may have force if the Appellant may be able to demonstrate which part of the Article would have the effect as submitted. There is always a minimum threshold which the Appellant must show, at the least, that there is a prima facie case that there could be a reference in the published part to unpublished data, or somehow published and unpublished data are intertwined. To argue that there was a possibility of cross-reference or intertwining that would give rise to possible confusion is to argue in a vacuum. The logical extension of such argument would be that, . . . , all the contents of the email correspondence, whether or not their contents had not been published (and in the latter case should not be disclosed under the Section 61 exemption), must be disclosed otherwise the Commissioner nor the Appellant would not know if there had been any reference to an overlapping*

situation. This amounts to a submission that there can be no exemption under Section 61(1). We cannot accept such submission."

12.68 It is nevertheless worth noting that this exemption provision does not exempt from application the provisions of the other data protection principles with which the data user is still obliged to comply, in particular, DPP1(2), i.e. fair and lawful collection of personal data. Where a code of ethics[68] is in place, the press shall observe and follow it when collecting and using materials gathered for news reporting.

Section 62 – statistics and research

12.69 Section 62 is comparatively easy to understand and of practical importance in exempting personal data from being used for preparing statistics or carrying out research. The utility value to be served by compiling statistics or conducting research is self-explanatory and conducive to the well-being of society as a whole.

12.70 **Section 62** exempts from application DPP3 when the following conditions are satisfied:

> *"(a) the data are to be used for preparing statistics or carrying out research;*
>
> *(b) the data are not to be used for any other purpose; and*
>
> *(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them."*

12.71 In order not to fall foul of this exemption provision, the data user must be careful to ensure compliance with these requirements, in particular, the requirement in (c) above, i.e. that the resulting statistics or research does not reveal the identities of the data subjects, or is compiled in such a way that makes it reasonably practicable for their identities to be ascertained.

12.72 Very few complaints have been brought before the Commissioner on the application of this exemption provision. Insofar as the requirements mentioned in this exemption provision are met, these raw data may continue to be retained by the data user for so long as this exemption applies. The latest version of the Code of Practice on Consumer Credit Data has specifically provided for the retention of data by the credit reference agency[69] to be used for purposes exempted under section 62.

Section 63 – exemption from section 18(1)(a)

12.73 This exemption provision supplements the application of sections 57 and 58 when being invoked by a data user to refuse to comply with a data access request

[68] See the Joint Code of Ethics issued by the Hong Kong Journalists Association.

[69] See clause 3.7 of the Code which was revised and took effect on 1 June 2003.

made under section 18(1)(b). For scope of application of sections 57 and 58, the reader is referred to paragraphs 12.20 to 12.43 above.

12.74 The statutory duty to inform the data subject whether the data user holds his personal data under section 18(1)(a) is exempted under **section 63** which provides as follows:

> ***"Exemption from section 18(1)(a)***
>
> *Where a data access request relates to personal data which are or, if the data existed, would be exempt from section 18(1)(b) by virtue of section 57 or 58, then the data are also exempt from section 18(1)(a) if the interest protected by that exemption would be likely to be prejudiced by the disclosure of the existence or non-existence of those data."*

12.75 There may be situations where, for reasons of security and/or the prevention or detection of crime, etc. mentioned in sections 57 and 58, the mere disclosure of the fact that the data do exist or not, would be likely to prejudice the interest protected by these exemption provisions. The classic example is the one quoted in paragraph 12.23 where the disclosure of the data pursuant to section 18(1)(a) might put the lives and well-being of the informant in jeopardy.

12.76 Given the drafting of sections 57 and 58 as they presently stand which do not exempt from application section 18(1)(a), but for the existence of the saving provision of section 63, the data user would still be obliged to comply with section 18(1)(a) upon receipt of a data access request so made even though other conditions under sections 57 and 58, as the case may be, are met. Section 63 is thus viewed as important in providing the data user with a statutory basis insofar as the prejudice test therein laid down is satisfied to refuse to comply with a data access request made under section 18(1)(a), giving a more complete and meaningful application to sections 57 and 58.

Section 63A – Human embryos, etc.

12.77 This new section was added in August 2007. The section provides that if personal data consist of information showing that an identifiable individual was, or may have been, born in consequence of a medical, surgical, obstetric or other procedure assisting or otherwise bringing about human reproduction by artificial means, such personal data are exempt from DPP6 and section 18(1)(b). The data are also exempted from section 18(1)(a) if the interest protected by that exemption could be likely to be prejudiced by the disclosure of the existence on non existence of the data.

Appendix I

The Codes of Practice Issued by the Commissioner under Section 12 of the Ordinance

---

1. Code of Practice on Identity Card Number and other Personal Identifiers

Identity Card Numbers are commonly collected and used by a data user to identify individuals and manage records relating to them. Copies of Identity Cards are often collected by a data user for use as evidence of its dealings with the individuals concerned. The Commissioner holds the view that indiscriminate collection and improper handling of Identity Card Numbers and copies may unduly infringe the privacy of the individual, besides creating opportunities for fraud. The Code, gazetted on 19 December 1997, was issued for the purpose of providing guidance on the appropriate handling of personal identifiers in general and Identity Card Numbers and copies in particular. A "*personal identifier*" is usually a series of numbers or letters, such as a passport number or staff card number, that uniquely identifies an individual and the most commonly used personal identifier in Hong Kong is by far Identity Card Number.

2. Code of Practice on Consumer Credit Data

In the ordinary course of business, a credit provider, who subscribes to the services of a credit reference agency, may provide consumer credit data to the credit reference agency and in return obtain a credit report of the individual for credit checking and assessment. In order to ensure that necessary privacy safeguards are followed, the Code was first issued in February 1998 and has since been revised twice. The latest version of the Code took effect on 2 June 2003. The Code gives practical guidance to data users on the handling of consumer credit data in compliance with the requirements of the Ordinance. It deals with collection, accuracy, retention, use, security, access and correction issues as they relate to personal data of individuals who are, or have been, applicants for consumer credit. The Code covers, on the one hand, credit reference agencies, and on the other hand, credit providers in their dealings with credit reference agencies and debt collection agents.

3. Code of Practice on Human Resource Management

The primary objective of the Code is to provide practical guidance to employers and their staff on how to properly handle personal data that relate to each phase

of the employment process. It is issued to assist human resources practitioners in complying with the requirements of the Ordinance in their performance of human resources management functions and activities and it deals with issues concerning collection, holding, accuracy, use, security, data subject access and correction requests in relation to the personal data of prospective, current and former employees. The Code was gazetted on 20 September 2000 and became effective on 1 April 2001.

(N.B. It is to be noted that these Codes of Practice, though not legally binding, breach of the Codes will give rise to a presumption against the data user in any proceedings under the Ordinance. Section 13 provides in essence that:

(a) where a Code of Practice has been issued in relation to any requirement of the Ordinance;

(b) the proof of a particular matter is essential for proving a contravention of that requirement;

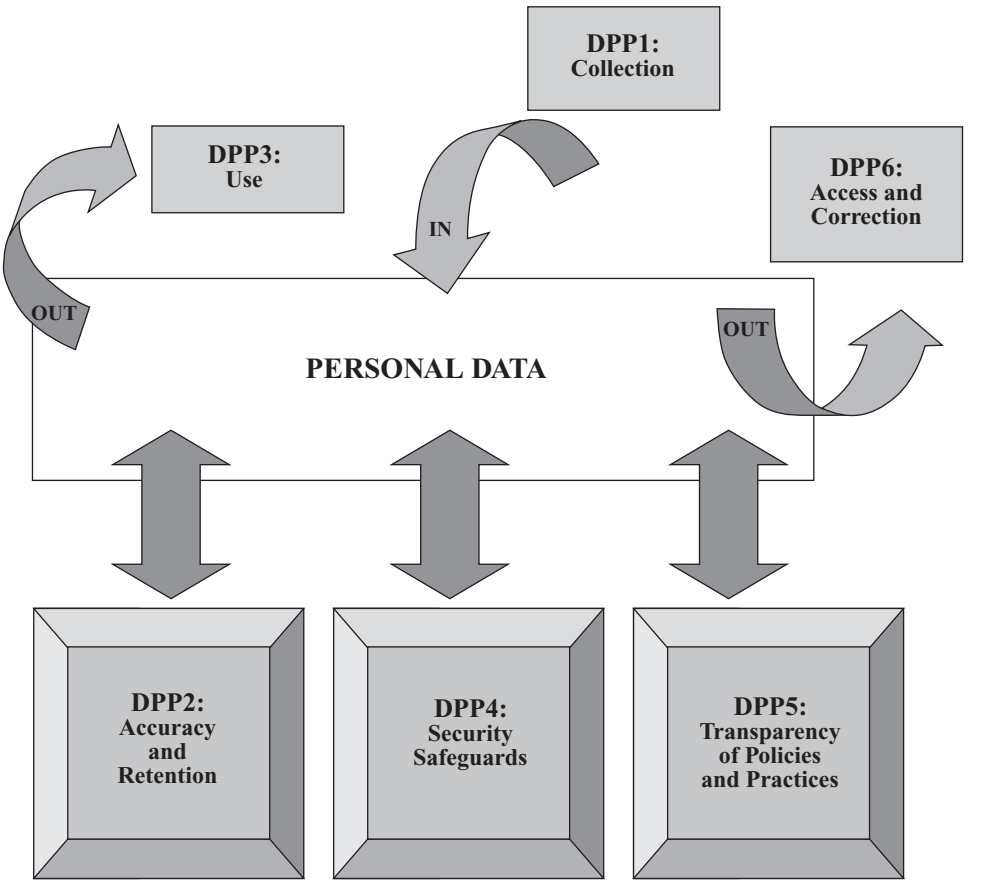
(c) the specified body conducting the proceedings (a magistrate, a court or the Administrative Appeals Board) considers that any particular provision of the Code of Practice is relevant to that essential matter; and if

(d) it is proved that that provision of the Code of Practice has not been observed;

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

Appendix II

Data Protection Principles: Relationship Chart



Appendix III

Checklist for Data Users in Ensuring Compliance with the Ordinance

The following are the pertinent questions that a data user should properly address in order to ensure that its personal data management practice complies with the requirements of the Ordinance:

1. Is there any function or activity involving the collection of personal data?

   (Please refer to Chapters 2, 3 and 4 on the meaning of "**personal data**", "**collection**" and **"data user"** respectively.)

2. What are the purposes of use? Is collection of personal data necessary and means of collection lawful and fair? Are data collected adequate and not excessive? What information should be provided to the data subject on or before collection?

   (Please refer to Chapter 5 for the requirements of **DPP1**.)

3. What are the practicable steps taken to ensure data accuracy and how long will the collected personal data be retained before erased?

   (Please refer to Chapter 6 for the requirements of **DPP2** and **section 26**.)

4. Does the use (which term includes disclosure and transfer) of personal data fall within the original purpose of collection or its directly related purpose?

   (Please refer to Chapter 7 for the requirements of **DPP3** and Chapter 12 on the applicability of the exemption provisions.)

5. What are the practicable steps taken to ensure that there are in place adequate security measures so that personal data collected are protected from unauthorized or accidental access, erasure or other uses?

   (Please refer to Chapter 8 for the requirements of **DPP4**.)

6. Are there privacy policies and practices in place and made generally available?

   (Please refer to Chapter 9 for the requirements of **DPP5**.)

7. Are the data access requests and data correction requests received being properly handled?

   (Please refer to Chapters 10 and 11 for the requirements of **DPP6** and **Part V** of the Ordinance.)

8. Are there any applicable exemptions from compliance with the relevant requirements of the Ordinance?

   (Please refer to Chapter 12 for the exemption provisions under **Part VIII** of the Ordinance.)

Appendix IV

Data Subject's Rights when his Personal Data Privacy Interest is Infringed

---

1. Mediation with the data user:

Mediation can be an effective and informal channel in abating the infringing act and in preventing repeated or continual acts or practice of personal data infringement. Sometimes misunderstanding of the application of the Ordinance can be clarified and avoided. The Commissioner encourages the conciliatory approach as a way of alternative dispute resolution.

2. Lodging of a complaint to the Commissioner under section 37:

An individual who wants to lodge a complaint can put it in writing in either Chinese or English, giving contact details and full particulars of the case to the Commissioner. For convenience, this can be done by using a complaint form obtainable from the Commissioner's office. The complaint will be handled in accordance with the Commissioner's Complaint Handling Policy. In general, the Commissioner will first liaise with the complainant to determine whether formal investigation should be commenced, e.g. where a *prima facie* case is established. The Commissioner may or may not liaise with the party complained against. If the Commissioner commences investigation and upon which it is revealed that the data user has contravened a requirement under the Ordinance, the Commissioner may serve an enforcement notice on the data user concerned to direct it to take steps to remedy the contravention. Contravention of an enforcement notice is an offence under section 64(7) of the Ordinance which could result in a fine and imprisonment. For cases where there are suspected contraventions of the provisions of the Ordinance, the Commissioner may, with the consent of the complainant, refer the case to the Hong Kong Police for investigation, to be followed by prosecution by the Department of Justice, where appropriate.

3. Appeal to the Administrative Appeals Board under section 9 of the Administrative Appeals Board Ordinance, Chapter 442, Laws of Hong Kong:

A data subject who is dissatisfied with the Commissioner's decision not to carry out or to continue to carry out an investigation has the right under section 39(4) of the Ordinance to make an appeal to the Administrative Appeals Board. A right is also conferred upon a data subject under section 47(4) of the Ordinance to appeal against a decision of the Commissioner not to serve an enforcement notice on the relevant data user in consequence of the investigation concerned.

4. Civil remedies:

Apart from criminal sanctions that can be imposed upon a data user who has contravened the Ordinance, where a data subject suffers damage by reason of a contravention of a requirement under the Ordinance by a data user, including injury to feelings, the data subject shall be entitled to compensation from the data user concerned through civil proceedings brought under section 66 of the Ordinance.

Appendix V

Data Protection Principles

1. Principle 1 – purpose and manner of collection of personal data

(1) Personal data shall not be collected unless –

(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are –

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that –

(a) he is explicitly or implicitly informed, on or before collecting the data, of –

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed –

(i) on or before collecting the data, of –

(A) the purpose (in general or specific terms) for which the data are to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which they were collected, of –

(A) his rights to request access to and to request the correction of the data; and

(B) the name and address of the individual to whom any such request may be made,

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

2. Principle 2 – accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that –

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used –

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that –

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

(ii) that data were inaccurate at the time of such disclosure,

that the third party –

(A) is informed that the data are inaccurate; and

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

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 – use of personal data

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

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 – security of personal data

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

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

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

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 – information to be generally available

All practicable steps shall be taken to ensure that a person can –

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 – access to personal data

A data subject shall be entitled to –

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data –

  (i) within a reasonable time;

  (ii) at a fee, if any, that is not excessive;

  (iii) in a reasonable manner; and

  (iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Appendix VI

Exemption Provisions under Part VIII of the Ordinance

Section 51 Interpretation

Where any personal data are exempt from any provision of this Ordinance by virtue of this Part, then, in respect of those data and to the extent of that exemption, that provision neither confers any right nor imposes any requirement on any person, and the other provisions of this Ordinance which relate (whether directly or indirectly) to that provision shall be construed accordingly.

Section 52 Domestic purposes

Personal data held by an individual and –

(a) concerned only with the management of his personal, family or household affairs; or

(b) so held only for recreational purposes,

are exempt from the provisions of the data protection principles, Parts IV and V and sections 36 and 38(b).

Section 53 Employment – staff planning

Personal data which consist of information relevant to any staff planning proposal to –

(a) fill any series of positions of employment which are presently, or may become, unfilled; or

(b) cease any group of individuals' employment,

are exempt from the provisions of data protection principle 6 and section 18(1)(b).

Section 54 Employment – transitional provisions

(1) Personal data –

(a) held by a data user –

(i) immediately before the appointed day;

(ii) who is the employer of the data subject; and

(iii) relating to the employment of the subject; and

(b) provided by an individual on the implicit or explicit condition that the subject would not have access to the data,

are exempt from the provisions of data protection principle 6 and section 18(1)(b) until the expiration of 7 years immediately following the enactment of this Ordinance.

(2) Personal data –

(a) to which subsection (1)(a) applies; or

(b) held by a data user –

(i) but not so held at any time before the appointed day;

(ii) who is the employer of the data subject; and

(iii) relating to the employment of the subject,

are exempt from the provisions of data protection principle 6 and section 18(1)(b) until 1 July 1996.

Section 55 Relevant process

(1) Personal data the subject of a relevant process are exempt from the provisions of data protection principle 6 and section 18(1)(b) until the completion of that process.

(2) In this section –

"completion" (完成), in relation to a relevant process, means the making of the determination concerned referred to in paragraph (a) of the definition of "relevant process";

"relevant process" (有關程序) –

(a) subject to paragraph (b), means any process whereby personal data are considered by one or more persons for the purpose of determining, or enabling there to be determined –

(i) the suitability, eligibility or qualifications of the data subject for –

(A) employment or appointment to office;

(B) promotion in employment or office or continuance in employment or office;

(C) removal from employment or office; or

(D) the awarding of contracts, awards (including academic and professional qualifications), scholarships, honours or other benefits;

(ii) whether any contract, award (including academic and professional qualifications), scholarship, honour or benefit relating to the data subject should be continued, modified or cancelled; or

(iii) whether any disciplinary action should be taken against the data subject for a breach of the terms of his employment or appointment to office;

(b) does not include any such process where no appeal, whether under an Ordinance or otherwise, may be made against any such determination.

Section 56 Personal references

Personal data held by a data user which consist of a personal reference –

(a) given by an individual other than in the ordinary course of his occupation; and

(b) relevant to another individual's suitability or otherwise to fill any position of employment or office which is presently, or may become, unfilled,

are exempt from the provisions of data protection principle 6 and section 18(1)(b) –

(i) in any case, unless the individual referred to in paragraph (a) has informed the data user in writing that he has no objection to the reference being seen by the individual referred to in paragraph (b) (or words to the like effect); or

(ii) in the case of a reference given on or after the day on which this section comes into operation, until the individual referred to in paragraph (b) has been informed in writing that he has been accepted or rejected to fill that position or office (or words to the like effect),

whichever first occurs.

Section 57 Security, etc. in respect of Hong Kong

(1) Personal data held by or on behalf of the Government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to prejudice any of the matters referred to in this subsection.

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

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and

(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for

believing that failure to so use the data would have been likely to prejudice any of those matters.

(3) Any question whether an exemption under subsection (1) is or at any time was required in respect of any personal data may be determined by the Chief Executive or Chief Secretary for Administration; and a certificate signed by the Chief Executive or Chief Secretary for Administration certifying that the exemption is or at any time was so required shall be evidence of that fact. *(Amended L.N. 362 of 1997; 34 of 1999 s. 3)*

(4) For the purposes of subsection (2), a certificate signed by the Chief Executive or Chief Secretary for Administration certifying that personal data are or have been used for any purpose referred to in subsection (1) shall be evidence of that fact. *(Amended L.N. 362 of 1997; 34 of 1999 s. 3)*

(5) The Chief Executive or Chief Secretary for Administration may, in a certificate referred to in subsection (3) or (4), in respect of the personal data to which the certificate relates and for the reasons specified in that certificate, direct the Commissioner not to carry out an inspection or investigation and, in any such case, the Commissioner shall comply with the direction. *(Amended L.N. 362 of 1997; 34 of 1999 s. 3)*

(6) A document purporting to be a certificate referred to in subsection (3) or (4) shall be received in evidence and, in the absence of evidence to the contrary, shall be deemed to be such a certificate.

(7) In this section –

"international relations" (國際關係) includes relations with any international organization;

"security" (保安) includes the prevention or preclusion of persons (including persons detained in accordance with the provisions of the Immigration Ordinance (Cap 115)) entering and remaining in Hong Kong who do not have the right to enter and remain in Hong Kong.

Section 58 Crime, etc.

(1) Personal data held for the purposes of –

(a) the prevention or detection of crime;

(b) the apprehension, prosecution or detention of offenders;

(c) the assessment or collection of any tax or duty;

(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(e) the prevention or preclusion of significant financial loss arising from –

(i) any imprudent business practices or activities of persons; or

(ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

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

(i) to which the discharge of statutory functions by the data user relates; or

(ii) which relates to the discharge of functions to which this paragraph applies by virtue of subsection (3); or

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

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

(i) prejudice any of the matters referred to in this subsection; or

(ii) directly or indirectly identify the person who is the source of the data.

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

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and

(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

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

(3) Paragraphs (f)(ii) and (g) of subsection (1) apply to any functions of a financial regulator –

(a) for protecting members of the public against financial loss arising from –

(i) dishonesty, incompetence, malpractice or seriously improper conduct by persons –

(A) concerned in the provision of banking, insurance, investment or other financial services;

(B) concerned in the management of companies;

(BA) concerned in the administration of provident fund schemes registered under the Mandatory Provident Fund Schemes Ordinance (Cap 485); *(Added 4 of 1998 s. 14)*

(C) concerned in the management of occupational retirement schemes within the meaning of the Occupational Retirement Schemes Ordinance (Cap 426); or

(D) who are shareholders in companies; or

(ii) the conduct of discharged or undischarged bankrupts;

(b) for maintaining or promoting the general stability or effective working of any of the systems which provide any of the services referred to in paragraph (a)(i)(A); or

(c) specified for the purposes of this subsection in a notice under subsection (4).

(4) For the purposes of subsection (3), the Chief Executive may, by notice in the Gazette, specify a function of a financial regulator. (*Amended 34 of 1999 s. 3*)

(5) It is hereby declared that –

(a) subsection (3) shall not operate to prejudice the generality of the operation of paragraphs (a), (b), (c), (d) and (f)(i) of subsection (1) in relation to a financial regulator;

(b) a notice under subsection (4) is subsidiary legislation.

58A. Protected product and relevant records under Interception of Communications and Surveillance Ordinance

(1) A personal data system is exempt from the provisions of this Ordinance to the extent that it is used by a data user for the collection, holding, processing or use of personal data which are, or are contained in, protected product or relevant records.

(2) Personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of this Ordinance.

(3) In this section –

"device retrieval warrant" (器材取出手令) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (20 of 2006);

"prescribed authorization" (訂明授權) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (20 of 2006);

"protected product" (受保護成果) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (20 of 2006);

"relevant records" (有關紀錄) means documents and records relating to –

(a) any application for the issue or renewal of any prescribed authorization or device retrieval warrant under the Interception of Communications and Surveillance Ordinance (20 of 2006); or

(b) any prescribed authorization or device retrieval warrant issued or renewed under that Ordinance (including anything done pursuant to or in relation to such prescribed authorization or device retrieval warrant).

Section 59 Health

Personal data relating to the physical or mental health of the data subject are exempt from the provisions of either or both of –

(a) data protection principle 6 and section 18(1)(b);

(b) data protection principle 3,

in any case in which the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of –

(i) the data subject; or

(ii) any other individual.

Section 60 Legal professional privilege

Personal data are exempt from the provisions of data protection principle 6 and section 18(1)(b) if the data consist of information in respect of which a claim to legal professional privilege could be maintained in law.

Section 61 News

(1) Personal data held by a data user –

(a) whose business, or part of whose business, consists of a news activity; and

(b) solely for the purpose of that activity (or any directly related activity),

are exempt from the provisions of –

(i) data protection principle 6 and sections 18(1)(b) and 38(i) unless and until the data are published or broadcast (wherever and by whatever means);

(ii) sections 36 and 38(b).

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

(a) the use of the data consists of disclosing the data to a data user referred to in subsection (1); and

(b) such disclosure is made by a person who has reasonable grounds to believe (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not they are published or broadcast) is in the public interest.

(3) In this section –

"news activity" (新聞活動) means any journalistic activity and includes-

(a) the –

(i) gathering of news;

(ii) preparation or compiling of articles or programmes concerning news; or

(iii) observations on news or current affairs,

for the purpose of dissemination to the public; or

(b) the dissemination to the public of –

(i) any article or programme of or concerning news; or

(ii) observations on news or current affairs.

Section 62 Statistics and research

Personal data are exempt from the provisions of data protection principle 3 where –

(a) the data are to be used for preparing statistics or carrying out research;

(b) the data are not to be used for any other purpose; and

(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them.

Section 63 Exemption from section 18(1)(a)

Where a data access request relates to personal data which are or, if the data existed, would be exempt from section 18(1)(b) by virtue of section 57 or 58, then the data are also exempt from section 18(1)(a) if the interest protected by that exemption would be likely to be prejudiced by the disclosure of the existence or non-existence of those data.

63A. Human embryos, etc.

(1) Personal data which consist of information showing that an identifiable individual was, or may have been, born in consequence of a reproductive technology procedure within the meaning of the Human Reproductive Technology Ordinance (47 of 2000) are exempt from the provisions of data protection principle 6 and section 18(1)(b) except so far as their disclosure under those provisions is made in accordance with section 33 of that Ordinance.

(2) Where a data access request relates to personal data which are or, if the data existed, would be exempt from section 18(1)(b) by virtue of subsection (1), then the data are also exempt from section 18(1)(a) if the interest protected by that exemption would be likely to be prejudiced by the disclosure of the existence or non-existence of the data.

Index

(All references are to paragraph number)

Table of Administrative Appeals Board Decisions and Court Cases