Foreword

The idea of a right to privacy, which arose in reaction to the rapid rise of newspapers, instant photography and the "paparazzi" of the 19th century, has evolved into a constitutional right in much of the developed world. It is enshrined in Hong Kong through Articles 28, 29, 30 and 39 of the Basic Law. Hong Kong stands proud as the first jurisdiction in Asia to enact legislation to safeguard personal data in the form of the Personal Data (Privacy) Ordinance, Cap 486 ("the Ordinance") which came into force in 1996. At its centre are the six Data Protection Principles based on the 1980 OECD Guidelines.[1] The office of the Privacy Commissioner for Personal Data was created under this legislation to provide oversight and ensure compliance. The *Octopus* scandal in mid-2010 eventually led to substantial changes being made to the Ordinance that were enacted in 2012 and 2013, the main amendments being the Direct Marketing provisions and the provision of legal assistance and representation to aggrieved persons. In this digital age, the Ordinance is proving to be the main safeguard of our privacy rights.

The Data Protection Principles seek to create broad common principles based on fairness that apply to the public and private sectors. The passage of twenty years since the enactment of the Ordinance has given rise to a substantial body of case law and administrative decisions on these principles and the other provisions of the Ordinance. The new amendments have already been the subject of judicial scrutiny.[2] This publication, which replaces its predecessor,[3] has the dual aim of

1. Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which contain a statement of Fair Information Practices.
2. Including my decision in *Chan Yim Wah Wallace v. New World First Ferry Services Ltd.* [2015] 3 HKC 382; HCPI 820/2013.
3. *Data Protection Principles in the Personal Data (Privacy) Ordinance — from the Privacy Commissioner's Perspective*, 2nd Ed., 2010

becoming a practitioner's guide on the important subject of personal data privacy, containing, as it does, a detailed exposition of the principles and provisions in the Ordinance and a comprehensive source of reference materials, and of enabling the Privacy Commissioner to discharge his major duty to promote awareness and understanding of the Ordinance.

I am sure it will be well received by the legal as well as the wider community of Hong Kong for the practical guidance it provides on good data protection practices.

Mohan BHARWANEY
Judge In Charge of the Personal Injury List of the High Court
Panel Judge under the Interception of
Communications and Surveillance Ordinance, Cap 589
July 2016

Preface

In 1996, Hong Kong enforced the Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong ("the Ordinance") and became the first jurisdiction in Asia operating with a dedicated piece of legislation on personal data privacy protection. The Privacy Commissioner for Personal Data ("the PCPD") was created in the same year, being the statutory body independent of the Government to oversee the compliance of the Ordinance.

The publication of this book coincides with the twentieth anniversary of the founding of the regulatory framework of personal data privacy in Hong Kong, reflecting on the changes which its two decades of life and growth have seen.

The origin of the law is attributable to the 1995 EU Directive[1] which aimed to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data without restricting or prohibiting the free flow of personal data.

PDP (Personal data privacy) was an acronym of which few had any understanding at that time. The first decade of the operation, amid the Information Age, was one of slow growth, until 2009 when there was a marked increase in the transfer and sale of customers' personal data by enterprises for direct marketing purposes.

1. Directive 95/46/EC of the European Parliament and of the Council of 25 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive requires European Community member states to implement national legislation that meets the minimum standards of data protection by 1998 and prohibits member states from transferring personal data to countries that do not have in place adequate protection of personal data. See http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

In 2012, the Ordinance was substantially amended as a result of a comprehensive review of the regulatory regime on direct marketing and the impact of information and communications technology on privacy protection.

As revealed in the findings of a survey[2] undertaken in 2014, personal data privacy has become a popular issue on both social agendas and those of senior management. An in-depth understanding of the Ordinance is considered an asset by individuals, organisations and practitioners alike.

It is not surprising that there are not many judicial decisions on the law as twenty years is not a lengthy period for the development of a new area of law. There are however hundreds of decisions made by the Administrative Appeals Board which is a quasi-judicial body established by statute to determine appeals lodged against the decisions made by the Commissioner in relation to complaints. Many of these quasi-judicial decisions are also published by the PCPD to ensure transparency of the reasoning and application of the law. The PCPD has the benefit of twenty years of experience as the regulator, receiving in the region of 20,000 enquiries and determining about 2,000 complaints on a yearly basis. With the start of the third decade of the operation of the PCPD and this Age of Artificial Intelligence, this book is offered as a practical guide on compliance to all stakeholders, as well as those who are interested in the personal data privacy landscape in Hong Kong.

My learned predecessors published the first and second editions of a handbook entitled Data Protection Principles in the *Personal Data (Privacy) Ordinance — from the Privacy Commissioner's perspective* in 2006 and 2010 respectively. Expanding on the commendable initiative of my predecessors, I attempt to roll out an all-in-one guide on personal data privacy law in Hong Kong, which also offers updates on the 2012 legislative amendments as well as other selected texts, cases and materials up to February 2016. Case notes of significant court judgments and Administrative Appeals Board decisions, as well as the three Codes of Practice issued by the PCPD are annexed.

This book is organised and written with a view to explaining the conceptual, legal and practical frameworks of the personal data privacy protection in Hong

2. "Baseline Survey of Public Attitudes on Privacy and Data Protection 2014" conducted by the Social Sciences Research Centre of The University of Hong Kong.

Kong, in the hope that readers, individuals or organisations; professionals or otherwise, will find it easy and user-friendly to delve into the most relevant statutory provisions for their need or interest in the topics.

I cannot thank enough all of the contributors who helped to make the publication of this book a reality, but special thanks must go to the Honourable Mr. Justice BHARWANEY for his Lordship's support in writing the most inspirational foreword to this book, Professor Guobin ZHU for being the co-editor with me, and the editorial team in my office. I would also like to record my appreciation to City University of Hong Kong Press for its dedicated efforts in providing valued assistance and publishing this book.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
July 2016

Preface

Over 125 years ago, Samuel Warren and Louis Brandeis first published "The Right to Privacy" in the *Harvard Law Review* (4 Harvard L.R. 193, Dec. 15, 1890), in which they articulated that right primarily as a "right to be let alone". This article, widely regarded as the first publication in the United States (and indeed the world) to advocate a right to privacy, opened a new page in the history of citizens' rights protection, and its influence, together with the concept of privacy, quickly travelled far beyond the American borders.

Although there is no uniform definition of the notion of privacy, it remains commonly understood as the "right to be let alone". Privacy certainly has a wider coverage in comparison to personal data privacy, the theme of the present guide. The Law Reform Commission of Australia, cited by many as an authority, has identified four categories of privacy interests requiring legal protection, namely: (i) the interest in controlling entry to a personal place (territorial privacy); (ii) the interest in freedom from interference with one's person and personal space (privacy of the person); (iii) the interest of the person in controlling the information held by others about him (information privacy); and (iv) the interest in freedom from interception of one's communications (communications and surveillance privacy).[1] According to this categorisation, personal data privacy falls under information privacy.

The right to privacy has been gradually established as one of the fundamental rights of the citizen and is widely recognised as such by international and regional human rights bodies as well as in the domestic legislation of many nations.

1. See Law Reform Commission of Australia, Privacy (Report No 22, 1983), vol. 1, para 46. See also S I Benn, "The Protection and Limitation of Privacy" (1978) 52 ALJ 601 and 686. Also quoted in Report on Civil Liability for Invasion of Privacy, prepared by the Law Reform Commission of Hong Kong, December 2004, available at: http://www.hkreform.gov.hk/en/publications/rprivacy.htm.

Article 17 of the International Covenant on Civil and Political Rights[2] which directly derives from Article 12 of the Universal Declaration of Human Rights (1948), provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Article 8 (1) "Right to respect for private and family life" of the European Convention on Human Rights (1950) also guarantees that "Everyone has the right to respect for his private and family life, his home and his correspondence".

In Hong Kong, the right to privacy as stipulated in the ICCPR was incorporated into law before the handover by way of the Hong Kong Bill of Rights Ordinance (Cap 383, 1991). Actually, Article 14 in this document, stipulating the protection of privacy, family, home, correspondence, honour and reputation, is simply a replica of the above quoted Article 17 of the ICCPR. Since the handover of Hong Kong, the right to privacy has acquired a constitutional status by virtue of Article 39 of the Basic Law of the Hong Kong and this has been compounded by the subsequent case law as well. Suffice to say that a constitutional framework of privacy law is already in place in Hong Kong.

Personal records have been with us for as long as the written word has, but computerisation of them has become widespread only since the second half of the twentieth century. This development has revolutionised personal record-keeping, because of the ease of storing, retrieving, combining and transferring data.[3] On the one hand, technology has significantly enhanced the quality of human life, but on the other public concern has arisen about the privacy implications of the resulting large-scale dissemination of personal data. This situation has called for increased lawmaking on information privacy.

2. ICCPR, 1966

3. See Reform of the Law relating to Information Privacy, prepared by the Privacy sub-committee of the Law Reform Commission, 1993, available at: http://www.hkreform.gov.hk/en/publications/infoprivacy.htm.

Hong Kong has taken the lead in the field of data protection. In 1995, the Personal Data (Privacy) Ordinance (Cap 486) was adopted to implement information privacy protection. The introduction of this law has imposed security safeguards on the keeping of personal data by a "data user" and granted the individual (as "data subject") the right to obtain copies of, and correct, personal data which relates to him. Most significantly for Hong Kong, the Office of the Privacy Commissioner for Personal Data, an independent statutory body, was set up to oversee the enforcement of the Ordinance in 1996.

Since the enactment of the law and the establishment of the Office of the Privacy Commissioner for Personal Data, Hong Kong has made great achievements in the protection of the right to privacy in general, and of personal data (privacy) in particular. The Hong Kong experience deserves praise along with wider dissemination and recognition.

From a law professor's perspective, the primary purpose of printing this book, *Personal Data (Privacy) Law in Hong Kong: A Practical Guide on Compliance*, is three-fold: firstly, to provide an easy reference to legal professionals, governmental officials, and corporate staff, who are the major data users; secondly, to provide the general public with quick and direct access to the personal data (privacy) law of Hong Kong; and thirdly, to disseminate Hong Kong's experience to a wider international audience through international publication distribution channels.

City University of Hong Kong Press is proud to be part of this significant enterprise. Personally, I am honored to be invited to co-edit this important work. For this, I am particularly grateful to Mr. Stephen Kai-yi WONG, the Privacy Commissioner for Personal Data, for his kind and friendly invitation, and also to his dedicated colleagues whose professionalism and efficiency has greatly impressed me. Last but not least, I wish to record my sincere thanks to my colleagues from the Press and in particular, to Edmund CHAN and Joanna PIERCE. I cherish this experience of collaboration between the two institutions very much.

Guobin ZHU, PhD
Professor of Law
Director of City University of Hong Kong Press
July 2016

Chapter 4

The Meaning of "Data User"

The main questions:

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

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, readers should read paragraphs 1.7 to 1.11 in Chapter 1 — Introduction, which contain important general information on using this Book.

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 under 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" within the definition under section 2(1) as a person who ". . . controls the collection . . . of the data".

4.3 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 lost in transit.

4.4 Mere physical possession of a newspaper or magazine does not render the reader a data user in relation to the personal data of individuals mentioned in the newspaper or magazine. However, the situation 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, subsequent publishing of a dossier about that person. It might then be argued that the reader became 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 the same conclusion as was reached at the subsequent *Eastweek* case. In *AAB No. 4/1997*, a hospital employee lodged a complaint about an incident in which three hospitals had permitted an

open letter written by an employee, which contained the personal data of the complainant, to be posted on their noticeboards. On appeal, the AAB upheld the Commissioner's decision not to investigate the case further. The AAB further 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 More Recent AAB Cases

4.7 In the case of *AAB No. 55/2006*, an individual, on behalf of an organisation, 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 then asked the company for copies of those two letters together with the covering letter from the regulatory body, but the company refused to comply. 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 forty days of his request. The Commissioner found that:

- the company had received the two letters from the individual on behalf of the organisation for the purpose of dealing with the complaint made to the regulatory body;
- the correspondence between the company and the regulatory body was about the complaint and did not concern the individual personally; and
- there was no collection of personal data about the complainant by the company and therefore the Ordinance did not apply.

Based on the above findings, the Commissioner considered that 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 the school had 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 *AAB No.8/2005* a student filed a complaint against his school for disclosing the examination results of an academic programme to his classmate before they were due for release. His suspicion was fueled by the fact that he had received an email from his classmate notifying all persons enrolled in the academic programme (of which his name was included in the list of recipients) of the arrangements for making a trip to the mainland to attend the graduation ceremony. The school denied that it had disclosed the examination results as alleged, and maintained that there was no evidence to show that the school was the data user in respect of the student's personal data in the email sent by his classmate. The AAB upheld the decision of the Commissioner that the school was not the data user.

4.10 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 in such circumstances the data user retained

control over the personal data; the disclosure of the relevant information under compulsion of law did not and could not vitiate their control.

Section 2(12)

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

> 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, the data for any of his own purposes.

4.12 The meaning of data being held, processed or used "solely on behalf of another person" and not for one's "own purposes" is of particular relevance.

4.13 For example, a janitor was engaged for the service of regularly disposing of documents that might contain personal data. Unless it can be shown that he collected the personal data that might be found in the documents for his own purposes, generally he is not considered, merely by collecting documents that might contain personal data for the purpose of disposal, to come within the definition of a data user. Another example is found in the case of the warehouse operators providing storage cubicles for use by their customers. Chattels and documents may be stored but the operators generally have no intention to collect the personal data that is found in these documents.

4.14 In *AAB No.12/2013*, a court clerk collected the personal data of a complainant before taking notes in a magistrate's court room. Since the purpose of collection was for the management of the court but not for the court clerk's own purpose, the AAB took the view that the court clerk was not the data user.[32]

32. In *AAB No.232/2013*, it was ruled that a rock climbing club, instead of the trainer retained by the club to provide training and sign the certificate of completion of training, was the data user in question.

4.15 Nowadays, the use of a third party contractor, such as a cloud service provider to store electronic data on behalf of individuals and companies has become increasingly popular. If the cloud service provider simply provides an electronic storage medium but does not have any intention to collect the personal data which may be transmitted to it for storage, it is to that extent not a data user as excluded under section 2(12).

4.16 By the same token, a service company providing secretarial services to a number of shelf companies/individuals using its premises as a registered office is not a data user when its staff collects incoming mail addressed to named individuals. This is because the service company does not have its own purpose to serve in collecting the personal data contained in the mail.

4.17 The requirements of the Ordinance do not apply to a person who is not a data user by operation of section 2(12). However, an organisation engaging the services provided by such person as an agent may be liable as principal under section 65(2) of the Ordinance in respect of the personal data that was entrusted to the agent for handling.

Meaning of "Person" in the Context of Data User

4.18 Although one would expect that the Ordinance primarily seeks to address 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 under the Ordinance.

4.19 Another point to note in relation to the interpretation of "data user" is the meaning of the word "person" and whether it extends to cover the Government as well. In this connection, reference could be made to the interpretation of the word "person" as defined in section 3 of the Interpretation and General Clauses Ordinance (Cap 1):

> "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.

4.20 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;

. . .

(ca) 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.

4.21 The Government as a whole is in possession of a substantial amount of personal data in relation to the residents of Hong Kong. Such data has been collected and is retained by various government bureaux and departments, according to their respective functions, such as law enforcement, revenue, social welfare, medical services etc.

4.22 In light of the wide definitions of the terms "data user", "person" and "public body", such terms may be interpreted 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 residents which involve the collection and use of personal data, the collective interpretation would effectively empower the Government to collect, virtually without limitation as to the scope of the personal data, and the exchange of such data among its various bureaux and departments. This would give rise to an anomalous result contrary to one of the principal tenets of the Ordinance, namely, to protect the personal data privacy of individuals by reference to the purpose of collection of the data and its intended use by the relevant data user in relation to that purpose.

4.23 Hence, so far as the relationship between the Government and residents 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.[33] Accordingly, under DPP1(1), a government department is not allowed to collect personal data in excess of that required for its own function and activity (as opposed to those of other government departments). Furthermore, the transfer of data amongst bureaux or departments is subject to the relevant restrictions under DPP3. For a more comprehensive discussion of DPP1(1)(c) and DPP3, readers are referred to paragraphs 5.1 to 5.29 in Chapter 5 and Chapter 7.

4.24 To further illustrate this point, a government department may operate through different district offices or branch offices under its supervision and control. In the event of any breach of a requirement under the Ordinance by a staff of one of these offices, the Commissioner will look to the government department in question as the data user and hence the target of investigation. This is because the government department concerned is viewed as a single person who is capable of devising, reviewing, supervising and controlling the personal data policies and practices to be followed by all the district offices or branch offices operated under it. The same applies, for example, to the case of the Hospital Authority which manages and supervises a number of public hospitals in Hong Kong.

Joint Data Users

4.25 The definition of the term "data user" extends to situations 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 requirements under the Ordinance.

33. 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.

4.26 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 it out to a tenant for rental profits. They may have collected the tenant's personal data in circumstances where 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.

4.27 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) is transferred to another company, 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. When 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.[34]

4.28 When a potential customer's personal data is first used for marketing purposes, the data user is obliged under section 35F(1) of the Ordinance to inform him of his right to opt-out of such marketing activities and to comply with the opt-out request pursuant to section 35G(3). If the data user continues to use personal data about the individual for direct marketing after receiving his opt-out request, he may be considered as having committed an offence under section 35G(4).[35] In order to comply with the statutory requirements under section 35G(3), a 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

34. 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.

35. Under section 35G(4), a data user who contravenes the requirements is liable to a maximum fine of $500,000 and to imprisonment for three years.

company have to maintain the opt-out list and must not make any further marketing approaches to those customers who have opted out[36] from the direct marketing activities in question. In *AAB No. 20/2009*, the crux of the complaint was the repeated receipt by the complainant of direct marketing materials sent by companies A and B which were joint promotion partners. The Commissioner took the view that upon the receipt of an opt-out request from the complainant by company A, it should have informed company B about it so that the latter would cease using the complainant's personal data for direct marketing purposes.

What is the Relationship between a Data User and a Data Processor?

4.29 The Amendment Ordinance made changes to DPP2 and DPP4 by introducing the term "data processor" which is defined as follows:

> "Data processor" means a person who –
>
> (a) processes personal data on behalf of another person; and
>
> (b) does not process the data for any of the person's own purposes.

4.30 It is common business practice these days for a data user to outsource the processing of personal data to a contractor, for example, to a document shredding company for carrying out safe destruction of confidential documents, and to an IT contractor to manage and maintain the staff attendance and payroll IT systems.

4.31 These data processors are not data users as they do not control the collection, holding and processing of the personal data and therefore are not subject to the regulatory remit of the Ordinance. From the Commissioner's regulatory experience, quite a number of data breaches were committed by

36. See *New Guidance on Direct Marketing*, available on the Website.

the contractors or agents appointed by the data users to process personal data on their behalf.[37]

4.32 To address this issue, the Amendment Ordinance sought to strengthen the protection of personal data by imposing a duty on data users who engage these data processors to use contractual or other means to ensure that the personal data that was transferred to the data processors was not kept longer than is necessary and to take reasonably practical steps for the security of the data. For details on how these new obligations are to be observed by the data user, readers may refer to Chapters 6 (on DPP2) and 8 (on DPP4).

Section 4

4.33 If a person falls within the definition of "data user", section 4 of the Ordinance applies to govern his act and conduct:

> 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.

4.34 The six data protection principles set out in Schedule 1 of the Ordinance are of vital importance to guide the act or practice in handling personal data. For this reason, they are the topics for discussion in the subsequent Chapters.[38] Section 64A(1) which makes contravention of a requirement under the Ordinance an offence, specifically excludes data protection principles. Although non-compliance with any of the data protection principles does not per se attract criminal sanction, when coupled with other provisions in the Ordinance that are relevant to the application of the

37. For instance, the leakage of complainants' sensitive personal data, which was the subject matter of the Commissioner's Investigation Report No. R06-2599, was caused by the uploading of the complainants' personal data (including names, addresses and HKID numbers) by the IT contractor onto a location of the server to which members of the public had access.

38. A checklist for data users in ensuring compliance with the requirements under the Ordinance is found in Appendix V of this Book. The remedies that a data subject may resort to if his personal data privacy right is infringed are summarized in Appendix VI.

Chapter 10

Data Protection Principle 6(a) to (d) and the Data Access Provisions in Part 5

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 should a data user do if it does not hold the personal data requested?
- What should a data user do if the requested data comprises personal data of other individual(s)?
- What charge may a data user levy for complying 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 5 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, readers should read paragraphs 1.7 to 1.11 in Chapter 1 — Introduction, which contain important general information on using this Book.

The Basis of a Data Access Request

10.1 The right to make a data access request is an important right vested in the data subjects under paragraphs (a) to (d) of Data Protection Principle 6 to ascertain whether a data user holds his personal data and, to obtain a copy of the data so held by the data user:

> 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 5 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. Failure to comply with a data access request in accordance with the requirements under the Ordinance without reasonable excuse may constitute an offence and render the offender liable on conviction to a fine.[200] In addition to the grounds provided under Part 5 which prescribe when a data user shall or may refuse to comply with a data access request, there are exemption provisions in Part 8 of the Ordinance which, when properly invoked, may exempt the data user from complying with a data access request.

200. A level three fine, see section 64A(1).

10.3 There are stringent provisions under Part 5 of the Ordinance on the manner and the procedure of complying with a data access request that a data user has to observe. Thus, when a data access request is received, the data user shall handle it according to the relevant provisions in complying with or refusing to comply with, the data access request.

10.4 Salient points on the making of a data access request by a data subject or his relevant person,[201] and on the handling and responding to such a request by the data user are set out below. *The Guidance Note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users* issued by the Commissioner provides general guidance on compliance with a data access request.[202]

What Constitutes a Data Access Request?

10.5 The first question to consider is what constitutes a data access request under the Ordinance. In this connection, "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 Section 18(1) is so drafted that neither the word "and" nor "or" appear between paragraphs (a) and (b). Taking the literal 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

201. As defined under sections 2(1) and 17A of the Ordinance.

202. Available on the Website.

adopts the view that the two paragraphs are not conjunctive and should be construed to cover two separate categories of request the choice between which a requestor, in making a data access request, is entitled to make. 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. Section 18(2) also provides that if a data access request is made by the same requestor under both paragraphs (a) and (b), they shall be treated as a single request.

10.8 When a data access request is made under section 18(1)(a), section 18(3) of the Ordinance 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). In addition to simply responding to the request made under section 18(1)(a), the data user can also choose to supply a copy of the personal data to the requestor pursuant to section 18(1)(b) of the Ordinance.

10.9 Prior to the Amendment Ordinance, it was unclear whether or not a data user could ignore a request made only under section 18(1)(b) if the data user did not hold the personal data requested. The Amendment Ordinance clarified this situation by amending section 19(1) to expressly require data users to inform a data requestor if it does not hold any of the requested data within forty days of receiving such a request.[203]

10.10 It should also be noted that reading paragraph (a) of section 18(1) alone, it is not clear whether "personal data" as used therein means that a requestor can ask for confirmation on whether or not a data user holds any of his personal data in general, or whether the requestor must identify a specific item of personal data in relation to which he is seeking confirmation. The Commissioner takes the view that the meaning of that term includes both. In other words, when making a data access request under paragraph (a),

203. The issue of whether a data user, in compliance with a data access request made under section 18(1)(a) of the Ordinance, may inform the requestor verbally that the data user does not hold the requested data, formed the subject matter of *AAB No. 10/2010*. The AAB referred the said question of law to the Court of Appeal for determination by way of case stated. The Court of Appeal, in *CACV 229/2011*, answered the question in the affirmative having considered the original provision of section 19(1) prior to the Amendment Ordinance, the purpose of the Ordinance and public policy, as well as the proposed amendments to section 19(1). See also paragraphs 10.29 to 10.31 for discussion on section 19(1).

the requestor may choose to ask a data user the general question of "do you hold any of my personal data in the personnel file?" or, alternatively, the more specific question of "do you hold my appraisal report dated xxx?" (the appraisal report being a specific document that contains the requestor's personal data).

10.11 It should also be noted that no reference is made in paragraph (a) or (b) of section 18(1) to 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 take 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 paragraph 10.37 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).

10.12 Similarly, the Commissioner has received complaints about failures to comply with data access requests that are worded as follows: "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 the representation of information in a document. Hence, unless the reason or explanation sought already exists in a document (which in most cases means in writing), the Commissioner takes the view that the data user has no obligation, upon receiving such a request, to document 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?

10.13 Section 18(1) provides that a data access request may be made by "an individual, or a relevant person on behalf of an individual". "Relevant person" is defined in section 2(1) and its meaning is further expanded in section 17A of the Ordinance for the purpose of making a data access or correction request.

10.14 Section 2(1) provides 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) where the individual is mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136) –
>
> (i) a person appointed under section 44A, 59O or 59Q of that Ordinance to be the guardian of that individual; or
>
> (ii) if the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by, the Director of Social Welfare or any other person under section 44B(2A) or (2B) or 59T(1) or (2) of that Ordinance, the Director of Social Welfare or that other person;

10.15 Section 17A provides as follows:

> Without limiting the definition of relevant person in section 2(1), in this Part –
>
> "relevant person", in relation to an individual, also includes a person authorised in writing by the individual to make, on behalf of the individual –
>
> (a) a data access request; or
>
> (b) a data correction request.

10.16 When a data user receives a data access request made by a "relevant person", it should ascertain the capacity of the requestor in order to satisfy itself that the requestor is a person specified under sections 2(1) or 17A of the Ordinance. The data user may request information as to the requestor's capacity (such as written authorisation signed by the data subject), evidence showing the requestor's parental relationship with the data subject who is a minor, or evidence showing that the requestor is the lawful guardian or

person appointed by the Court to manage the affairs of the data subject who is incapable of managing his affairs. If a data user cannot reasonably establish the relationship between the requestor and the data subject, the data user must refuse to comply with the data access request.

10.17 Section 18(1) provides that a relevant person may make a data access request on behalf of a data subject. The provisions of the Ordinance, however, give no indication, 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 following two situations: 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 own purposes, so as to enable himself 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.

10.18 For example, a parent who has been denied physical access to his child by the Court or the custodian parent may try to lodge a data access request under the Ordinance with a social welfare organisation or the child's school, seeking to obtain the personal data of the child, on the basis that he is the "relevant person" of that child. However, from the subject matter raised in the request (e.g. a request for information on the whereabouts of the child which is obviously known to the child in question) it may be argued that the parent requesting the data is making the data access request for his own benefit, rather than in the child's interest. In situations like these, the Commissioner will be inclined to take the view that the request is not 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?

10.19 The Ordinance does not prescribe any particular form or mode by which a data access request may be made. However, under sections 20(3)(a) and (e), if a data access request is not made "in writing in the Chinese or

English language" or the request is not made in the form prescribed by the Commissioner, these may 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 10.78 to 10.83 below.

10.20 Cases handled by the Commissioner suggested that the absence of any prescribed form for a data access request often caused confusion. In particular, a data user receiving such a request could easily be unaware of it being a data access request, hence failing its obligation to respond to it in strict compliance with the Ordinance. This has a significant impact on data users who have regular dealings with individuals. 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.

10.21 The Commissioner took the view that in 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 state or make reference 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[204] by which data access requests are to be made.

10.22 The Data Access Request Form, by design, aims to make clear, both to the requestor and the data user, the following essential matters:

- the fact that a data access request is made under the Ordinance;
- the particular provision(s) under which such request is 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 to frame his request as specifically as possible);

204. Available on the Website.

- how to handle (including the time for compliance with) such a request, and the possible consequences of failure to do so.

10.23 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 grounds under section 20(3)(e) to refuse compliance with it. Even if a request is not made by using the Data Access Request Form prescribed by the Commissioner, data users are still encouraged to comply with such a request if it substantially contains the details required, as the use of the prescribed form is merely a technical requirement.

10.24 In *AAB No. 20/2014*, the AAB took the view that a letter written by the complainant to a bank, requesting the bank to either retain certain CCTV footage until the complainant agrees to destroy the same or provide him with a copy of the CCTV footage, may not amount to a data access request made pursuant to section 18(1) of the Ordinance. The AAB had taken into account that the "request" was not made in the specified form and the letter itself did not contain the substance to qualify as a valid data access request.

10.25 The requestor in making a data access request must provide true and accurate information to the data user. A requestor who does not do so may commit an offence under section 18(5) and (6) of the Ordinance:

> (5) A person commits an offence if the person, in a data access request, supplies any information which is false or misleading in a material particular for the purposes of having the data user –
>
> (a) inform the person whether the data user holds any personal data which is the subject of the request; and
>
> (b) if applicable, supply a copy of the data.
>
> (6) A person who commits an offence under subsection (5) is liable on conviction to a fine at level 3 and to imprisonment for six months.

10.26 Such an offence is intended to deter persons from conducting fishing expeditions for personal data through providing false or misleading information to the data user when making a data access request.

How and When to Comply with a Data Access Request?

10.27 A data user, upon receiving a data access request, must comply with such a request (unless there are grounds which allow or require the data user to refuse to comply with it, under section 20 or Part 8 of the Ordinance). The next question is how and when to comply with such a request.

Statutory Period

10.28 First, it should be noted that a data user must respond within forty days after receiving the request.

10.29 Section 19(1)(a) and (b) provides as follows:

> (1) Subject to subsection (2) and sections 20 and 28(5), a data user must comply with a data access request within 40 days after receiving the request by –
>
> (a) if the data user holds any personal data which is the subject of the request –
>
> (i) informing the requestor in writing that the data user holds the data; and
>
> (ii) supplying a copy of the data; or
>
> (b) if the data user does not hold any personal data which is the subject of the request, informing the requestor in writing that the data user does not hold the data.

10.30 What should a data user do if it does not hold the personal data requested? Pursuant to section 19(1)(b) (as introduced by the Amendment Ordinance) a data user must inform the data requestor in writing within the statutory period of forty days after receiving the data access request that it does not hold the personal data.[205] It is also advisable for the data user to inform the data requestor of the reason why it does not hold the personal data, for example, that the requested data has been destroyed after the purpose

205. This obligation is made subject to section 19(1A). For detailed discussion, please refer to paragraphs 10.49 to 10.52.

for which the data was to be used has been served. This may ease the data requestor's suspicion that the erasure is made in bad faith. For instance, examination papers may be destroyed by an education institution regularly in accordance with its data retention policy and after publication of the examination results.

10.31 However, if evidence suggests that a data user has deliberately destroyed the requested data after receiving the data access request with a view to avoiding its statutory obligation to supply a copy of data to the requestor, this may amount to non-compliance with the data access request.

10.32 Furthermore, it should be noted that 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, section 19(3)(a) provides 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; . . .

10.33 It can be seen that the relevant point in time by reference to which personal data is 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 may 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.

10.34 The operation of section 19(3)(a) may pose questions 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 8 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 existed after receipt but before compliance with the data access request? The 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, is not restricted insofar as it is properly invoked with reasons stated and the requestor is notified in accordance with section 21.

10.35 Sometimes, a data access request may be framed in such a way that it contains a subjective element (e.g. "all data that affects my reputation"). In complaints arising from this type of requests, 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 judgement of the data user in selecting the relevant data that needs to be provided.

Broad and Generic Requests for Personal Data

10.36 Often, a data subject may, in the data access request, ask for copies of "all personal data" relating to him held by the data user. This may, however, create serious practical difficulty for the data user, especially where there have been extensive dealings between the parties, during which a large amount of personal data may have been collected and/or created, e.g. where the data subject is or used to be employed by the data user for many years. In these circumstances, the data user may reasonably ask the requestor to provide further information in order to assist the data user to locate the requested personal data. Failure to provide such information may entitle the data user to refuse to comply with the data access request.[206]

However, a data user cannot refuse to comply with a request simply by relying on the excuse that the request is made in generic or broad terms. If it is still reasonably practicable for the data user to extract "all personal data" requested without requiring any further information from the requestor, the data user should comply with the data access request.

206. Section 20(3)(b) of the Ordinance.

10.37 In the case of *AAB No. 24/2001*, the complainant asked for "all of [her] personal data" held by the appellant, including but not limited to certain named categories. Despite repeated requests for clarification from the appellant, the complainant refused to narrow the scope of her data access requests in any way. The appellant, having omitted to provide the complainant with some of her personal data, was found by the Commissioner to have failed to comply fully with the data access request.

10.38 Upon appeal by the appellant against the enforcement notice issued by the Commissioner directing it to conduct a "thorough search" for the requested data, the AAB found in favour of the appellant based on 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; . . .

10.39 According to the AAB's decision, it appears that section 20(3)(b), in addition to constituting grounds of refusal to comply with a data access request, may also operate to limit the scope of data which the data user is obliged to provide in compliance with the request even where no such formal refusal is made pursuant to section 21. In particular, 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 falls under the description of the data requested).[207]

207. 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.