

**PERSONAL DATA (PRIVACY) LAW  
IN  
HONG KONG**

**A Practical Guide on Compliance**

**Third Edition**

**Edited by**

**Ada CHUNG Lai-ling**

**Guobin ZHU**



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



香港城市大學出版社  
City University of Hong Kong Press

# Table of Contents

Foreword	xxiii
Preface   Ada CHUNG Lai-ling	xxv
Preface   Guobin ZHU	xxix
Acknowledgments	xxxiii
Chapter 1 Introduction	1
Chapter 2 The Meaning of "Personal Data"	9
Chapter 3 The Meaning of "Collect"	33
Chapter 4 The Meaning of "Data User"	47
Chapter 5 Data Protection Principle 1	61
Chapter 6 Data Protection Principle 2	107
Chapter 7 Data Protection Principle 3	127
Chapter 8 Data Protection Principle 4	161
Chapter 9 Data Protection Principle 5	195
Chapter 10 Data Protection Principle 6(a) to (d) and the Data Access Provisions in Part 5	203
Chapter 11 Data Protection Principle 6(e) to (g) and the Data Correction Provisions in Part 5	239
Chapter 12 Exemption Provisions in Part 8	253
Chapter 13 The Commissioner's Statutory Duties in Investigations	301

©2024 City University of Hong Kong

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, Internet or otherwise, without the prior written permission of the City University of Hong Kong Press.

ISBN: 978-962-937-688-8

Published by

City University of Hong Kong Press  
Tat Chee Avenue  
Kowloon, Hong Kong  
Website: [www.cityu.edu.hk/upress](http://www.cityu.edu.hk/upress)  
E-mail: [upress@cityu.edu.hk](mailto:upress@cityu.edu.hk)

Printed in Hong Kong

Chapter 14	Data Breach Handling and Notifications	325
Chapter 15	Criminal Offences	339
Chapter 16	Doxxing	373
Chapter 17	Cross-border Transfers of Personal Data from Hong Kong	403
Chapter 18	An Overview of the Mainland's Personal Information Protection Regime	413
Appendix I	Selected Case Notes on Court Judgments	445
Appendix II	Major Differences between the PIPL, the GDPR and the PDPO	516
Appendix III	Checklist for Data Users in Ensuring Compliance with the Ordinance	525
Appendix IV	Data Subject's Rights when his Personal Data Privacy is Infringed	529
Index		533
List of Court Cases and Administrative Appeals Board Decisions		551

## Contents in Detail

### Chapter 1 Introduction

Regulatory Approach	3
Disclaimer	6
Abbreviations Used in This Book	6

### Chapter 2 The Meaning of "Personal Data"

Introduction — Meaning of the Term "Data"	10
Definition of "Personal Data"	11
Paragraph (a) — "Relating Directly or Indirectly to a Living Individual"	11
Paragraph (b) — "From which it is Practicable for the Identity of the Individual to be Directly or Indirectly Ascertained"	14
Paragraph (c) — "In a Form in which Access to or Processing of the Data is Practicable"	16
Consideration of Certain Types of Information	18
IP Addresses	18
Email Addresses	19
Biometric Data such as DNA and Fingerprint Data	20
Examination Scripts	21
Mobile Phone Numbers	21
Digital Content of Mobile Phones	22
A Person's Whereabouts	24

Is Fabricated Information Personal Data?	25
Physical Tracking and Monitoring through Electronic Devices	25
Identifiability of an Individual — Existing Issues and a Possible Way Forward	26
Metadata	26
Artificial Intelligence	27
Anonymisation and Pseudonymisation	28
Identifiability and Personal Data	29

### Chapter 3 The Meaning of “Collect”

The <i>Eastweek</i> Case	34
The Meaning of “Collect”	35
When Does the Use of CCTV for Security or Monitoring Purposes Amount to the Collection of Personal Data?	38
Information Privacy and Other Privacy Interests	41

### Chapter 4 The Meaning of “Data User”

Meaning of “Data User” with Reference to the <i>Eastweek</i> Case	48
Meaning of “Data User” with Reference to AAB Cases	49
Section 2(12)	51
Meaning of “Person” in the Context of Data User	53
Joint Data Users	55
What is the Relationship between a Data User and a Data Processor?	57
Section 4	58

### Chapter 5 Data Protection Principle 1

Overview	62
The General Requirements of DPP1	62
Collection of HKID Card Numbers and Copies of HKID Cards	64

Collection of HKID Card Numbers for Customer Loyalty Programmes	71
Collection of HKID Card Numbers by the Property Management Sector	73
Collection of HKID Card Numbers through Mobile Apps	74
Collection of Personal Data for Direct Marketing Purposes	74
Collection of Employees’ Health Data	75
Collection of Health Data during the COVID-19 Pandemic	77
Collection of the Criminal Records of Prospective Employees	78
Collection of a Person’s Whereabouts	79
DPP1(2)	80
Collection of Personal Data through Blind Recruitment Advertisements	82
Collection of Personal Data by Covert Means	83
Collection of the Activities of Individuals that Take Place inside a Private Residence by Systematic Surveillance and Using a Long-focus Lens	86
Passive Collection of the Whereabouts of Individuals	88
Employees Providing Past Medical Records and Consequential Disciplinary Action	88
Giving Misleading Information to Obtain a Credit Report from a Credit Reference Agency	89
Collection of Personal Data from the Public Domain	90
Collection of Biometric Personal Data and Consent	91
DPP1(3)	94
Application of DPP1(3)	95
Obligation Not Absolute — “All Practicable Steps”	96
Notification Requirements	98
Purposes of Data Use	99
The Classes of Persons to Whom the Data May be Transferred	101
The Right to Request Access to and Correction of the Data	103
Transparency and Explainability	104

Requirements on Notification when Collecting Personal Data for Direct Marketing Purposes	106
--	-----

## Chapter 6 Data Protection Principle 2

Overview	108
DPP2(1)	108
DPP2(2) and Section 26	113
Requirements under DPP2(3) and (4): Personal Data Transferred to a "Data Processor"	123
Data Retention Period — Existing Issues and a Possible Way Forward	124
Regulation of Data Processors — Existing Issues and a Possible Way Forward	126

## Chapter 7 Data Protection Principle 3

Overview	128
The General Requirements of DPP3	128
What Does "Use" Mean?	128
What is a "New Purpose"?	128
The Original Purpose of Collection	130
The Purposes of Collection Stated in the PICS	131
The Lawful Functions and Activities of the Data User	133
Restrictions of Use Imposed upon Data Users by Data Providers or Data Subjects	134
Transferring Personal Data between Data Users	136
Personal Data Collected from the Public Domain	137
Purposes Directly Related to the Original Purpose of Collection	143
Avoidance of Disclosing Unnecessary and Excessive Personal Data	147
Is the Sale of Personal Data a Directly Related Purpose of Use?	153
Prescribed Consent	155
Prescribed Consent Given by a Relevant Person	158

Requirements on Consent for Use when Collecting Personal Data for Direct Marketing Purposes	160
---	-----

## Chapter 8 Data Protection Principle 4

Overview	162
The General Requirements of DPP4	162
Data Breaches	170
Banking and Insurance Industries	171
Government and Public Bodies	172
Providers of Telecommunications, Internet and Credit Services	176
Legal Practitioners	180
Hospitals and Clinics	182
Mobile Application Developers	184
Travel Industry	186
Food and Beverage Industry	187
Media Industry	188
Photofinishing Industry	188
E-commerce Industry	189
Application of DPP4: Storage and Transmission of Data	190
Outsourcing the Processing of Personal Data to Data Processors	191
Regulation of "Data Processors" — Existing Issues and a Possible Way Forward	194

## Chapter 9 Data Protection Principle 5

Overview	196
The General Requirements of DPP5	196
What Should a PPS Include?	197
PPS Should be Made Generally Available	198
Other Information to be Made Available	201

Exercise of the Commissioner's Enforcement Powers under Section 50	202
--	-----

## Chapter 10 Data Protection Principle 6(a) to (d) and the Data Access Provisions in Part 5

Overview	204
The Basis of a Data Access Request	204
What Constitutes a Data Access Request?	205
Who May Make a Data Access Request?	207
How to Make a Data Access Request	209
How and When to Comply with a Data Access Request	211
Statutory Period	211
Broad and Generic Requests for Personal Data	213
Steps to be Taken on Failure to Comply with a Data Access Request within the Statutory Period	217
Language and Format when Responding to a Data Access Request	218
Data Access Request Made to the Hong Kong Police Force for Criminal Conviction Records	220
Requested Data Comprising Personal Data of Another Individual	221
Charge for Complying with a Data Access Request	223
When Must a Data User Refuse to Comply with a Data Access Request?	227
When May a Data User Refuse to Comply with a Data Access Request?	229
Steps to Take in Refusing to Comply with a Data Access Request	232
Proper Exercise of the Right to Access Personal Data	234

## Chapter 11 Data Protection Principle 6(e) to (g) and the Data Correction Provisions in Part 5

The Relationship between a Data Correction Request and a Data Access Request	240
--	-----

Who Can Make a Data Correction Request and How Should it be Made?	241
Compliance with a Data Correction Request	242
Circumstances in which a Data User Shall or May Refuse to Comply with a Data Correction Request	245
Steps to Take in Refusing to Comply with a Data Correction Request	249

## Chapter 12 Exemption Provisions in Part 8

Overview	255
Introduction	255
Exemptions in General	256
Section 51A — Performance of Judicial Functions	258
Section 52 — Domestic Purposes	259
Sections 53 and 54 — Staff Planning and Employment	261
Section 55 — Relevant Process	262
Section 56 — Personal References	263
Section 57 — Security, etc. in Respect of Hong Kong	264
Section 58 — Crime, etc.	266
Section 58A — Protected Product and Relevant Records under Interception of Communications and Surveillance Ordinance	276
Section 59 — Health	277
Section 59A — Care and Guardianship of Minors	280
Section 60 — Legal Professional Privilege	281
Section 60A — Self-incrimination	283
Section 60B — Legal Proceedings, etc.	284
Section 61 — News	289
Section 62 — Statistics and Research	294
Section 63 — Exemption from Section 18(1)(a)	295
Section 63A — Human Embryos, etc.	296
Section 63B — Due Diligence Exercise	296

Section 63C — Emergency Situations	299
Section 63D — Transfer of Records to Government Records Service	299

### Chapter 13 The Commissioner's Statutory Duties in Investigations

Introduction	302
The Commissioner's Statutory Duties of Investigation	302
Lodging a "Complaint"	304
Restrictions on Investigations Initiated by a "Complaint"	309
Discretion of the Commissioner	313
The Commissioner's Decision Whether to Carry Out an Investigation	321

### Chapter 14 Data Breach Handling and Notifications

What is a Data Breach?	326
What Should be Done to Prepare for a Data Breach?	326
How Should a Data Breach be Handled?	327
Step 1: Immediate Gathering of Essential Information	327
Step 2: Containing the Data Breach	328
Step 3: Assessing the Risk of Harm	329
Step 4: Considering Giving Data Breach Notifications	330
Step 5: Documenting the Breach	331
What is a Data Breach Notification?	331
To Whom Should the Notification be Given?	332
What Should be Included in the Data Breach Notification?	332
When Should a Data Breach Notification be Given?	333
How Should a Data Breach Notification be Given?	334
Notifications to the Data Subjects	334
Notifications to the PCPD	335
Lesson Learnt: Preventing Recurrence	335

Good Data Breach Handling Makes Good Business Sense	336
Steps Taken by the Commissioner	336
Data Breach Handling and Notifications — Existing Issues and a Possible Way Forward	338

### Chapter 15 Criminal Offences

Overview	340
Direct Marketing Offences	340
Outline of the Regulatory Regime	341
What Amounts to "Direct Marketing"?	342
What is a "Marketing Subject"?	344
What is a "Permitted Class" of Marketing Subjects / Persons / Personal Data?	345
What "Notification" is Required before Conducting Direct Marketing?	346
What is the "Consent" Required before Conducting Direct Marketing?	348
What is a "Response Channel"?	351
Withdrawal of Consent by the Data Subject (Opt-out Right)	352
Nature of the Offence in the Data User's Failure to Comply with the Data Subject's Opt-out Request	353
Records of Convictions	355
Overarching Principles	355
Modern Trend of Online Marketing	356
Offences Relating to the Commissioner's Enforcement Power	357
Overview	357
The Commissioner's Discretionary Power in Issuing an Enforcement Notice	358
Remedying the Contravention and Preventing its Recurrence	359
Relevant Timeframe	360
Penalty and Defence	361

Contravention of DPPs — Current Issues and a Possible Way Forward	362
Offences Relating to the Commissioner's Investigation Power	363
Other Offences	364
Miscellaneous Offences	364
Other Criminal Offences under the Ordinance	365
Prosecution Deadline for Summary Offences	370
Criminal Liability of Director or Officer of the Company	370
Cyber-bullying	370

## Chapter 16 Doxxing

Introduction	374
Offences for Disclosing Personal Data Obtained without Consent	376
Elements of the Offence — Section 64(1) of the Ordinance	378
Elements of the Offence — Sections 64(3A) and (3C) of the Ordinance	379
Specified Harm	380
Harassment, Molestation, Pestering, Threat or Intimidation to the Person	380
Bodily Harm or Psychological Harm to the Person	381
Harm Causing a Person Reasonably to be Concerned for the Person's Safety or Well-being	382
Damage to the Property of the Person	382
Defence	383
Onward-forwarding of Doxxing Posts	384
Criminal Investigation and Prosecution Powers	384
Power to Require Material and Assistance by Issuing a Written Notice	385
Application for a Court Warrant to Search Premises and Access Electronic Devices	386
Power to Access Electronic Devices without a Court Warrant	387

Powers to Stop, Search and Arrest	388
Prosecution Power	389
The Commissioner's Powers to Serve Cessation Notices and Apply for Injunctions	389
Circumstances under which the Commissioner May Serve Cessation Notices and the Consequences of Non-compliance	389
Content of a Cessation Notice	392
Appeal against a Cessation Notice	392
Injunction	393
<i>Secretary for Justice &amp; Commissioner of Police v. Persons     unlawfully and wilfully conducting themselves in any of     the acts prohibited under paragraph 1(A), (B) or (C)     in the indorsement of claim [2019] HKCFI 2773     (HCA 1957 of 2019)</i>	393
<i>Secretary for Justice v. Persons unlawfully and wilfully     conducting themselves in any of the acts prohibited     under paragraph 1(a) and (b) in the indorsement of     claim and the Internet Society of Hong Kong Limited [2019]     HKCFI 2809 (HCA 2007 of 2019)</i>	395
<i>Secretary for Justice v. Persons unlawfully and wilfully     conducting themselves in any of the acts prohibited     under paragraph 1(a), (b) or (c) in the indorsement of     claim [2020] HKCFI 2785 (HCA 1847 of 2020)</i>	397
Power to Apply for an Injunction	398
Implementation Guideline	398
Enforcement Actions Taken by the PCPD after the Amendment Ordinance 2021 Came into Operation	399
Overseas Experiences and Developments	401

## Chapter 17 Cross-border Transfers of Personal Data from Hong Kong

Overview	404
Regulation under the Ordinance	404

History of Section 33 of the Ordinance	404
DPPs in Schedule 1 to the Ordinance	405
Recommended Model Contractual Clauses ("RMCs")	406
Data Ethics	409
Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area	410
The Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)	410
Draft Practical Guidance of Cybersecurity Standards — Requirements for Protection of Personal Information for Cross-boundary Transfers within the Guangdong-Hong Kong-Macao Greater Bay Area	412
<b>Chapter 18 An Overview of the Mainland's Personal Information Protection Regime</b>	
Introduction	414
The Personal Information Protection Law ("PIPL")	415
Key Definitions	417
Personal Information	417
Sensitive Personal Information	417
Processing of Personal Information	417
Personal Information Processor	417
Principles for Processing Personal Information	418
Legality, Necessity and Good Faith	418
Purpose Limitation and Data Minimisation	418
Openness and Transparency	418
Accuracy, Retention and Erasure	419
Accountability and Governance	420
Legal Bases for Processing Personal Information	420
Consent	421

Obligations of Personal Information Processors	422
Security Safeguards	422
Appointment of Personal Information Protection Officers	423
Appointment of Local Representative	423
Compliance Audits	423
Personal Information Protection Impact Assessment	423
Engagement of Third Parties to Process Personal Information	424
Rights of Individuals	424
Rights of Access and Correction	425
Right of Erasure, to Restrict or Refuse Personal Information Processing	425
Right to Data Portability	425
Other Specific Requirements	426
Processing of Sensitive Personal Information	426
Breach Notifications	426
Obligations of Internet Platforms	427
Automated Decision Making	427
Cross-border Transfer of Personal Information	428
Security Assessment	429
Certification	432
Standard Contract	433
The Regulations on Facilitating and Regulating Cross-border Data Flow	434
Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area ("the GBA")	437
Enforcement and Legal Liability	438
Supervisory Authorities	438
Administrative Fines	439
Other Penalties	440
Compensation and Litigation	440
The Cybersecurity Law	441

**Appendix I Selected Case Notes on Court Judgments**

1. <i>Cathay Pacific Airways Limited v. Administrative Appeals Board &amp; Another</i> [2008] 5 HKLRD 539 (HCAL 50/2008)	447
2. <i>Chan Chuen Ping v. The Commissioner of Police</i> [2014] 1 HKLRD 142 (HCMP 2741/2013)	450
3. <i>Chan Yim Wah Wallace v. New World First Ferry Services Limited</i> (HCPI 820/2013, Date of Decision: 8 May 2015)	453
4. <i>Dr Alice Li Miu-ling v. The Hong Kong Polytechnic University</i> (DCEO 1/2004, Date of Judgment: 1 November 2012)	458
5. <i>Eastweek Publisher Limited &amp; Another v. Privacy Commissioner for Personal Data</i> [2000] 2 HKLRD 83 (CACV 331/1999)	462
6. <i>HKSAR v. Hong Kong Broadband Network Limited</i> [2018] 2 HKLRD 1049 (HCMA 624/2015, Date of Judgment: 26 January 2017) (on appeal from TWS 6311/2015)	465
7. <i>HKSAR v. Leung Chun-kit Brandon</i> (HCMA 49/2016, Date of Judgment: 2 June 2017) (on appeal from ESS 24178/2015)	472
8. <i>Junior Police Officers' Association of the Hong Kong Police Force &amp; Another v. Electoral Affairs Commission &amp; Others</i> [2020] HKCA 352 (CACV 73/2020, Date of Judgment: 21 May 2020)	480
9. <i>Lily Tse Lai Yin &amp; Others v. The Incorporated Owners of Albert House &amp; Others</i> (HCPI 828/1997, Date of Decision: 10 December 1998)	485
10. <i>M v. M</i> (FCMC 1425/1988, Date of Judgment: 10 June 1997)	487
11. <i>Ng Shek Wai v. Medical Council of Hong Kong</i> [2015] 2 HKLRD 121 (HCAL 167/2013)	490
12. <i>Oriental Press Group Ltd v. Inmediahk.net Ltd</i> [2012] 2 HKLRD 1004 (HCA 1253/2010)	494
13. <i>Secretary for Justice v. Persons unlawfully and wilfully conducting themselves in any of the acts prohibited under paragraph 1(a) and (b) in the indorsement of claim and the Internet Society of Hong Kong Limited</i> [2019] HKCFI 2809 (HCA 2007/2019)	497

14. <i>Secretary for Justice &amp; Commissioner of Police v. Persons unlawfully and wilfully conducting themselves in any of the acts prohibited under paragraph 1(A), (B) or (C) in the indorsement of claim</i> [2019] HKCFI 2773 (HCA 1957 of 2019)	501
15. <i>Sham Wing Kan v. Commissioner of Police</i> [2020] HKCA 186 (CACV 270/2017, Date of Judgment: 2 April 2020)	505
16. <i>Tsang Po Mann v. Tsang Ka Kit and Another</i> [2021] 1 HKLRD 1301	509
17. <i>Tso Yuen Shui v. Administrative Appeals Board</i> (HCAL 1050/2000, Date of Decision: 16 November 2000)	511
18. <i>Wu Kit Ping v. Administrative Appeals Board</i> [2007] 4 HKLRD 849 (HCAL 60/2007)	514

<b>Appendix II Major Differences between the PIPL, the GDPR and the PDPO</b>	516
--	-----

<b>Appendix III Checklist for Data Users in Ensuring Compliance with the Ordinance</b>	525
--	-----

**Appendix IV Data Subject's Rights when his Personal Data Privacy is Infringed**

Conciliation with the Data User	529
Lodging of a Complaint with the Commissioner under Section 37	529
Appeal to the Administrative Appeals Board under Section 9 of the Administrative Appeals Board Ordinance (Cap. 442)	530
Civil Remedies	531

## Key Members of the Editorial Team

**Ms Cecilia SIU Wing-sze**

LL.B., LL.M. (HKU), LL.M. (UCL)

Accredited Mediator (HKMAAL, CEDR)

Solicitor (HKSAR & England and Wales)

Assistant Privacy Commissioner (Legal, Global Affairs and Research)  
Office of the Privacy Commissioner for Personal Data, Hong Kong, China

**Mr Billy KWAN Kai-yu**

BBA (Law), LL.B (HKU)

Solicitor (HKSAR)

Assistant Privacy Commissioner (Complaints and Criminal Investigation)  
Office of the Privacy Commissioner for Personal Data, Hong Kong, China

**Ms Ines LEE Hiu-ying**

LL.B., MSocSc (Counselling) (HKU)

Solicitor (HKSAR & England and Wales)

Head of Legal

Office of the Privacy Commissioner for Personal Data, Hong Kong, China

# Chapter 1

## Introduction

- 1.1** The Personal Data (Privacy) Ordinance (Cap. 486) (“the Ordinance”) aims to protect the privacy of individuals (“data subjects”) in relation to their personal data. It is, by design, principles-based and technology neutral. It is generally more instructive than prohibitive and remedial rather than punitive as regards contravening acts. Its core instructive provisions are encapsulated in the six data protection principles (“DPPs”) found in Schedule 1 of the Ordinance. These principles are the cornerstones of the Ordinance.
- 1.2** The enactment of the six DPPs aimed to promote a culture of protecting the privacy of personal data at every stage (from collection, holding, processing and use to deletion) based on international data protection standards enshrined in the *OECD Privacy Guidelines* of 1980<sup>1</sup> and the EU Data Protection Directive of 1995.<sup>2</sup> Contraventions of the DPPs by a data user do not per se constitute criminal offences. A data user only becomes criminally liable under the Ordinance if he fails to comply with the terms of an enforcement notice issued by the Privacy Commissioner for Personal Data (the “Commissioner”) when a contravention is found. A data user will also commit an offence if, having undertaken to comply with an enforcement notice, he intentionally performs an act or omission specified in the enforcement notice. An enforcement notice issued by the Commissioner after an investigation will direct the non-compliant data user to take steps to remedy and prevent recurrence of the contravention of the Ordinance. Contravention of DPPs can also form the basis of a civil lawsuit by the aggrieved individual for compensation of damage suffered,<sup>3</sup> whether or not an enforcement notice has been issued.

1. *OECD Privacy Guidelines 1980* is a commonly used abbreviated title for the original 1980 version of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

2. In formulating the Ordinance, the Law Reform Commission of Hong Kong also made reference to the then draft version of Directive 95/46/EC of the European Parliament and Council.

3. Section 66 of the Ordinance.

1.3 After its enactment in 1995, the Ordinance was amended upon the passing of the Personal Data (Privacy) (Amendment) Ordinance in 2012 ("Amendment Ordinance 2012")<sup>4</sup> with the introduction of, inter alia, Part 6A regulating direct marketing activities, which came into force on 1 April 2013. In 2021, the Ordinance underwent another major amendment. The Personal Data (Privacy) (Amendment) Ordinance 2021 ("Amendment Ordinance 2021") aims to combat doxxing acts that are intrusive to personal data privacy, through the criminalisation of such acts and confers on the Commissioner statutory powers to issue notices to demand the cessation or restriction of disclosure of doxxing messages. The amendments that came into operation on 8 October 2021 also confer on the Commissioner power to conduct a criminal investigation and institute prosecution for doxxing-related offences, to strengthen enforcement against doxxing cases.

1.4 As personal data has become more valuable and ubiquitous in the digital age and contravention of the DPPs may have legal consequences, it is in every data user's interest to understand and comply with the Ordinance. However, some provisions of the Ordinance may need to be construed constructively beyond their literal meaning. Data users would undoubtedly benefit from the Commissioner's explanation of compliance requirements with practical examples and cases decided in the local context as illustrations.

1.5 Relatively few decisions and judgments concerning the protection of personal data privacy provide authoritative interpretations of the provisions of the Ordinance, including the DPPs. However, the Commissioner has handled a considerable number of enquiries, complaints and compliance checks and investigations in respect of potential or actual contraventions of the requirements of the Ordinance. The Commissioner's decisions, based on interpretation of the relevant provisions of the Ordinance, have occasionally been tested in Court and in appeals to the Administrative Appeals Board ("AAB"),<sup>5</sup> whose determinations carry authoritative weight and precedential value.

1.6 Against this background, it is in the public interest for the Commissioner to state openly the criteria, principles and approaches applied in the discharge of the Commissioner's roles as regulator, facilitator and educator, when interpreting, administering and enforcing the provisions of the Ordinance.

4. Amendment Ordinance 2012 was gazetted on 6 July 2012.

5. Under the relevant provisions of the Ordinance and the Administrative Appeals Board Ordinance (Cap. 442), certain decisions of the Commissioner may be appealed.

It is hoped that such clarification and explanation will:

- help data users understand and comply with the requirements of the Ordinance;
- help the legal advisors of both data users and data subjects give correct and practicable advice to their clients;
- help data subjects understand the Commissioner's likely position on a particular issue when they consider lodging a complaint with the Commissioner;
- provide reference material for consideration by the Court or the AAB in cases relating to the Ordinance; and
- provide academics and other interested persons with materials for further study and research.

## Regulatory Approach

1.7 Broadly, the Commissioner's regulatory approach is consistent with common law rules on statutory interpretation, in particular the principles of interpretation<sup>6</sup> laid down by the Interpretation and General Clauses Ordinance (Cap. 1), particularly section 2A(1), which provides as follows:

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.

and section 19, which provides that:

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.<sup>7</sup>

6. These include the "literal rule," which accords primacy to the literal meaning of the language used in the legislation; the "golden rule," which is a 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.

7. In how to apply the rule of "fair, large and liberal" construction and interpretation, reference can be made to the Court of Final Appeal in the case of *The Medical Council of Hong Kong v. David Chow Si 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 a medical practitioner who was removed from the register for a specified period, the Court took the following five interpretative factors into account: (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 through a side-wind.

1.8 The Commissioner is mindful of the generally recognised principle of “presumption against absurdity” in statutory interpretation,<sup>8</sup> which is explained in *Bennion on Statutory Interpretation*<sup>9</sup> 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.<sup>10</sup>
- (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.

1.9 In the judgment of the Court of First Instance of the High Court on appeal from a criminal conviction under Part 6A of the Ordinance,<sup>11</sup> Wong J (as he then was) cited the approach taken by the Court of Final Appeal in interpreting a statute, i.e., to adopt a purposive approach:<sup>12</sup>

A purposive interpretation was adopted. The statutory language was construed, having regard to its context and purpose. Words were to be given their ordinary and natural meaning unless their context or purpose pointed to a different meaning. Context was to be considered in first instance, not only when ambiguity was thought to arise. Context was to be taken in its widest sense and included other statutory provisions and the general law. The purpose of a statutory provision might be evident from the provision itself, the recommendation of a report such as that by the Law Reform Commission, the Explanatory Memorandum to the relevant bill or a statement by the responsible official of the Government in relation to that bill in the Legislative Council.<sup>13</sup>

8. Otherwise known as the “golden rule” of interpretation, that whatever the literal meaning of the language used in the legislation, there is a presumption that it did not truly intend to bring about an absurd result.

9. Sixth Edition, LexisNexis Butterworths.

10. 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 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).

11. *HKSAR v. Hong Kong Broadband Network Limited* [2018] 2 HKLRD 1049 (HCMA 624/2015, on appeal from TWS 6311/2015).

12. *HKSAR v. Cheung Kiu Yin* (2009) 12 HKCFAR 568.

13. *Ibid* at paragraph 64.

1.10 The principles of statutory interpretation were helpfully summarised by Ma CJ (as he then was),<sup>14</sup> as follows:

- (1) In construing statutory provisions, the Court does not merely look at the relevant words. It construes the relevant words having regard to their context and purpose.
- (2) The context of the relevant statutory provision should be taken in its widest sense and will of course include the other provisions of the statute. It may also be relevant in any given case to look at the history of the relevant provisions.
- (3) Ascertaining the purpose of the statutory provision is obviously relevant, not only to help provide the relevant context, but to give meaning to the words used. In this latter respect, it is to be observed that often the meaning of words by themselves will not be clear unless regard is paid to the context and purpose. Words have to be construed but they must not be construed in vacuum.
- (4) The purpose may be clear from the provision itself or it may be necessary to look at the Explanatory Memorandum to the bill introducing the provision or a ministerial or official statement may be utilised for this purpose.

1.11 The Commissioner notes that the Law Reform Commission Report entitled *Reform of the Law Relating to the Protection of Personal Data* published in August 1994 has often been referred to in interpreting the Ordinance. The Commissioner is also mindful of the observation by Fok PJ<sup>15</sup> that:

The modern approach to statutory construction is not in issue. The proper starting point is to look at the relevant words or provisions having regard to their context and purpose. ... The purpose of a statutory provision may be gleaned from the provision itself or from a relevant report of the Law Reform Commission or the Explanatory Memorandum to the bill or from a statement of a responsible official to the Legislative Council in respect of a bill ...

Nevertheless, the object of the exercise is to ascertain the legislative intent of the language of the statute and, in this regard, a court cannot attribute to a statutory provision a meaning which the language, understood in the light of its context and statutory purpose, cannot bear.

1.12 Hence, in dealing with cases that require the interpretation of a particular DPP and/or provision of the Ordinance that, according to its language, seems

14. *Town Planning Board v. Town Planning Appeal Board* (2017) 20 HKCFAR 196 at paragraph 29.

15. *T v. Commissioner of Police* (2014) 17 HKCFAR 593 at paragraphs 194–195.

to be open to more than one interpretation, the Commissioner will adopt the interpretation that does not produce an absurd or impractical result, in regard to its context and purpose, bearing in mind that the primary purpose of the Ordinance is to protect individuals' right to privacy in relation to their personal data.

- 1.13 The Commissioner will strictly adhere to the applicable legal principles under the Ordinance and will adopt a consistent approach to interpreting the provisions of the Ordinance, including the DPPs. However, the Commissioner may find it necessary to re-consider a stance that she previously adopted in light of her regulatory experience and changes in circumstances in furtherance of the underlying objectives of the Ordinance, i.e., to protect individuals' personal data privacy. Such circumstances may include amendments to the Ordinance, the possibility that an interpretation previously adopted may later be shown to be erroneous or incomplete by the Court or the AAB, the views of other relevant judicial authorities or developments in the handling and processing of personal data and social values, locally and around the globe.

#### Disclaimer

- 1.14 Statements made or views expressed in this publication are intended for reference only. They shall not give rise to any liability on the part of the Commissioner or to any defence or estoppel of any kind in proceedings involving the Commissioner. They shall not bind the Commissioner in the exercise of the Commissioner's statutory functions in any way. Readers are advised to seek professional advice, where necessary, on the application of the Ordinance to any given situation.

#### Abbreviations Used in This Book

- 1.15 "AAB" means the Administrative Appeals Board, established under section 5 of the Administrative Appeals Board Ordinance (Cap. 442).

"AAB Ordinance" means the Administrative Appeals Board Ordinance (Cap. 442).

"Amendment Ordinance 2012" means the Personal Data (Privacy) (Amendment) Ordinance 2012.

"Amendment Ordinance 2021" means the Personal Data (Privacy) (Amendment) Ordinance 2021.

"Commissioner" means the Office of the Privacy Commissioner for Personal Data, established under section 5(1) of the Personal Data (Privacy) Ordinance (Cap. 486) 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) under Schedule 1 of the Ordinance.

"GDPR" means the General Data Protection Regulation of the European Union, which took effect on 25 May 2018.<sup>16</sup>

"HKID Card" means the Hong Kong Identity Card.

"LRC" means the Law Reform Commission of Hong Kong.

"LRC Report" means the Law Reform Commission Report entitled *Reform of the Law Relating to the Protection of Personal Data* published in August 1994.

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

"PCPD" means the Office of the Privacy Commissioner for Personal Data, Hong Kong.

"PICS" means Personal Information Collection Statement, which is a form of written notification under the requirements of DPP1(3).

"PIPL" means the Personal Information Protection Law of the Mainland which took effect from 1 November 2021.<sup>17</sup>

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

"Website" means the Commissioner's website at [www.pcpd.org.hk](http://www.pcpd.org.hk).

- 1.16 Unless the context requires otherwise, all words in the masculine gender appearing in this publication include the feminine and neuter gender, and all words in the singular include the plural, and vice versa.

16. The Commissioner published a booklet entitled *European Union General Data Protection Regulation 2016* to enhance understanding and raise the awareness of stakeholders in Hong Kong of the law and its possible impact. An updated edition was published on 12 June 2020 and can be downloaded from the Website.

17. The Commissioner published a booklet entitled *Introduction to the Personal Information Protection Law of the Mainland* in November 2021 to introduce the background and major requirements of the PIPL, and provide a brief overview of the similarities and differences between the Ordinance and the PIPL. The booklet is available on the Website.

## Chapter 2

### The Meaning of “Personal Data”

#### The main questions:

- What constitutes “data”?
- What constitutes “personal data”?
- How does each of the conditions laid down in paragraphs (a), (b) and (c) of the definition of personal data apply?
- Do IP addresses, email addresses, fingerprints, examination scripts, mobile phone numbers, digital content on mobile phones and a person’s whereabouts constitute “personal data” under the Ordinance?
- Can fabricated information be regarded as an individual’s personal data?
- What is the distinction between an “identified” individual and an individual capable of being “identified”?
- How should the existing definition of “personal data” be construed in light of overseas trends and rapid technological advancements?

## Introduction — Meaning of the Term “Data”

2.1 The definition of the term “data” is provided under 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.

2.2 The term “document” is 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 is 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, for information to constitute data, such information must have been recorded in a document as defined. This point may seem obvious, but it is worth emphasising to avoid misunderstanding.

2.4 Information not represented in any document (hence not constituting personal data) may be found in situations where, for example, information is committed to a person’s memory, or spoken but not recorded. The question of whether a verbal utterance amounts to disclosure of personal data was considered in *AAB No. 21/1999*, in which a civil servant came to know certain sensitive personal information about the complainant through handling her complaint. Since there was no evidence to prove that the sensitive personal information had ever existed in a recorded form, the AAB ruled that no personal data was involved and thus the case fell outside the jurisdiction of the Commissioner. In *AAB No. 6/2004*, the verbal replies (not recorded) given by certain employees to the employer in relation to questions about the number of private telephone calls made by a particular staff member and the contents thereof did not constitute personal data of that staff member. Further, in *AAB No. 17/2017*, it was held that conversations between the complainant and a property officer outside the complainant’s flat and in the management office did not amount to personal data.

## Definition of “Personal Data”

2.5 “Personal data” is defined under 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 The meaning of the term “data” as described in paragraphs 2.1–2.4 above is reasonably clear. Whether any data constitutes personal data therefore depends on whether such data satisfies all three of the 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, uncertainty may arise in their application, 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 the concept of “relatedness” is 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 Court of Appeal of England and Wales in detail. In *Durant v. Financial Services Authority* [2003] EWCA Civ 1746, it was held that in determining what constituted personal data, two relevant considerations are:

- whether the information was biographical in a significant sense; and
- that the information should have the individual as its focus rather than some other person with whom he may have been involved.

However, applying the arguments or principles of this English authority to Hong Kong cases must be undertaken with great care. As pointed out by the learned judge in *Wu Kit Ping v. Administrative Appeals Board* [2007] 4 HKLRD 849:

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.<sup>1</sup>

- 2.9 In the case of data that bears 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 relates directly to the sole proprietor, whether or not a relationship exists may become progressively less clear in cases where, for instance, 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.
- 2.10 In the case of *Wu Kit Ping*, the complainant made a data access request to a data user asking them to supply her with written statements concerning her medical treatment, which had been given by medical officers to the data user. The data user supplied the relevant documents to the complainant but made certain redactions, which can be divided into three categories:
- (i) the names of the writers and recipients (not being the complainant) in several letters and a statement concerning the complainant's diagnosis, treatment and use of medications;
  - (ii) a statement concerning the writer's own conduct of the treatment of the complainant in his professional capacity, in a letter from the writer to a recipient who was not the complainant; and
  - (iii) the writer's general statements made in a letter.
- 2.11 The Court considered that the names of the writers and recipients in category (i) were the personal data of the writers and recipients, not the complainant, and they did not fall within the scope of personal data "relating directly or indirectly" to the complainant. The redactions were therefore lawful. In respect of category (ii), the Court considered that the redacted part was an opinion related directly

<sup>1</sup> The cases of *Durant* and *Wu Kit Ping* have been referred to by the Hon Bharwaney J in his judgment in *Chan Yim Wah Wallace v. New World First Ferry Services Limited* (HCP1 820/2013). See further in Chapter 12.

to the complainant, and hence it was her personal data, and should have been disclosed to the complainant. Since the general statements in category (iii) have broad general application and did not directly or indirectly relate to the complainant, the Court concluded that they were not her personal data.

- 2.12 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 the personal data of Mr Y but merely a record of the reason why Mr Y could not be reached for an appraisal interview.
- 2.13 The question of whether the views and opinions expressed by an owner in an owners' committee meeting were his personal data was examined in AAB No. 28/2010. The AAB held that the views and opinions expressed by the owner on how the owners' committee should be conducted and how the observer should behave during the meetings did not amount to personal data of the owner as these views and opinions were not related directly or indirectly to the owner. It can therefore be seen that while the definition of data includes the expression of opinion under the Ordinance, such opinions must relate directly or indirectly to a living individual for them to fall within the scope of personal data protected under the Ordinance.
- 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 and not trivial. However, when dealing with a complaint, the Commissioner may be inclined to avoid an absurd result if the relationship between the data concerned in the complaint and the complainant is none but trivial, and may exercise her discretion to refuse to investigate such a 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 the legal proceedings to which the concerned individual was a party, was not the personal data of the individual. According to the AAB, the invoice, although addressed to a named individual, related to the trading price in a business transaction rather than to the individual personally.
- 2.16 The Ordinance protects the personal data of living individuals and does not extend to that of deceased persons. This is illustrated by the decision of AAB No. 27/2005, in which the complainant, who was the grandson-in-law and lawful guardian of an elderly woman, complained about a social worker because she had disclosed to the elderly residential care home the fact that the elderly woman had died. The AAB held that for the Ordinance to apply, the personal data must relate to a living individual, and it does not include that of a deceased person.

Similarly, in AAB Nos. 16 & 17/2019, the AAB ruled that the complainant was not entitled to request access to information about her deceased father, as it did not fall within the scope of personal data under the Ordinance.

**Paragraph (b) — “From which it is Practicable for the Identity of the Individual to be Directly or Indirectly Ascertained”**

2.17 In applying the condition laid down in paragraph (b) to personal data, the first thing to note is that the word “practicable” wherever it appears in the Ordinance, is defined under section 2(1) to mean “reasonably practicable”.

2.18 In the case of AAB No. 16/2000, the appellant made a complaint to the Commissioner about a public transport company because whenever he entered or exited through the toll gates using his senior citizen concessionary payment card, indicator lights flashed and an alarm went off. This would reveal to all persons nearby that he was over 65, which, according to him, amounted to disclosure of his personal data. The AAB in its decision confirmed the Commissioner’s view that there had been no disclosure of information regarding the complainant’s age and the card could be purchased or possessed by anyone. The fact that the light and sound were emitted when the appellant used a concessionary payment card to pass through the toll gate did not make it reasonably practicable for the identity of the appellant to be directly or indirectly ascertained. The light and sound signals only identified the type of card used, not the person using it.

2.19 Secondly, in deciding whether certain data held by a party satisfies 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 reference to the individual should be able to be construed from the context of all the relevant information that is available, of which the personal data of that individual forms part. For example, an employer holding a personnel file on one of his employees would not necessarily have the name of or other identifying information about the employee explicitly stated on every page. If the employer should be asked whether the information contained on 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 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 satisfied.

2.20 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, 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 is 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 is found attached to a personnel file created for a particular employee, although no name is 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.

2.21 This can also be illustrated by a scenario where fingerprint data is collected by an employer for the purpose of recording attendance. While it may not be practicable for the identity of an employee to be ascertained solely from the fingerprint data, it can be linked with other data held by the employer, for example, the staff number assigned to each employee, which in turn will point to the identity of a particular staff member. It will then become practicable for the employer to ascertain the identity of an employee who swipes a fingerprint scanner installed for recording attendance to gain access to the office premises.

2.22 Where part of the personal data is anonymised 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 met, hence failing to satisfy the definition of personal data.

2.23 The question of 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 set up by the residents of an estate. The individual alleged that the three Chinese characters of his name were used in a poetic expression posted on the forum. The Commissioner opined that it was not practicable to identify the individual from the data 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 on the forum as his nickname and address, and concluded that the data, taken together, was personal data, as