BUTTERWORTHS HONG KONG

Data Privacy Law
HANDBOOK

Third Edition

LexisNexis®
Butterworths

Data Privacy Law Handbook

Table of Contents

The commentary in this book states the law as at 1 June 2024.

PERSONAL DATA (PRIVACY) ORDINANCE

(CAP 486)

Introduction

The Personal Data (Privacy) Ordinance (Cap 486) (the 'Ordinance') regulates personal records. Brought into force on 20 December 1996, the present Ordinance applies to all accessible data relating to an identifiable individual (the 'data subject') which are contained in any recording medium. Regulation is effected through the application of six 'data protection principles'. These principles restrict data users in their collection, processing and use of personal data and confer on the data subject the right to access and correct such data. The legislation also establishes the Office of the Privacy Commissioner for Personal Data to oversee compliance with the requirements of the present Ordinance. Data subjects may complain to the Commissioner regarding any contravention of the present Ordinance affecting them. Where the contravention causes the data subject loss or injured feelings that individual may institute civil proceedings for compensation. Criminal sanctions are stipulated for any contravention other than a breach of a data protection principle.

The background to the legislation

The Personal Data (Privacy) Ordinance (Cap 486) implements most of the recommendations of the Hong Kong Law Reform Commission's 1994 Report on Reform of the Law Relating to the Protection of Personal Data. Whereas the American courts have recognised a legal right to privacy, English courts have consistently declined to do so. For the foundations of the protection of privacy in Hong Kong, the Law Reform Commission's starting point was the relevant treaty provisions contained in the International Covenant on Civil and Political Rights together with the European Convention for the Protection of Human Rights and Fundamental Freedoms. However, these treaties were developed in the wake of World War II and were inadequate in coping with the explosive growth in computerisation and telecommunications gathering momentum since the 1970s. In 1980, this recognition had prompted the Council of Europe and the Organisation for Economic Co-operation and Development to formulate a set of data protection principles providing more comprehensive protection.

Most of the world's industrialised economies have adopted these data protection principles as the basis of the legal regulation of personal data. However, the data privacy laws of the different jurisdictions diverge somewhat in the manner in which they endeavour to enforce the principles. The present Ordinance has been particularly influenced by the English, Australian and New Zealand data privacy laws. However, whilst many of the present Personal Data (Privacy) Ordinance (Cap

the data, the right to access and correct them. This right is expressly qualified by s 20 so as not to extend to data also relating to another individual. Accordingly, to hold that an evaluator is also the subject of the data would, by denying access, stymie a principal objective of the present Ordinance and the scope of 'relate to' should be read down accordingly.

It follows from the requirement that the data relate to a living individual that data relating to artificial legal persons or partnerships are not covered. This interpretation is strengthened by the long title of the present Ordinance with its reference to protecting the privacy of individuals. This has also been held to be the position under the Privacy Act 1993 (New Zealand) (repealed)'s requirement that personal information must be 'about' an identifiable individual. Accordingly, where a bank had disclosed bank statements of a company which the plaintiff had operated and which detailed transactions of a personal nature, it was held that information was about the transactions of the company and not those of the plaintiff, no matter how identified with the company the individual was: see *C v ASB Bank Ltd* (1997) 4 HRNZ 306 (Complaints Review Tribunal, NZ); and Waters N, 'Cases and complaints' (1997) 4(6) Privacy Law & Policy Reporter, at p 116. However, data relating to a sole proprietorship arguably may, no separate legal entity being involved.

(2) Identifiable

To constitute 'personal data', it must be reasonably practicable to 'directly or indirectly' ascertain the identity of the data subject. Anonymous data are not covered. Where identification can be ascertained solely from the data in question such ascertainment is direct. 'Indirect' ascertainment extends the test to where identification can be practicably effected by recourse to other information held by the data user or readily obtainable by him. An example would be data criticising members of a particular organisation, without singling out any specific individual. If the data user also holds a list of all members, then the critical data would be identifiable as regards those members.

(3) Retrievability

The third and final requirement of 'personal data' is that they be in a form in which access to, or processing of, the data is reasonably practicable. Data relating to identifiable individuals may for practical purposes be unavailable to the data user holding them. For example, a long report may make scattered references to an individual, but without an index it may not be reasonably practicable to locate them. An objective standard of reasonableness is appropriate, although that hallowed common law creature the 'reasonable man' may be replaced in this context by the 'reasonable data user'. The requirement that data be reasonably retrievable accommodates all relevant factors ranging from the sensitivity of the data to the resources of the data user. Whereas a florist's old invoices may well not be reasonably retrievable, vital medical records held in unindexed manual files should be subject to a more stringent threshold of retrievability. Application of the reasonableness test ensures that a data user cannot exclude the application of the Personal Data (Privacy) Ordinance (Cap 486) merely by resorting to poor records management.

discipline. Where the collection is from other sources, the data purposes will be determined by the circumstances of the collection.

Personal data may only be used for a purpose other than the purpose of collection (or a directly related purpose) if an exemption applies or the data subject's prescribed consent is obtained. 'Prescribed consent' is defined in s 2(3) as 'the express consent of the person given voluntarily'. 'Express' is the contrary of implied or inferred and means affirmative assent. The requirement would not be fulfilled by merely advising a data subject that a change of purpose was proposed unless his objection is received. It is also implicit in the concept of 'consent' that it be informed. This requires that the consent must relate to a proposition which is reasonably specific, as opposed to a blanket acquiescence without meaningful restrictions. Subject to these provisos, a single consent may relate to a series of transactions. For an example where it was held that there was no prescribed consent for a transfer of data to a third party, see *Wing Lung Bank Ltd v Privacy Commissioner for Personal Data* [2010] 6 HKC 266.

(4) Principle 4: Security of personal data

This requires that data users take all reasonably practicable steps to protect personal data. The principle identifies a number of relevant considerations in determining the adequacy of security measures. To comply with this principle, the data user should classify its data holdings according to their sensitivity. An assessment then needs to be made regarding potential security risks and the corresponding protective measures required.

Unlike the other provisions of the Personal Data (Privacy) Ordinance (Cap 486), principle 4 applies to data which is not reasonably practical to retrieve or process. This accommodates the concern that unstructured data may upon falling into the wrong hands then be organised and systematically used to the detriment of the data subject.

(5) Principle 5: Information to be generally available

This principle exhorts data users to be open and transparent not only to data subjects but the public generally regarding their data policies and practices, the kinds of personal data held, and their main purposes. To comply, a data user should promulgate these matters by convenient means ranging from notice-boards to website statements.

(6) Principle 6: Access to personal data

This principle provides the data subject with the right to ascertain from a data user whether it holds data on him or her and if so to access and correct or qualify that data. The mechanics of this process are elaborate and are spelt out in Pt 5 of the Personal Data (Privacy) Ordinance (Cap 486). By providing for access, this principle enables the data subject to monitor the extent to which a data user is complying with the other five principles. By conferring access rights, it provides data users with a crucial mechanism for enhancing data quality, as often the data

the consent of the data subject before the data user is permitted to use the personal data in directing marketing. Where data users intend to provide personal data to another for the latter's use of the data in direct marketing, they must give data subjects details of the intended provision of the personal data and to obtain the consent of the data subject before the data user is permitted to provide the personal data to the other person.

Another major change under the Personal Data (Privacy) (Amendment) Ordinance 2012 (18 of 2012) is concerned with the disclosure of personal data obtained from a data user without the data user's consent. Under s 64, an offence is committed where a person discloses the data:

(1) with an intent to obtain a gain;
(2) with an intent to cause loss to the data subject; or
(3) causing psychological harm to the data subject.

The Personal Data (Privacy) (Amendment) Ordinance 2012 also implements other reform proposals, including introducing provisions empowering the Commissioner to provide legal assistance to data subjects who wish to seek compensation pursuant to s 66 of the Personal Data (Privacy) Ordinance (Cap 486); providing for some new exemptions to the data protection principles; and miscellaneous amendments to the data protection principles.

The direct marketing provisions and the provisions on legal assistance by the Commissioner in the 2012 amendment Ordinance came into effect on 1 April 2013, while the other provisions came into effect on 1 October 2012.

In the reform exercise, the Government did not take up a number of other proposals recommended by the Commissioner. These include: more stringent control of sensitive personal data; direct regulation of data processors and sub-contracting activities; conferring criminal investigation and prosecution power to the Commissioner; empowering the Commissioner to require data users to pay monetary penalties for serious contraventions of the Data Protection Principles; and the setting up of a territory-wide do-not-call register against direct marketing activities. See further Office of the Privacy Commissioner for Personal Data, 'PCPD's Submission in Response to Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance' (31 December 2010).

In 2020, the Government announced that it was undertaking a review of the Personal Data (Privacy) Ordinance (Cap 486) in light of the rapid development of information and communication technologies and the widespread use of internet and mobile communications. The amendments being considered by the Government at the time of writing include the following:

(1) introducing a mandatory data breach notification mechanism;
(2) requiring data users to formulate a clear data retention policy which specifies a retention period for personal data collected;

2 WLR 203 (HL). The defendant was a police officer who accessed and viewed data held by a police computer for possible use by his private debt collecting company. Under the Data Protection Act 1984 (c 35) (UK) (repealed), it was a criminal offence to 'use' personal data for unregistered purposes (the 1998 Act now adopts the wider concept of 'processing' instead of 'use' of the data). The issue was whether the simple search or retrieval of data constituted 'use' of those data or whether something further had to be done with the data. By a narrow majority their Lordships held that under the 1984 Act 'use' meant the latter. The minority judgments argued that the privacy of the individual required that the simple search and retrieval of data be viewed as 'use'. Unlike the English Act, the long title of the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) specifically affirms that it aims to 'protect the privacy of individuals in relation to personal data'. This arguably provides a sufficient basis to distinguish *R v Brown* [1996] 2 WLR 203 (HL) and conclude that 'use' under the present Ordinance does extend to the search of data whether or not anything further is done with it. This broader interpretation has been adopted by the Australian Privacy Commissioner regarding the Privacy Act 1988 (Australia): see Australian Privacy Commissioner, Plain English Guidelines to Information Privacy Principles 8-11 (Human Rights Australia, 1996 Issue), at p 11.

[2.08] Document

'Document' is defined in s 3 of the Interpretation and General Clauses Ordinance (Cap 1) to mean any publication and any matter written, expressed or described upon any substance by means of letters, characters, figures or marks, or by more than one of these means. The definition of 'document' in the present section of the present Personal Data (Privacy) Ordinance (Cap 486) extends this to the specified 'documents' which are not in writing. A letter may come within this description: see *Carlish v East Ham Corpn and Edwards* [1948] 2 KB 380, [1948] 2 All ER 550 (QB); and *Lewisham Metropolitan Borough and Town Clerk v Roberts* [1949] 2 KB 608, [1949] 1 All ER 815 (CA, Eng). So may a tape recording of a conversation and a cinematograph film: see *Grant v Southwestern and County Properties Ltd* [1975] Ch 185, [1974] 2 All ER 465 and *Senior v Holdsworth, ex p Independent Television News Ltd* [1976] QB 23, [1975] 2 All ER 1009 (CA, Eng) respectively. See further *Halsbury's Laws of England* (4th edn, Vol 13, 2007 Reissue), at para 37, note 4.

[2.09] Contract of service

At common law work performed by an employee pursuant to a 'contract of service' is distinguishable from that of an independent contractor pursuant to a 'contract for services'. The phrase is to be construed by applying English common law: see *Lee Ting-Sang v Chung Chi-Keung and Anor* [1990] 1 HKLR 764, [1990] HKCU 370, [1990] 2 AC 374 (PC). In the absence of a written agreement, the issue is one of fact. The fundamental test is whether the person was performing the services as a person in business on his own account: see *Wong Man-Luen and Hong Kong Wah Tung Stevedore Co* [1971] HKLR 390, [1971] HKCU 29; *Lam Sik v Sen International Ventures Corp (HK) Ltd* [1994] 3 HKC 405 (DC); *Lee Ting-Sang v Chung Chi-Keung and Anor* [1990] 1 HKLR 764, [1990] HKCU 370, [1990] 2 AC 374 (PC); *Cheng Yuen v The Royal Hong Kong Golf Club* [1997] 1 HKC 243,

(1) whether the information is biographical in a significant sense, that is, going beyond the recording of the individual's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised; and

(2) whether the information has the individual as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest. The court further stated that in short, personal data is information that affects an individual's privacy, whether in his personal or family life, business or professional capacity.

Commenting on the *Durant v Financial Services Authority* [2003] EWCA 1746, [2004] IP & T 814 (CA, Eng) case, the English Court of Appeal in *TLT and Ors v Secretary of State for the Home Department and Anor* [2018] 4 WLR 101 (CA, Eng) noted that the question of 'focus' cannot sensibly be taken to mean that only a single individual can be in focus. Instead, it again contemplates a 'continuum' or spectrum. The court rejected a narrow approach to interpreting the words 'relate to', observing that data which is 'about' the person would be data relating to the person.

In *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450, [2007] 4 HKLRD 849 (CFI), it was held that the name of the maker of a report is the personal data of the maker and not the personal data of the individual who is the subject of the report. However, an opinion by the maker about a data subject is personal data of the data subject. An opinion expressed in the same document, by the maker of the document, about the maker himself will not constitute the personal data of the data subject, unless the opinion also relates to the data subject. In that case, the court held that a statement directed at the maker's conduct, in the maker's professional capacity, of the medical treatment of a patient, is an opinion which relates directly to the patient and is consequently personal data of the patient. While the court in *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450, [2007] 4 HKLRD 849 (CFI) reached the same conclusions as the English court in the *Durant v Financial Services Authority* [2003] EWCA 1746, [2004] IP & T 814 (CA, Eng) case, the court noted that because of the substantial differences between the English and Hong Kong legislation, great care must be taken in attempting to apply either arguments or principles used in the English cases when considering the present Personal Data (Privacy) Ordinance (Cap 486).

Where a person gives an eyewitness account to an investigating agency about an accident in which an injured person, or the injuries suffered by him or her, is mentioned, the information is not personal data of the injured person: *Chan Yim Wah Wallace v New World First Ferry Services Ltd* [2015] 3 HKC 382 (CFI), at [83]. The eyewitness account of the accident is also not personal data of the witness, except to the extent that it contains his or her personal particulars such as identity card number, addresses, telephone numbers and other contact details and also except to the extent that the witness speaks of any injuries he or she might have suffered in the same accident: *Chan Yim Wah Wallace v New World First Ferry Services Ltd* (above).

In *Sham Wing Kan (岑永根) v Commissioner of Police* [2020] 3 HKC 254, [2020] 2 HKLRD 529, [2020] HKCA 186, at [172]–[174], *dicta* of the Court of Appeal

[5.08] Servant or agent

A servant is, generally speaking, a person who is subject to the commands of his master both as to the work he is to do and also the manner in which it is to be done: see *Yewens v Noakes* (1880) 6 QBD 530 (CA, Eng). Whether one person is the servant of another is a question of fact: see *Brady v Giles* (1835) 1 Mood & R 494; and *Jones v Scullard* [1898] 2 QB 565 (QB). The term 'servant' is equivalent to the term 'employee' under a contract of service (as to which, see **[2.09]** above).

An agent is a person who has the authority, express or implied, to act on behalf of another, and who consents to act: *Pole v Leask* (1863) 33 LJ Ch 155, at 161. In *Ching Yuen Tung v Bep Aketik* [1978] 1 MLJ 211, at 213, Lee Hun Hoe CJ stated:

> The word 'agent' may be used in at least two other senses. First, the word is frequently used to describe the position of a person who is employed by another to perform duties often of a technical or professional nature which he discharges as the other's alter ego and not merely as an intermediary between the principal and the third party, ... Secondly, the word has often been used in business in a complementary and not a legal sense ...

See further *Halsbury's Laws of England* (4th edn, Vol 1(2), 1989 Reissue), at para 1 and *Halsbury's Laws of England* (4th edn, Vol 16(1A), 2022 Reissue), at paras 1 et seq.

[5.09] Definition

For 'Commissioner', see s 2 above.

---

6. Commissioner to hold no other office

The person appointed to be the Commissioner shall not, without the specific approval of the Chief Executive— *(Amended 34 of 1999 s. 3)*

(a) hold any office of profit other than his office as Commissioner; or

(b) engage in any occupation for reward outside the functions of his office.

[6.01] Enactment history

Section 6 was amended by the Adaptation of Laws (No 15) Ordinance 1999 (34 of 1999), deemed to have come into operation on 1 July 1997.

[6.02] Chief Executive

As to meaning, see **[2.14]** above.

[7.04] Power

'Power' is defined in s 3 of the Interpretation and General Clauses Ordinance (Cap 1) to include any privilege, authority and discretion. 'In the ordinary course of events when power is given to a person to do a thing, he may refuse to exercise it': see *Kannan v Menteri Buruh Dan Tenaga Rakyat* [1974] 1 MLJ 90, at 91, per Syed Othman J.

[7.05] Definition

For 'Commissioner', see s 2 above.

---

8. Functions and powers of Commissioner

(1) The Commissioner shall—

(a) monitor and supervise compliance with the provisions of this Ordinance;

(b) promote and assist bodies representing data users to prepare, for the purposes of section 12, codes of practice for guidance in complying with the provisions of this Ordinance, in particular the data protection principles;

(c) promote awareness and understanding of, and compliance with, the provisions of this Ordinance, in particular the data protection principles;

(d) examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the person proposing the legislation;

(e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government or statutory corporations;

(f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and information technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data; *(Amended 18 of 2012 s. 4)*

(g) liaise and co-operate with any person in any place outside Hong Kong—

failure to comply with a provision of a code render a data user liable to civil or criminal proceedings: s 13(1) below. Such failure shifts the onus onto the defendant: non-compliance with a relevant provision of an approved code will suffice to prove the statutory breach unless the data user can produce evidence of compliance with the statutory requirement 'otherwise than by way of observance of that provision'. This further emphasises the subordinate role of codes of practice.

As at the time of publication, the Commissioner has issued three codes of gazetted pursuant to s 12(1):

(1) The Code of Practice on the Identity Card Number and other Personal Identifiers was gazette on 19 December 1997. With the exception of the requirement restricting the issue of a card with an identity card number printed on it (which took effect on 19 December 1998), the requirements of the code took effect on 19 June 1998. The Code gives practical guidance to the requirements of the Personal Data (Privacy) Ordinance (Cap 486) as applied to the collection, retention, accuracy, use and security of identity card ('ID') numbers and copies of the ID card and other personal identifiers. A revised edition of the Code was issued in April 2016. A booklet on the issue is available from the office of the Privacy Commissioner.

(2) The Code of Practice on Consumer Credit Data was first issued on 27 February 1998, taking effect on 27 November 1998. The Code has been revised on a number of occasions since it was first issued. The Code protects the privacy interest of individuals in relation to their personal data used in the provision of consumer credit. In particular, it regulates the exchange of such data between lending institutions and credit reference agencies. See also the Fact Sheet 'Understanding the Code of Practice on Consumer Credit Data—Frequently Asked Questions—On the Sharing of Mortgage Data for Credit Assessment Purposes', which is available from the office of the Privacy Commissioner. A revised edition of the Code was issued in January 2013.

(3) The Code of Practice on Human Resource Management was notified in the gazette on 22 September 2000 and came into effect on 1 April 2000. The purpose of the Code is to provide practical guidance to employers and their staff on how to properly handle personal data relating to the employment process and in the performance of human resource management functions and activities. A revised edition of the Code was issued in April 2016.

[12.03] England

Under the present Personal Data (Privacy) Ordinance (Cap 486), codes of practice perform a similar role as they do under the Data Protection Act 2018 (UK), s 125(4).

PART 4

DATA USER RETURNS AND REGISTER OF DATA USERS

14. Data user returns

(1) Subject to subsection (2), the Commissioner may, by notice in the Gazette, specify a class of data users to which this section shall apply.

(2) The Commissioner shall, before specifying a class of data users in a notice under subsection (1), consult with—

(a) such bodies representative of data users belonging to that class; and

(b) such other interested persons,

as he thinks fit.

(3) This section shall not apply to a data user except a data user belonging to a class of data users specified in a notice under subsection (1) which is in force.

(4) A data user shall submit to the Commissioner a return— *(Amended 18 of 2012 s. 7)*

(a) in the specified form;

(b) containing the prescribed information required by the return in relation to the data user;

(c) in the case of—

(i) a data user which belongs to the class of data users concerned on the day on which the notice under subsection (1) specifying that class commences, not earlier than 3 months before, and not later than, each anniversary of that day;

(ii) a data user which first belongs to the class of data users concerned on a day after the day on which the notice under subsection (1) specifying that class commences, not earlier than 3 months before, and not later than, each anniversary of that first-mentioned day; and

(d) accompanied by the prescribed fee.

(5) The Commissioner shall cause a notice to be published not less than once during every period of 6 months—

(a) in—

(i) the Gazette; and

deemed to belong only to that class of data users specified in the first of those notices to be published in the Gazette. *(Amended 18 of 2012 s. 7)*

(c) *(Repealed 18 of 2012 s. 7)*

(10) *(Repealed 18 of 2012 s. 7)*

(11) A data user who, in purported compliance with subsection (4) or (8), knowingly or recklessly in a data user return or change notice supplies any information which is false or misleading in a material particular, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months. *(Added 18 of 2012 s. 7)*

[14.01] Enactment history

Subsection (6) was amended by LN 130 of 2007, effective 1 July 2007. Subsections (4), (5), (7) and (9) were amended, and sub-s (11) added by the Personal Data (Privacy) (Amendment) Ordinance 2012 (18 of 2012), effective 1 October 2012.

[14.02] General note

The provisions of Pt 4 provide for notification rather than 'registration' as such as the Commissioner's approval is not required for processing personal data. Contrary to a recommendation of the Hong Kong Law Reform Commission, the present Personal Data (Privacy) Ordinance (Cap 486) does not impose a blanket notification requirement. It is for the Commissioner to identify classes of data users meriting the requirement and the implication is that he will proceed selectively. There is also provision for a register assisting individuals to identify those data users that are likely to hold personal data relating to them. Requiring data users to notify the Commissioner facilitates his office in more closely monitoring their activities. The present Ordinance does not identify any criteria in determining which classes of data users warranting the requirement. Nor to date have any classes been designated. However, the effective enforcement of the statutory scheme and in particular the data protection principles may be enhanced by the application of the notification requirement depending on the nature of the data involved and the role of the class of data users concerned. Data users processing highly sensitive data, such as medical data may be thought to warrant the imposition of the requirement, as too those generating a high level of complaints to the Commissioner. There are also data users who operate in effect behind a screen because they collect data from other data users rather than directly from data subjects. Reference agencies servicing entire industries may cull data from a variety of sources for processing. The imposition of the notification requirement on such data users may help redress this lack of transparency.

Knowledge includes the state of mind of a person who shuts his eyes to the obvious: see *James & Son Ltd v Smee* [1955] 1 QB 78, [1954] 3 All ER 273 (DC, Eng), at 91 and 278, per Parker J; and *Westminster City Council v Croyalgrange Ltd* [1986] 2 All ER 353, [1986] 1 WLR 674 (HL). Moreover, there is authority for saying that where a person deliberately refrains from making inquiries the results of which he might not care to have, this constitutes in law actual knowledge of the facts in question: see *Knox v Boyd* [1941] JC 82, at 86; *Taylor's Central Garages (Exeter) Ltd v Roper* (1951) 115 JP 445, [1951] WN 383 (DC, Eng), at 449 and 450, per Devlin J; and *Westminster City Council v Croyalgrange Ltd* (above); and see also *Mallon v Allon* [1964] 1 QB 385, [1963] 3 All ER 843 (DC, Eng), at 394 and 847. Yet mere neglect to ascertain what could have been found out by making reasonable inquiries is not tantamount to knowledge: see *Taylor's Central Garages (Exeter) Ltd v Roper* (above), per Devlin J; and cf, *London Computator Ltd v Seymour* [1944] 2 All ER 11 (DC, Eng); but see also *Mallon v Allon* (above).

As to when the knowledge of an employee or agent may be imputed to his employer or principal, see *Halsbury's Laws of England* (4th edn, Vol 11(1), 1973 Reissue), at para 55.

[14.12] Recklessly

A person is reckless if he does an act which in fact involves an obvious and serious risk of harmful consequences where he was aware of the risk and where it was, in the circumstances known to him, unreasonable to take the risk: *Sin Kam Wah Lam Chuen Ip and Anor v HKSAR* (2005) 8 HKCFAR 192, [2005] 2 HKLRD 375, [2005] HKCU 672 (CFA), *R v G and Anor* [2004] 1 AC 1034 (HL). Conversely, a defendant could not be regarded as culpable so as to be convicted of the offence if, due to his age or personal characteristics, he genuinely did not appreciate or foresee the risks involved in his actions As to what would constitute 'harmful' consequences for the purposes of the above test, see *Data Protection Registrar v Amnesty International (British Section)* [1995] Crim LR 633 (DC, Eng). See further *Halsbury's Laws of England* (4th edn, Vol 11(1), 1973 Reissue), at paras 14 and 15.

[14.13] False or misleading

It may be doubted whether the addition of the words 'or misleading' is in itself of great practical importance, for there is authority for saying that information may be false because it conveys a false impression although it is literally true: see *R v Lord Kylsant* [1932] 1 KB 442, [1931] All ER Rep 179 (CA, Eng); and *R v Bishirgian; R v Howeson; R v Hardy* [1936] 1 All ER 586 (CA, Eng). Yet there may be statements which cannot create a wrong impression in the mind of a person of intelligence and education, but are apt to mislead lesser or less tutored minds and which, therefore, are misleading though not false: cf, *Eno v Dunn* (1890) 15 App Cas 252 (HL), at 258, per Lord Watson. Nevertheless it is obvious that the abstract possibility that confusion may be created is not sufficient and that no information can be regarded as misleading unless there is 'a reasonable probability of confusion': cf, *Re Bayer Products Ltd's Application* [1947] 2 All ER 188 (CA, Eng), at 190, per Lord Greene MR. On the other hand, the fact that information is designed to mislead seems to give rise to a strong inference that it is likely to

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

[35K.01] Enactment history

This section was added by the Personal Data (Privacy) (Amendment) Ordinance 2012 (18 of 2012), effective 1 April 2013.

[35K.02] General note

This section imposes an opt-in arrangement whereby a data subject's consent is required before a data user may provide personal data to another for the latter's use of the data in direct marketing. For the background to the introduction of this provision, see **[35J.02]** above.

[35K.03] Written consent

Unlike the position for the giving of consent to a data user for the data user's use of personal data for its own direct marketing purposes (under s 35E), written consent of the data subject is required before a data user can transfer personal data to another for the latter's use of the data for direct marketing. As to the policy reason why written consent is required in this context, see **[35J.03]** above.

The consent may be given through the response channel notified to the data subject under s 35J(2)(c) or other written means: sub-s (3).

The consent may be given generally or selectively: sub-s (1)(a). As to the meaning of general or selective consent, see **[35E.03]** above. The data user may only provide data to another to the extent consistent with the consent given: sub-ss (1)(c) and (2).

[35K.04] Data provided for gain

If the personal data is to be provided to another person for gain, the intention to so provide must have been specified in the notification to the data subject in accordance with s 35J(2)(b)(i) before the data user is permitted to provide the data to the other person: sub-s (1)(b).

As to the meaning of provision of personal data for gain, see s 35A(2) above.

[35K.05] Permitted class of persons

The term is defined in s 35A(1). For example, if consent has been given to provide personal data to 'financial services companies' and 'telecommunications network service providers' for use in direct marketing, then the permitted class of persons would be any company whose nature of business is financial services or

(a) if the contravention involves a provision of personal data of a data subject for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or

(b) in any other case, to a fine of $500,000 and to imprisonment for 3 years.

(7) A person who contravenes subsection (5) commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years.

(8) In any proceedings for an offence under subsection (6) or (7), it is a defence for the data user or person charged to prove that the data user or person took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(9) This section does not affect the operation of section 26.

[35L.01] Enactment history

This section was added by the Personal Data (Privacy) (Amendment) Ordinance 2012 (18 of 2012), effective 1 April 2013.

[35L.02] General note

Whether or not a data subject has consented to a data user's provision of personal data to another for the latter's use in direct marketing, the data subject may (at any time after receiving a notification under s 35J(2)(b)) require the data user to cease to provide the data to any person for use in direct marketing: sub-ss (1) and (2). The data subject may require the data user to cease to provide the data to any person and not simply those referred to in the notification under s 35J(2)(b). If the data user fails to comply with the requirement, the data user commits an offence: sub-ss (3) and (6).

The data subject may also require the data user to notify any person to whom the data has already been provided to cease to use the data in direct marketing: sub-s (1)(b). The data user must then give such notification to the person in writing: sub-s (4). If the person who receives the written notification continues to use the data in direct marketing, then that person commits an offence: sub-ss (5) and (7).

[35L.03] Use

As to meaning, see **[2.07]** above.

[35L.04] Provision of personal data for gain

As to the meaning, see s 35A(2) above.

or practice done or engaged in, as the case may be, may prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person); *(Amended 32 of 2021 s. 4)*

(e) the Commissioner is satisfied that the relevant data user has not been a data user for a period of not less than 2 years immediately preceding the date on which the Commissioner received the complaint; or *(Amended 32 of 2021 s. 4)*

(f) the Commissioner is of the opinion that the complaint relates to an offence under section 64(1), (3A) or (3C) and decides to carry out a specified investigation (as defined by section 66C). *(Added 32 of 2021 s. 4)*

(2) The Commissioner may refuse to carry out or decide to terminate an investigation initiated by a complaint if he is of the opinion that, having regard to all the circumstances of the case— *(Amended 18 of 2012 s. 22)*

(a) the complaint, or a complaint of a substantially similar nature, has previously initiated an investigation as a result of which the Commissioner was of the opinion that there had been no contravention of a requirement under this Ordinance;

(b) the act or practice specified in the complaint is trivial;

(c) the complaint is frivolous or vexatious or is not made in good faith;

(ca) the primary subject matter of the complaint, as shown by the act or practice specified in it, is not related to privacy of individuals in relation to personal data; or *(Added 18 of 2012 s. 22)*

(d) any investigation or further investigation is for any other reason unnecessary.

(3) Where the Commissioner refuses under this section to carry out an investigation initiated by a complaint, he shall, as soon as practicable but, in any case, not later than 45 days after receiving the complaint, by notice in writing served on the complainant accompanied by a copy of subsection (4), inform

of the Commissioner's functions or the proper exercise of the Commissioner's powers under this Ordinance; *(Added 18 of 2012 s. 25)*

(b) disclosing in the course of proceedings—

(i) for an offence under this Ordinance; and

(ii) before any court or magistrate,

any matter relevant to those proceedings;

(c) reporting evidence of any crime to such authority as he considers appropriate;

(d) disclosing to a person any matter referred to in subsection (1) which, in the opinion of the Commissioner or prescribed officer, may be ground for a complaint by that person. *(Amended 18 of 2012 s. 25)*

(3) Subject to subsection (4), the Commissioner may disclose in any report made by him under this Ordinance any matter that in his opinion ought to be disclosed in order to establish grounds for his findings and recommendations other than a matter the disclosure of which in his opinion would involve the disclosure of personal data that is exempt from data protection principle 6 by virtue of an exemption under Part 8. *(Amended 18 of 2012 s. 25)*

(4) If a report is made by the Commissioner on an inspection or investigation, and the report contains personal data, the Commissioner must not publish the report unless— *(Amended 18 of 2012 s. 25)*

(a) a copy of the report in the form in which it is to be published has been supplied to the relevant data user;

(b) that copy is accompanied by a notice in writing inviting the data user to advise the Commissioner, in writing and not later than 28 days after being served with the copy, whether—

(i) in the opinion of the data user there is any matter in the copy the disclosure of which would involve the disclosure of personal data that is exempt from the provisions of data protection principle 6 by virtue of an exemption under Part 8; and *(Amended 18 of 2012 s. 25)*

(ii) the data user objects to the disclosure of the matter; and

(c) either—

[46.06] Magistrate

As to meaning, see **[13.05]** above.

[46.07] Administrative Appeals Board

As to meaning, see **[13.07]** above.

[46.08] Use

As to meaning, see **[2.07]** above.

[46.09] Level 3

As to meaning, see **[14.14]** above.

[46.10] Definitions

For 'Commissioner', 'prescribed officer', 'complaint', 'personal data', 'data protection principle', 'inspection', 'investigation', 'relevant data user' 'data user' and 'adverse action', see s 2 above.

---

47. Persons to be informed of result of inspection or investigation

(1) Where the Commissioner has completed an inspection, he shall, in such manner and at such time as he thinks fit, inform the relevant data user of—

(a) the result of the inspection;

(b) any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the data user;

(c) any report arising from the inspection that he proposes to publish under section 48; and

(d) such other comments arising from the inspection as he thinks fit to make.

(2) Where the Commissioner has completed an investigation, he shall, in such manner and at such time as he thinks fit, inform the relevant data user of—

(a) the result of the investigation;

(b) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to

as they are retained. The retention of personal data is governed by principle 2(2) and s 26 above.

These provisions require that the data user delete personal data which has served its purpose. Insofar as a reference will be compiled in relation to a particular position it follows that upon the position being filled the reference should be deleted.

The House of Lords has held that an employer ordinarily owes a duty of care to his employee in preparing a reference: see *Spring v Guardian Assurance Plc* [1995] 2 AC 296 (HL).

[56.03] Definitions

For 'personal data', 'employment' and 'data protection principle', see s 2 above.

---

57. Security, etc. in respect of Hong Kong

(1) Personal data held by or on behalf of the Government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong is exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to prejudice any of the matters referred to in this subsection. *(Amended 18 of 2012 s. 2)*

(2) Personal data is exempt from the provisions of data protection principle 3 in any case in which— *(Amended 18 of 2012 s. 2)*

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data is held for any of those purposes); and *(Amended 18 of 2012 s. 2)*

(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

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

(3) Any question whether an exemption under subsection (1) is or at any time was required in respect of any personal data may be determined by the Chief Executive or Chief Secretary for Administration; and a certificate signed by the Chief