ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Hong Kong SAR China

Status of Consent for Processing Personal Data

JUNE 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Mark Parsons

Partner, Hogan Lovells

ACKNOWLEDGEMENTS

This Report benefitted from contributions and editing support from Elizabeth Santhosh and Catherine Shen.

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Hong Kong's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

The main data protection law in Hong Kong is the Personal Data (Privacy) Ordinance ("**PDPO**")[1] – which was passed in 1995 and took effect in December 1996. The PDPO gives effect to the Data Protection Principles ("**DPPs**"), which are located in Schedule 1 to the PDPO and provide for how "data users"[2] may lawfully collect, use, and disclose personal data.[3] The DPPs are complemented by other provisions of the PDPO which establish compliance requirements for organizations that process personal data, including detailed provisions on direct marketing in Part 6A of the PDPO.[4]

Generally, notification, rather than consent, is the primary or default justification for collecting, using, and disclosing personal data under the DPPs and the PDPO. That said, in practice, organizations often implement notifications in the form of consent so as to generate a reliable record of that the data subject has received a notification.

Sector-based regulations have not significantly impacted the approach taken under the PDPO. Hong Kong banks are subject to the common law bank secrecy rules known as the "**Tournier Principles**,"[5] which apply to bank customers' information (whether or not this information is personal data). Under the Tournier Principles, customers' consent is required before the bank may disclose the customers' information, subject to exceptions, such as legal compulsion.

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PDPO

Although the PDPO's privacy management framework is based primarily on notification rather than consent, consent plays several important, albeit secondary, roles.

Under DPP 1, data users are required to take all practicable steps on or before the time of collection to inform data subjects of the collection of their personal data, the purposes for which it will be processed, and the classes of persons to whom it may be transferred. However, if the data user subsequently wishes to use the personal data for any other purpose, the data user must obtain the data subject's consent in accordance with DPP 3. Additionally, the combination of personal data as part of a "matching procedure" requires the consent of the data subject or the Privacy Commissioner for Personal Data ("**PCPD**").[6]

Part 6A of the PDPO also requires consent in respect of the use of personal data for direct marketing purposes,[7] though, notably, such consent may take the form of "an indication of no objection" to the use of personal data in direct marketing, or provision of data for such use.[8] This permits an "opt-out" form of consent, provided that there is some form of affirmative action by the data subject to indicate consent.

---

[1] Available at https://www.elegislation.gov.hk/hk/cap486

[2] A "**data user**" in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data (PDPO, s 2(1)).

[3] PCPD, "The Personal Data (Privacy) Ordinance," available at https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

[4] PCPD, "The Personal Data (Privacy) Ordinance."

[5] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.

[6] PDPO, s 30. Note that a "**matching procedure**" refers to "a procedure whereby personal data collected for 1 or more purposes in respect of 10 or more data subjects is compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison: (a) is (whether in whole or in part) for the purpose of producing or verifying data; or (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data, may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against any of those data subjects" (PDPO, s 2(1)).

[7] See, in particular, PDPO, ss 35E and 35K.

[8] PDPO, s 35A(1).

Section 33 of the PDPO – which seeks to regulate international transfers of personal data but has not yet been brought into force – would establish data subject consent as one of several legal bases for international transfers of personal data.

3. ROLE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA ("PCPD")

The Privacy Commissioner for Personal Data ("**PCPD**") is an independent statutory authority which is responsible for administering the PDPO.[9]

In keeping with its responsibilities under the PDPO to, among others, promote awareness and understanding of, and compliance with the PDPO,[10] PCPD issued detailed guidance in 2013 as to its expectations for consent in the context of direct marketing ("**Guidance on Direct Marketing**").[11]

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

There is no general definition of "consent" under the PDPO.

Part 6A of the PDPO provides a limited definition of "consent" which applies only to provisions on direct marketing. This definition includes "an indication of no objection" to the use of personal data in direct marketing, or provision of data for such use.[12] For example, consent for this purpose would likely be valid where a form allows data subjects to tick a checkbox to opt out of use of their personal data for direct marketing purposes, but a data subject leaves the checkbox unticked.

4.2. "Prescribed consent"

DPP 3 requires the data subject's "prescribed consent" for use of his/personal data for any purpose other than the purpose for which the data was to be used at the time of collection, or a purpose directly related thereto.[13]

"Prescribed consent" refers to express consent of the person, which has been given voluntarily[14] and has not been withdrawn by notice in writing served on the person to whom the consent has been given.[15] Note that the requirement for "prescribed consent" is deemed to have been satisfied for use or disclosure of personal data for direct marketing purposes if the data user has complied with certain requirements under Part 6A of the PDPO.[16]

4.3. Withdrawal of consent

Consent may be withdrawn, in which case the data user should immediately terminate any processing activities that had been conducted on the basis of consent.

In order to withdraw "prescribed consent," the data subject must serve a notice in writing on the person to whom consent was given.[17] Withdrawal of consent is without prejudice to acts done pursuant to consent before the notice of withdrawal is served.[18]

---

[9] See, generally, Parts 2 and 3 of the PDPO.
[10] PDPO, s 8(1)(c)
[11] PCPC Guidance Note, "New Guidance on Direct Marketing" (January 2013) ("**Guidance on Direct Marketing**"), available at https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf
[12] PDPO, s 35A(1).
[13] DPP 1(1) read with DPP 1(4).
[14] PDPO, s 2(3)(a)
[15] PDPO, s 2(3)(b),
[16] PDPO, ss 35H and 35M.
[17] PDPO, s 2(3).
[18] PDPO, s 2(3).

For direct marketing under Part 6A of the PDPO, a data subject may, at any time, require a data user to cease using the data subject's personal data in direct marketing[19] or providing the data subject's personal data to any other person for use by that other person in direct marketing.[20] A data user who receives such a requirement from a data subject must, without charge to the data subject, comply with the requirement,[21] or the data user will face criminal liability.[22]

4.4. Bundled consent

PCPD's Guidance on Direct Marketing indicates that PCPD would interpret bundled consent as a collection of data in violation of DPP 1(2) (which requires that collection of personal data should be lawful and fair in the circumstances of the case).[23]

As a matter of administrative practice, the PCPD requires that consent to direct marketing should not be "bundled" with general data protection consent and notifications.

There is also no provision of law as to whether access to services may be conditional on the user consenting to specific collection or use of data.

5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The PDPO does not designate any specific categories of personal data as "sensitive." Except where personal data is to be used or disclosed for direct marketing purposes, the general provisions of the PDPO concerning notification and/or consent to the collection and processing of personal data apply irrespective of the sensitivity of the personal data in question.

5.1. Children

A parent or legal guardian may give consent for use of a minor's personal data for a new purpose under DPP 3[24] if the minor is incapable of understanding the new purpose and deciding whether to give the prescribed consent,[25] and the parent or legal guardian has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject. [26]

5.2. Direct marketing

Part 6A of the PDPO sets out detailed requirements for the use of personal data for direct marketing purposes, stipulating the information which data users must disclose to data subjects in connection with the direct marketing and requiring the data user to notify the data subject of its intention to use or disclose the personal data for direct marketing purposes before the first such use or disclosure.

6. CONSENT FOR CROSS-BORDER DATA TRANSFERS

Section 33 of the PDPO concerns the regulation of international transfers of personal data but has not yet been brought into force. This provision, if enacted in its current form, would permit data users to transfer personal data outside of Hong Kong if the data subject consents in writing to the transfer[27] or if any of the remaining five lawful bases for cross-border transfer under Section 33(2) of the PDPO applies.

---

[19] PDPO, s 35G(1).
[20] PDPO, s 35L(1)(b).
[21] PDPO, ss 35G(3) and 35L(3).
[22] PDPO, ss 35G(4) and 35L(6)
[23] Guidance on Direct Marketing, page 7.
[24] DPP 3(2)(a)(i).
[25] DPP 3(2)(b).
[26] DPP 3(2)(c).
[27] PDPO, s 33(2)(c).

7. TRANSPARENCY AND NOTICE

The PDPO is fundamentally a notification-based regime in respect of most types of processing, and imposes obligations on data users to notify data subjects of the collection and processing of their personal data.

DPP 1 requires that "all practicable steps" are taken to ensure that data subject is *explicitly* informed:

- on or before data collection, of:
  - the purpose (in general or specific terms) for which the data will be used;[28]
  - the classes of persons to whom the data may be transferred;[29]
  - whether supplying the data is obligatory or voluntary;[30] and
  - if obligatory, the consequences for failing to supply the data; [31]
- on or before first use of the data, of:
  - the data subject's rights to request access to and the correction of the personal data;[32] and
  - contact details of the individual who will handle requests to exercise these rights. [33]

In practice, PCPD takes a fairly rigorous approach to assessing whether or not DPP 1 has been met, and there is often little leeway to argue that notification is not practicable.

Where "prescribed consent" is required to process personal data for a new purpose after the time of collection, this consent is required to be express and voluntarily given. [34]

Part 6A of the PDPO prescribes more stringent requirements for use or disclosure of personal data for direct marketing purposes.

Before a data user can seek consent to use personal data for direct marketing purposes,[35] the data user must inform the data subject of the following in writing in an easily understandable and readable format:[36]

- the data user's intention to use the personal data for direct marketing purposes;[37]
- the fact that data user's right to use the data subject's personal data for such purposes is contingent on the data subject's consent; [38]
- the types of personal data that will be used for direct marketing purposes; [39] and
- the types of goods and/or services that will be marketed using the data.[40]

Before a data user can provide a data subject's personal data to another person for use by that other person in direct marketing (note that PCPD's Guidance on Direct Marketing terms this "**cross-marketing**"[41]), the data user must provide the data subject with the following information in writing and in an easily understandable and readable format:[42]

---

[28] DPP 1(3)(b)(i)(A).
[29] DPP 1(3)(b)(i)(B).
[30] DPP 1(3)(a)(i).
[31] DPP 1(3)(a)(ii).
[32] DPP 1(3)(b)(ii)(A).
[33] DPP 1(3)(b)(ii)(B).
[34] PDPO, s 2(3)(a)
[35] PDPO, ss 35C(1) and 35E(1).
[36] PDPO, s 35C(4).
[37] PDPO, s 35C(2)(a)(i).
[38] PDPO, s 35C(2)(a)(ii).
[39] PDPO, s 35C(2)(b)(i).
[40] PDPO, s 35C(2)(b)(ii).
[41] Guidance on Direct Marketing, paragraph 3.28.
[42] PDPO, s 35J(4).

- that the data user intends to so provide the personal data;[43]
- that the data user may not so provide the data unless the data user has received the data subject's written consent to the intended provision;[44]
- whether the data is provided for gain;[45]
- the kinds of personal data to be provided;[46]
- the classes of persons to which the data is to be provided; [47] and
- the classes of marketing subjects in relation to which the data is to be used.[48]

The data user must also provide a channel that data subjects may use, without charge, to withdraw their consent to the above.[49]

Additionally, a data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.[50]

8. SANCTIONS AND ENFORCEMENT

Generally, the PDPO treats breaches of consent requirements in a similar manner to breaches of other requirements under the ordinance.

As the general basis for processing of personal data under the PDPO is notification rather than consent, in most instances, the approach to enforcement under the PDPO would be for PCPD to issue an enforcement notice.[51] The breach of an enforcement notice under the PDPO gives rise to liability, on a first conviction, to a fine of HK$50,000 and imprisonment for 2 years.[52] A daily penalty of HK$1,000 applies to continued breach of an enforcement notice.[53] On any second or subsequent conviction of breaching an enforcement notice, a fine of HK$100,000 and imprisonment for 2 years.[54] The daily penalty also increases to HK$2,000. [55]

However, the PDPO creates specific offenses for certain forms of misconduct relating to a lack of consent:

8.1. Disclosing personal data without consent

Disclosing personal data obtained from a data user without the data user's consent, with intent to obtain gain in money or property[56] or cause loss in money or other property to the data subject [57] is an offense punishable with a fine of HK$1,000,000 and imprisonment for 5 years.[58]

Disclosing personal data obtained from a data subject without the data subject's consent, with intent to cause harm to the data subject or any family member of the data subject[59] or recklessness as to

---

[43] PDPO, s 35J(2)(a)(i).
[44] PDPO, s 35J(2)(a)(ii).
[45] PDPO, s 35J(2)(b)(i).
[46] PDPO, s 35J(2)(b)(ii).
[47] PDPO, s 35J(2)(b)(iii).
[48] PDPO, s 35J(2)(b)(iv).
[49] PDPO, ss 35C(2)(c) and 35J(2)(c).
[50] PDPO, s 35F(1).
[51] PDPO, s 50.
[52] PDPO, s 50A(1)(a)(i).
[53] PDPO, s 50A(1)(a)(ii).
[54] PDPO, s 50A(1)(b)(i).
[55] PDPO, s 50A(1)(b)(ii).
[56] PDPO, s 64(1)(a).
[57] PDPO, s 64(1)(b).
[58] PDPO, s 64(3).
[59] PDPO, s 64(3A)(a).

whether harm would be caused, or likely to be caused to such persons[60] is punishable with a fine and imprisonment for 2 years.[61] If such harm is caused,[62] then the punishment increases to a fine of HK$1,000,000 and imprisonment for 5 years.[63]

8.2. Using or disclosing personal data for direct marketing purposes without consent

Breaches of consent requirements relating to direct marketing and cross-marketing give rise to liability for a fine of HK$500,000 and imprisonment for 3 years[64] or if personal data is provided in breach of those requirements for gain, a fine of HK$1,000,000 and imprisonment for 5 years.[65]

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

Hong Kong law does not provide a legal basis for processing personal data without consent that is specifically premised on a risk impact assessment, such as the GDPR's "legitimate interests" basis.[66]

As discussed above, the PDPO's data protection framework is based primarily on notification, and accordingly, consent is not generally required for processing of personal data. Further, the PDPO does not expressly require data users to undertake a risk impact assessment in relation to processing of personal data, though note that the DPPs generally require that collection of personal data should be by means which are lawful[67] and fair in the circumstances of the case.[68]

There does not appear to have been any legislative debate on this subject, and a "legitimate interests"-type basis for processing personal data was not raised in the last round of PDPO reform in 2012-2013, or in the proposed reforms tabled by the Constitutional and Mainland Affairs Bureau in January 2020.

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

The PDPO provides a number of specific exemptions from the consent requirement in DPP 3. Under these exceptions, consent would not be required to process personal data for the following purposes:

- preventing or detecting crime if application of DPP 3 would prejudice this objective;[69]
- a purpose relating to the physical or mental health of the data subject if application of DPP 3 would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;[70]
- a purpose required or authorized by or under any enactment or rule of law or by an order of a Hong Kong court;[71]
- a purpose required in connection with any legal proceedings in Hong Kong; [72]

---

[60] PDPO, s 64(3A)(b).
[61] PDPO, s 64(3B).
[62] PDPO, s 64(3C).
[63] PDPO, s 64(3D).
[64] PDPO, ss 35C(5), 35E(4), 35F(3), s 35G(4), s 35J(5)(b), 35K(4)(b), 35L(7), and 35L(6)(b).
[65] PDPO, ss 35J(5)(a), 35K(4)(a), and 35L(6)(a).
[66] See GDPR, Article 6(1)(f).
[67] DPP 1(2)(a).
[68] DPP 1(2)(b).
[69] PDPO, s 58(2).
[70] PDPO, s 59.
[71] PDPO, s 60B(a).
[72] PDPO, s 60B(b).

- a purpose required for establishing, exercising or defending legal rights in Hong Kong; [73]
- news activity;[74]
- preparing statistics and carrying out research, provided that the data is not used for any other purpose and the resulting statistics and/or research are not made available in a form that identifies individual data subjects;[75]
- a due diligence exercise in connection with a proposed business transaction;[76]
- identifying an individual who is reasonably suspected to be, or is, involved in a life-threatening situation if application of DPP 3 would prejudice this objective;[77]
- informing the individual's family members or relevant persons of the individual's involvement in the life-threatening situation if application of DPP 3 would prejudice this objective;[78] and
- the carrying out of emergency rescue operations or provision of emergency relief services if application of DPP 3 would prejudice this objective.[79]

PCPD's administrative practice in relation to the use of publicly available personal data shows some flexibility. The PCPD issued guidance that use of publicly available personal data without notice to or consent by data subjects is permissible, provided that the use does not go beyond the data subject's reasonable privacy expectations.[80] Consent under DPP 3 is required where a reasonable person in the data subject's situation would find the reuse of the data unexpected, inappropriate, or otherwise objectionable, taking into account all factors in the circumstances.[81]

10.1. Health exception (PDPO, s 59) in the context of COVID-19

PCPD has taken a practical stance in relation to the exemption from the consent requirement in Section 59 of the PDPO, which provides that the consent requirement under DPP3 does not apply in situations where failure to disclose personal data would be likely to cause serious harm to the physical health of the data subject or any other individual.

PCPD considers that the right to privacy under the PDPO is not absolute and must be weighed against other competing rights and interests, such as the interest in maintaining public health and, in the context of workplaces, the employer's statutory obligation to ensure a safe workplace for other employees.

In a media statement published on March 21, 2020, PCPD stated that if employers need to collect employees' health data to protect their employees and the wider community, a self-reporting system is preferred to a mandatory system where health data is collected indiscriminately.[82] Employers should seek to process the data in an anonymized manner. Personal Information Collection Statements ("**PICS**") should also be provided when/before collecting employees' personal data to inform them of the data collected and the purposes of collection, and the classes of persons to whom their data may be transferred.

On March 30, 2020, PCPD issued a media statement, entitled "Fight COVID-19 Pandemic Guidelines for Employers and Employees" ("**Pandemic Guidelines**").[83]

---

[73] PDPO, s 60B(c).
[74] PDPO, s 61.
[75] PDPO, s 62.
[76] PDPO, s 63B.
[77] PDPO, s 63C(1)(a).
[78] PDPO, s 63C(1)(b).
[79] PDPO, s 63C(1)(c).
[80] PCPD, "Guidance on Use of Personal Data Obtained from the Public Domain" (August 2013), available at https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_public_domain_e.pdf
[81] PCPD, "Guidance on Use of Personal Data Obtained from the Public Domain," page 4.
[82] PCPD, "Response to media enquiry on privacy issues arising from COVID-19" (March 21, 2020), available at https://www.pcpd.org.hk/english/media/response/enquiry_20200321.html
[83] PCPD, "Fight COVID-19 Pandemic Guidelines for Employers and Employees" (March 30, 2020), available at https://www.pcpd.org.hk/english/news_events/media_statements/press_20200330.html

These Guidelines took a liberal view of disclosures to government, advising that it is permissible for employers to disclose employees' personal health data (e.g., identity, health status, location data, etc.) to the government for the purpose of protecting public health from COVID-19. The data should be solely used for tracking down and treating the infected and tracing their close contacts when pressing needs arise.

The Pandemic Guidelines also address the collection of employees' personal data by employers in the context of COVID-19. The PCPD stressed that the collection and processing of employees' personal data should be specifically related to and used for the purposes of public health and should be limited in both duration and scope as required in the particular situation.

In particular:

- **Body temperature data**: Over the period of the pandemic, it is generally justifiable for employers to collect temperature measurements or limited medical symptoms of COVID-19 information of employees and visitors solely for the purposes of protecting the health of those individuals (and others in the workplace or other premises).
- **Travel history**: There is no general prohibition against collecting this information. It is justifiable for employers to ask for travel data from employees who have returned from overseas, especially those from high-risk areas. Similar to health data, the collection of travel data should be purpose-specific, and minimal data should be collected.

These Guidelines further explained that if an employee contracts COVID-19, the employer may notify other employees, visitors and the property management office etc. without disclosing personally identifiable information of the infected.

There is currently no legal obligation on Hong Kong businesses to notify the Centre for Health Protection ("**CHP**") of the Department of Health or any other authority about any suspected or known COVID-19 cases.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG