ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Singapore

Status of Consent for Processing Personal Data

AUGUST 2022

AUTHORED BY

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Lim Chong Kin

Managing Director, Corporate & Finance, Drew & Napier LLC

David Alfred

Director, Drew & Napier LLC

ACKNOWLEDGEMENTS

Cover photograph by Aditya Chinchure on Unsplash.

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

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

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

Since Singapore's Personal Data Protection Act 2012 ("**PDPA"**)[1] was first passed in November 2012, consent has been the central requirement for collecting, using, or disclosing personal data under Singapore's data protection law.

However, the most recent round of amendments to the PDPA—which were enacted in 2020 and took effect in 2021—brought substantial changes to the original framework adopted in 2012. These changes are characteristic of Singapore's unique ability to "hybridize" its legal system in order to increase compatibility with the legal systems of other jurisdictions and thereby facilitate cross-border data flows and trade.

This report analyzes the respective roles that consent and related provisions like "legitimate interests," "deemed consent by notification," and the "business improvement exception" play in Singapore's data protection framework.

2. CONSENT AND PRIVACY SELF-MANAGEMENT UNDER THE PERSONAL DATA PROTECTION ACT ("PDPA")

The PDPA provides the baseline standard of protection for personal data in Singapore and includes provisions relating to—among others—consent, notification, purpose, access, correction, portability, security, data breach notification, accuracy, retention, and overseas transfers.

The PDPA complements sector-specific legislative and regulatory frameworks, such as the Banking Act and the Insurance Act, and also establishes a national "Do Not Call Registry" – individuals may register their Singapore telephone numbers with the Registry to opt out of receiving unwanted telemarketing messages.

By way of background, the PDPA generally does not apply to the following:

- any individual acting:
  - on a personal or domestic basis;[2]
  - in his/her capacity as an employee with an organization;[3]
- any public agency in relation to the collection, use, or disclosure of personal data;[4]
- personal data in a record that has been in existence for at least 100 years;[5]
- personal data about a deceased individual, except that provisions relating to disclosure (including consent) and security of personal data shall apply in relation to personal data of a deceased individual who has been dead for 10 years or less;[6] and
- "business contact information"[7] – which is defined as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax

[1] Available at https://sso.agc.gov.sg/Act/PDPA2012
[2] PDPA, s 4(1)(a).
[3] PDPA, s 4(1)(b).
[4] PDPA, s 4(1)(c). Collection, use, disclosure, and processing of personal data by public agencies are governed by the Public Sector (Governance) Act 2018 and Singapore Government Instruction Manual on Infocomm Technology and Smart Systems Management. The requirements applicable to public agencies, including those relating to consent, are set out in the Government Personal Data Protection Policies (available at https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection-laws-and-policies).
[5] PDPA, s 4(4)(a).
[6] PDPA, s 4(4)(b).
[7] PDPA, s 4(5).

number and any other similar information about the individual not provided by the individual solely for his personal purposes."[8]

Section 3 of the PDPA states that the purpose of the PDPA is to "govern the collection, use, and disclosure of personal data by organizations in a manner that recognizes the right of individuals to protect their personal data and the needs of organizations to collect, use, and disclose such data."

In relation to consent and lawful processing, the PDPA provides that:

- organizations must not collect, use, or disclose personal data about an individual (i.e., data subject) except:
  - with the consent of the individual;
  - with the deemed consent of the individual; or
  - where required or authorized to do so by the PDPA or any other written law.[9]
- organizations may collect, use, or disclose personal data about an individual only for purposes that:
  - a reasonable person would consider appropriate in the circumstances, and
  - have been notified to the individual (if required under the PDPA).[10]

Following amendments to the PDPA in 2020, the PDPA now contains a number of provisions which allow for collection and use of personal data without consent. These are set out in Schedule 1 ("Collection, use and disclosure of personal data without consent") and Schedule 2 ("Additional bases for collection, use and disclosure of personal data without consent") of the PDPA and cover the following:

- "Vital Interests of Individuals;"
- "Matters Affecting the Public" (including "Public Interest" in the Second Schedule);
- "Legitimate Interests;"
- "Business Asset Transactions;"
- "Business Improvement Purposes;" and
- "Research" (in the Second Schedule).

Additionally, Section 46(1) of the PDPA sets out the requirements with which organizations must comply when obtaining consent under the so-called "**Do Not Call**" provisions.

One significant obligation under the Do Not Call provisions is that an organization must check the Do Not Call Registry before sending a specified message, unless the user or subscriber of the relevant Singapore telephone number has given clear and unambiguous consent in evidential form, or the organization is exempted under the Personal Data Protection (Exemption from s. 43) Order (S 817/2013).

On direct marketing via telephone, PDPC's "Advisory Guidelines on Requiring Consent for Marketing Purposes" – which were issued in May 2015[11] – clarify the interplay between Section 14(2) of the PDPA (which relates to consent for collection, use, or disclosure of personal data) and Section 46(1) of the PDPA (which relates to consent to the sending of a specified message to a Singapore telephone number). Although the two provisions relate to different parts of the PDPA and have slightly different requirements, they are similar in that both establish the key principle that an organization cannot, as a condition of providing a certain item, require an individual to give his/her consent beyond what is reasonable to provide a good or service.

---

[8] PDPA, s 2(1).
[9] PDPA, s 13.
[10] PDPA, s 18.
[11] Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisoryguidelinesonrequiringconsentformarketing8may2015.pdf?la=en

3. ROLE OF THE PERSONAL DATA PROTECTION COMMISSION ("PDPC")

The Personal Data Protection Commission ("**PDPC**") was established on January 2, 2013, to administer and enforce the PDPA. This role subsequently passed to the Infocomm Media Development Authority ("**IMDA**") when it was established in 2016. Concurrently, the PDPC's decision-making powers were delegated to a Commissioner for Personal Data Protection ("**Commissioner**").

3.1. Advisory

The PDPC's stated aim is "to balance the protection of individuals' personal data with organizations' need to use the data for legitimate purposes."[12] To achieve this, the PDPC implements policies relating to personal data protection and develops advisory guidelines[13] to help organizations understand and comply with the PDPA.[14]

Regarding the consent requirements under the PDPA, the PDPC's Advisory Guidelines on Key Concepts in the PDPA ("**Key Concepts Guidelines**")[15] – which were last updated in October 2021 – explain the scope of organizations' obligation under Section 13 of the PDPA and related provisions (which the PDPC refers to as the "**Consent Obligation**").[16]

In recent years, the PDPC's most notable actions have been their efforts to rebalance the role of consent in the PDPA framework by proposing and holding a public consultation on novel exceptions to consent and extension of the role of "deemed consent," which culminated in the 2020 amendments to the PDPA.

Since these amendments took effect, the PDPC's advice to organizations has promoted the new exceptions to consent and "deemed consent" to the extent that it now appears that the PDPC regards these as the primary legal bases for processing personal data under Singapore law and has effectively relegated actual consent (whether express or implied) to a secondary role. For example, the PDPC's Key Concepts Guidelines state:

> "*The PDPA recognizes that organizations need to collect, use, and disclose personal data for reasonable purposes that are articulated in the PDPA through deemed consent and exceptions to the consent obligation. For all other purposes, section 13 of the PDPA provides that organizations are allowed to collect, use or disclose an individual's personal data if the individual gives his consent for the collection, use or disclosure of his personal data.*"[17]

3.2. Sanctions and enforcement

Under the PDPA, the PDPC is empowered to take enforcement actions in response to contravention of various data protection requirements, including the requirement to obtain consent for the collection, use, or disclosure of personal data.[18]

Possible enforcement actions may include giving a direction to the organization to ensure that it complies with the PDPA[19] and/or requiring the organization to pay a financial penalty of up to S$1,000,000.[20] On April 4, 2022, Singapore's Government announced that the maximum financial penalty under the PDPA would increase to the higher of 10% of the organization's annual turnover in Singapore or S$1,000,000 with effect from October 1, 2022.

---

[12] PDPC, "About Us," available at https://www.pdpc.gov.sg/who-we-are/about-us
[13] Available at https://www.pdpc.gov.sg/Guidelines-and-Consultation?type=advisory-guidelines
[14] Available at https://www.pdpc.gov.sg/Guidelines-and-Consultation
[15] Available at https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act
[16] See, generally, Key Concepts Guidelines, Chapter 12.
[17] Key Concepts Guidelines, paragraph 12.1
[18] See, generally, PDPA, Part 9C.
[19] PDPA, s 48I.
[20] PDPA, s 48J.

In general, the PDPC is active in enforcing the PDPA. The PDPC has addressed the PDPA's consent requirements in relation to particular factual scenarios in a number of its published decisions.[21] Some recent published decisions concerning consent requirements include the following:

a. *Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7[22]

A debt recovery business recorded video footage of a visit by its employees to a debtor's premises and subsequently made the footage available online. The company was found to be in breach of its obligation to obtain consent.

b. *H3 Leasing* [2019] SGPDPC 9[23]

A business which rented out motor vehicles made personal data of an individual hirer available online when the individual fell into arrears. The PDPC determined that the company's online disclosure of personal data was not necessary for the purpose of recovering the debt owed to it and hence, that the PDPA's provision on debt collection did not apply. Accordingly, the company was found in breach of its obligation to obtain consent.

c. *German European School Singapore* [2019] SGPDPC 8[24]

A school collected and used a hair sample and the personal data of a student (a minor) in the course of conducting a random drug test. The school was found to have obtained valid consent on the grounds that the student's parents had provided implied consent by notification and by conduct.

4. SECTORAL LEGISLATION

While the PDPA provides the baseline legislation for protection of personal data in Singapore, certain organizations are also subject to sector-specific laws and regulations. The PDPA contains exemptions to accommodate existing regulations and other reasonable situations, and the PDPC also works with sectoral regulators to oversee compliance with personal data protection requirements in their respective domains.

Some statutory provisions require consent to be obtained for collection of information comprising personal data, such as for the conduct of human biomedical research and for handling of human tissue under the Human Biomedical Research Act ("**HBRA**").[25] The Ministry of Health ("**MOH**") has also provided specific guidance to Research Institutions, Institutional Review Boards, Tissue Banks and researchers on the consent obligation for the conduct of human biomedical research and handling of human tissue under the HBRA.[26]

Additionally, certain sectoral legislation contains provisions which permit the sharing of information about individuals without their consent where overriding interests prevail. Within the financial sector, for instance, the Banking Act (Cap. 19) ("**BA**")[27] includes a provision on privacy of customer information which specifically relates to disclosure of customer information.[28] Specifically, banks in Singapore may not disclose customer information except as expressly provided in the BA (in particular, the Third Schedule to the BA).

---

[21] Available at https://www.pdpc.gov.sg/Commissions-Decisions
[22] Available at https://www.singaporelawwatch.sg/Portals/0/Docs/Judgments/2020/[2020]%20SGPDPC%207.pdf
[23] Available at https://www.singaporelawwatch.sg/Portals/0/Docs/Judgments/2019/[2019]%20SGPDPC%209.pdf
[24] Available at https://www.singaporelawwatch.sg/Portals/0/Docs/Judgments/2019/[2019]%20SGPDPC%208.pdf
[25] Available at https://sso.agc.gov.sg/Act/HBRA2015
[26] Available at https://www.moh.gov.sg/docs/librariesprovider5/legislation/guidance-on-appropriate-consent_17-may-2019.pdf
[27] Available at https://sso.agc.gov.sg/Act/BA1970
[28] BA, s 47.

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

The term "consent" is not defined in the PDPA. However, the PDPC's Key Concepts Guidelines clarify that consent may take different forms, including express consent (e.g., in writing or verbally) as well as implied consent (e.g., consent which is implied or inferred from the circumstances).[29]

The PDPA does not expressly require that consent must be freely given. However, such a requirement may be implicit in the meaning of the word "consent." The PDPA also prohibits certain activities that may affect whether consent is freely given, including the use of false or misleading information or deceptive or misleading practices in order to obtain consent.[30]

The PDPA also does not expressly require that consent must be clear and unambiguous, except in the context of consent to receive telemarketing messages (referred to in the PDPA as "specified messages") given by individuals whose telephone number is on the Do Not Call Register.[31] Such consent must also be evidenced in written or other form so as to be accessible for subsequent reference.[32]

5.2. "Deemed consent"

The PDPA includes provisions covering situations where an individual has not given actual consent but is "deemed" by law to have given consent.[33] Consent may be deemed by conduct,[34] by contractual necessity,[35] or by notification.[36]

The concept of "deemed consent" has become essential in the architecture of the PDPA because it offers wide possibilities for extending the scope of the exceptions to consent. In practice, deemed consent under the PDPA is the equivalent of several legal bases unrelated to consent in equivalent legislations, including the GDPR.

5.3. Withdrawal of consent

The PDPA expressly states that organizations may not prohibit individuals from withdrawing consent.[37] Individuals may withdraw consent (including deemed consent) by giving reasonable notice to the organization.[38] On receiving such a notice, the organization must inform the individual of the likely consequences of withdrawing consent.[39]

Once consent is withdrawn, the organization must cease (and cause its data intermediaries and agents to cease) collecting, using, or disclosing personal data, unless collection, use, or disclosure without the individual's consent is required or authorized under the PDPA or another written law.[40]

5.4. Bundled consent

The PDPA prohibits organizations from:

---

[29] Key Concepts Guidelines, paragraphs 12.4 to 12.6.
[30] PDPA, s 14(2).
[31] PDPA, s 43(2)(a).
[32] PDPA, s 43(2)(b).
[33] PDPA, ss 15 and 15A.
[34] PDPA, ss 15(1) and 15(2).
[35] See PDPA, ss 15(3) to 15(9). See also "Deemed consent by contractual necessity" below.
[36] PDPA, s 15A. See "Deemed consent by notification" below.
[37] PDPA, s 16(2). Note that there is an equivalent provision for telemarketing under the Do Not Call provisions (PDPA, s 47(2)).
[38] PDPA, s 16(1). See also PDPA, s 47(1) for telemarketing.
[39] PDPA, s 16(2). See also PDPA, s 47(3) for telemarketing.
[40] PDPA, s 16(4).

- requiring individuals to consent to the collection, use, or disclosure of their personal data as a condition for providing a product or service to the individuals beyond what is reasonable to provide the product or service;[41] and
- obtaining or attempting to obtain consent for collecting, using, or disclosing personal data by providing false or misleading information with respect to the collection, use, or disclosure of the personal data, or using deceptive or misleading practices.[42]

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

Unlike many other data protection laws in the region, the PDPA does not provide for a category of "sensitive" or "special" data.

However, the PDPC has consistently recommended that personal data of a sensitive nature should be subjected to a higher standard of protection.[43] The PDPC has confirmed on multiple occasions that it takes a stricter view of cases where compromised personal data is of a sensitive nature. This approach is recognized in the PDPC's Key Concepts Guidelines, albeit in the specific context of data protection risk/impact assessments required under specific provisions of the PDPA.[44]

The PDPC has released guidelines[45] that an organization may not collect, use, or disclose an individual's National Registration Identity Card ("**NRIC**") number, Birth Certificate number, Foreign Identification Number, or Work Permit number unless such collection, use, or disclosure is required by law or is necessary to establish the individual's identity to a high degree of fidelity. This is in addition to the PDPA's consent requirements in Sections 13 to 17 of the PDPA, notification in Section 20 of the PDPA, and purpose limitation in Section 18 of the PDPA. The guidelines specifically refer to the risk of unintended disclosure with the result that such national identity numbers may be obtained and used for illegal activities such as identity theft and fraud.

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

The PDPA specifically requires organizations that transfer personal data to a country or territory outside Singapore to provide the transferred personal data with, or apply to such data, a standard of protection comparable to that provided by the PDPA.[46]

Under the Personal Data Protection Regulations 2021 ("**PDPR**"),[47] organizations are taken to have satisfied this requirement if they obtain the consent of the individual concerned for the transfer of the individual's personal data to the particular country or territory outside of Singapore.[48]

Consent requirements for cross-border transfer of personal data differ from general consent requirements for collection, use, and disclosure of personal data. Specifically, the PDPR requires that when seeking an individual's consent for transfer of his/her personal data out of Singapore, the organization must, among others, give the individual a "reasonable summary in writing of the extent to which the transferred personal data will be protected to a comparable standard."[49]

---

41 PDPA, s 14(2)(a). Note that there is an equivalent provision for telemarketing under the Do Not Call provisions (PDPA, s 46(1)).

42 PDPA, s 14(2)(b). Note that there is an equivalent provision for telemarketing under the Do Not Call provisions (PDPA, s 46(2)).

43 "Being Accountable to Stakeholders," *DPO Connect* (September 2019), available at https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/Sept-19/Being-Accountable-To-Stakeholders

44 Key Concepts Guidelines, paragraph 12.69(b).

45 PDPC Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers (August 31, 2018), available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf?la=en

46 PDPA, s 26.

47 Available at https://sso.agc.gov.sg/SL/PDPA2012-S63-2021

48 PDPR, regulations 10(2)(a) and 10(2)(b).

49 PDPR, regulation 10(3)(a).

This would implicitly include a list of the countries or territories to which the personal data will be transferred. In practice, save for specifically identified transfers to a particular organization, it would likely be difficult to provide such information in sufficient detail, given that each recipient is likely to implement different ways of protecting the personal data.

8. TRANSPARENCY AND NOTICE

The PDPA requires that when organizations obtain consent for collection, use, and disclosure of personal data, such organizations must inform individuals of the purposes for such collection, use, or disclosure either before or at the time that the data is collected[50] or if it is used for a purpose that was not notified at or prior to collection, before use or disclosure of the personal data for that purpose.[51]

As discussed above, for transfers of personal data outside Singapore, the PDPR also requires organizations to give the individual(s) concerned a reasonable summary of the extent to which the transferred personal data will be protected to a standard comparable to the PDPA.[52]

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

9.1. Background: 2021 amendments to the PDPA

As discussed above, the PDPA was recently amended to include additional circumstances in which organizations may collect, use, and disclose personal data without individuals' consent, specified in the First and Second Schedules to the PDPA.[53]

These amendments were initiated by the PDPC on July 27, 2017, with the launch of a public consultation on "Approaches to Managing Personal Data in the Digital Economy."[54] After receiving feedback from the the public consultation, the PDPC published a response in February 2018.[55] The relevant amendments came into force via the Personal Data Protection (Amendment) Act 2020 (Commencement) Notification 2021, which was gazetted on January 29, 2021. Accompanying regulations have also been introduced to support these amendments, including the PDPR in 2021.

The amendments introduced, among others, two new provisions—"deemed consent by notification" and "legitimate interests"—which reflect the need to provide organizations with meaningful alternatives to consent that are balanced with appropriate safeguards, especially to address situations where consent cannot be easily or meaningfully obtained, and where organizations can demonstrate an appropriate justification for their processing of personal data, taking into consideration any possible risks to the individual.

9.2. Legitimate interests of organizations

The new Part 3 to the First Schedule now enables organizations to collect, use, or disclose personal data in circumstances where such collection, use, or disclosure is in the legitimate interests of the organization or other person.

The PDPA provides for two distinct categories of legitimate interests, outlined below.

---

50 PDPA, s 20(1)(a).
51 PDPA, s 20(1)(b).
52 PDPR, regulations 10(2)(a) and 10(2)(b).
53 PDPA, s 17.
54 Available at https://www.pdpc.gov.sg/guidelines-and-consultation/2017/07/public-consultation-for-approaches-to-managing-personal-data-in-the-digital-economy
55 Available at https://www.pdpc.gov.sg/news-and-events/announcements/2018/02/pdpcs-response-to-public-consultation-on-approaches-to-managing-personal-data-in-the-digital-economy

a. General legitimate interests provision

The first category is a general, open-ended legitimate interests provision,[56] which permits organizations to collect, use, or disclose personal data where:

- the collection, use, or disclosure is in the legitimate interests of the organization or another person;[57] and
- such legitimate interests outweigh any adverse effect on the individual.[58]

The Key Concepts Guidelines define "legitimate interests" generally as "any lawful interests of an organization or other person (including other organizations)."[59] This provision could therefore cover a wide range of different circumstances and purposes, including:

- detecting and preventing illegal activities, such as fraud and money-laundering, or threats to physical, IT, and network security;
- preventing misuse of services; and
- conducting corporate due diligence.[60]

Prior to collecting, using, or disclosing personal data on this basis, organizations must conduct an assessment[61] (very similar to the "balancing test" under Article 6 of the GDPR) "to ensure that the interests of individuals are protected."[62] Specifically, organizations must:

- identify any adverse effect that the proposed collection, use, or disclosure of personal data is likely to have on the individual;[63] and
- implement measures to eliminate, reduce the likelihood of, and/or mitigate any adverse effect on the individual.[64]

Organizations seeking to rely on legitimate interests must also be able to identify the benefits arising from collection, use, or disclosure of personal data on this ground, which should not be speculative but may be tangible (e.g., increased business efficiency and cost savings) or intangible (e.g., improved customer experience).[65]

Annex C to the Key Concepts Guidelines also contains a checklist which provides non-binding guidance on relevant factors to include in the risk/impact assessment.[66]

These include:

- the sensitivity of the personal data;
- the reasonableness of the purposes for collection, use, and/or disclosure of the data;
- the likely impact to the individual; and
- possible mitigation measures.

The PDPA does not include an express requirement for organization to document their assessments. However, the Key Concepts Guidelines require that organizations document both their assessments

---

[56] PDPA, First Schedule, Part 3, paragraph 1.
[57] PDPA, First Schedule, Part 3, paragraph 1(1)(a).
[58] PDPA, First Schedule, Part 3, paragraph 1(1)(b).
[59] Key Concepts Guidelines, paragraph 12.56.
[60] Key Concepts Guidelines, paragraph 12.63.
[61] PDPA, First Schedule, Part 3, paragraph 1(2)(a).
[62] Key Concepts Guidelines, paragraph 12.57.
[63] PDPA, First Schedule, Part 3, paragraph 1(3)(a).
[64] PDPA, First Schedule, Part 3, paragraph 1(3)(b).
[65] Key Concepts Guidelines, paragraph 12.57.
[66] PDPC, "Assessment Checklist for Legitimate Interests Exception" available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-C--Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.pdf?la=en

and any steps that they have taken to mitigate risks and provide this documentation to the PDPC when required. [67]

Organizations are also required to provide individuals with reasonable access to information about organizations' collection, use and/or disclosure of personal data for the individuals' legitimate interests (i.e., to disclose the organizations' reliance on the legitimate interests exception and the situation or purpose that qualifies as a legitimate interest).[68]

b. General legitimate interests provisions

The second category is a closed list of legitimate interests provisions, which permit organizations to collect, use, and/or disclose personal data where necessary for a number of specific situations, without requiring organizations to obtain consent or undertake a risk impact assessment.[69]

This specific situations recognized in this category include collection, use, and disclosure of personal data:

- where necessary for:
  - "evaluative purposes"[70] (for instance, determining the suitability or qualifications of the individual for appointment, employment, promotion, or removal from employment or office[71]);
  - investigations or proceedings;[72]
  - recovery of a debt owned by the individual;[73]
  - payment of a debt owed to the individual;[74]
  - provision of legal services by the organization to another person;[75]
  - obtaining legal services;[76]
  - credit reporting;[77] or
  - manage a private trust or benefit plan;[78]
- to provide a service to an individual (*B*) for *B*'s personal or domestic purposes, where *B* has provided the personal data of another individual (*A*) to enable the organization to provide this service;[79]
- of an individual, where that individual's personal data is included in a document that was produced in the course, and for the purposes, of the individual's employment, business, or profession,[80] and the collection, use, or disclosure is for a purpose that is consistent with the purpose for which the document was produced; [81] or
- where reasonable for the purposes of, on in relation to, entering into[82] or terminating:[83]
  - an employment relationship with the individual; or

---

[67] Key Concepts Guidelines, paragraph 12.62.
[68] PDPA, First Schedule, Part 3, paragraph 1(2)(b). Note that they Key Concepts Guidelines clarify that this does not mean that organizations must disclose their risk/impact assessments to individuals.
[69] PDPA, First Schedule, Part 3, paragraphs 2 to 10.
[70] PDPA, First Schedule, Part 3, paragraph 2.
[71] PDPA, s 2(1).
[72] PDPA, First Schedule, Part 3, paragraph 3.
[73] PDPA, First Schedule, Part 3, paragraph 4(a).
[74] PDPA, First Schedule, Part 3, paragraph 4(b).
[75] PDPA, First Schedule, Part 3, paragraph 5.
[76] PDPA, First Schedule, Part 3, paragraph 5.
[77] PDPA, First Schedule, Part 3, paragraph 6.
[78] PDPA, First Schedule, Part 3, paragraph 7.
[79] PDPA, First Schedule, Part 3, paragraph 8.
[80] PDPA, First Schedule, Part 3, paragraph 9(a).
[81] PDPA, First Schedule, Part 3, paragraph 9(b).
[82] PDPA, First Schedule, Part 3, paragraph 10(a).
[83] PDPA, First Schedule, Part 3, paragraph 10(b).

- the appointment of an individual to any office.

9.3. "Deemed consent by notification"

The recent amendments to the PDPA also introduced a new provision on "deemed consent by notification" legal basis to collect, use, or disclose an individual's personal data.[84]

As with "legitimate interests" in Part 3 of the First Schedule to the PDPA, organizations seeking to rely on deemed consent by notification must implement a risk impact assessment. Specifically, to rely on this provision, an organization must:

- take reasonable steps to bring to the individual's attention:
  - the organization's intention to collect, use, or disclose the individual's personal data;[85]
  - the purpose for which the organization will collect, use, or disclose the data;[86] and
  - a reasonable period within which the individual may notify the organization that the individual does not consent to the proposed collection, use, or disclosure, and a reasonable manner by which the individual may do so;[87]
- conduct an impact assessment to determine that that the proposed collection, use, or disclosure of the personal data is not likely to have an adverse effect on the individual;[88] and
- comply with any other specified requirements.[89]

Regulation 14 of the PDPR provides detailed prescriptions on how organization should assess the impact of the proposed collection, use or disclosure of personal data. The assessment must cover all of the following information:

- the types and volume of personal data to be collected, used or disclosed;
- the purpose or purposes for which the personal data will be collected, used, or disclosed;
- the method or methods by which the personal data will be collected, used, or disclosed;
- the mode by which the individual will be notified of the organization's proposed collection, use or disclosure (as the case may be) of the individual's personal data;
- the period within which, and the mode by which, the individual may notify the organization that the individual does not consent to the organization's proposed collection, use or disclosure (as the case may be) of the individual's personal data;
- the rationale for the period and mode mentioned in the preceding paragraph.

The organization must retain a copy of its assessment throughout the period that the organization collects, uses, or discloses personal data about the individual under this section of the PDPA.

10. COLLECTING, PROCESSING, AND SHARING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

10.1. Business improvement purposes

Broadly, this exception permits an organization and its related corporation to share data for certain purposes (termed "relevant purposes" in the PDPA),[90] namely:

---

[84] PDPA, s 15A.
[85] PDPA, s 15A(4)(b)(i).
[86] PDPA, s 15A(4)(b)(ii).
[87] PDPA, s 15A(4)(b)(iii).
[88] PDPA, s 14A(4)(a). PDPA, s 15A(5) expands on the requirements for the impact assessment.
[89] PDPA, s 14A(4)(c).
[90] PDPA, First Schedule, Part 5, paragraph 1(1).

- improving, enhancing, or developing goods and services or methods and processes;[91]
- learning about and understanding the behavior and preferences of individuals in relation to goods and services ("**modeling**");[92]
- identifying goods or services that may be suitable for individuals or personalizing or customizing any such goods or services for individuals ("**personalization**").[93]

The requirements for such sharing for a relevant purpose are that:

- the relevant purpose in question cannot reasonably be achieved without the collection, use, or disclosure of the personal data in an individually identifiable form;[94]
- a reasonable person would consider the sharing of the personal data for the relevant purpose to be appropriate in the circumstances;[95] and
- the organization and its related corporation are bound by any contract, agreement, or binding corporate rules requiring the recipient of the personal data to implement and maintain appropriate safeguards for the personal data.[96]

Additionally, in cases of data sharing for relevant purposes of modeling or personalization, then data sharing is only permitted if:

- the organization that discloses the data collected from individuals who were its existing customers at the time of collection;[97] and
- when the data is disclosed, those individuals are also prospective or existing customers of the recipient corporation.[98]

For an organization to *use* personal data for a relevant purpose, the following requirements apply:

- the relevant purpose for which the organization uses the personal data cannot reasonably be achieved without the use of the personal data in an individually identifiable form;[99] and
- a reasonable person would consider such use of personal data to be appropriate in the circumstances.[100]

10.2. Deemed consent by contractual necessity

Unlike other data protection laws in the region, the PDPA does not provide an exception to consent requirements, or distinct legal basis, for performance of a contract between the individual and the organization.

However, he recent amendments to the PDPA introduced new provisions on deemed consent by contractual necessity (Sections 15(3) to 15(9) of the PDPA), which serve a similar function to exceptions/ legal bases for performance of a contract in other laws.

Under the relevant provisions of the PDPA, where an individual (*P*) provides personal data to an organization (*A*) with a view to entering into a contract with *A*, *P* is deemed to consent to:

---

[91] PDPA, First Schedule, Part 5, paragraph 1(2)(a)-(b).
[92] PDPA, First Schedule, Part 5, paragraph 1(2)(c).
[93] PDPA, First Schedule, Part 5, paragraph 1(2)(d).
[94] PDPA, First Schedule, Part 5, paragraph 1(3)(a).
[95] PDPA, First Schedule, Part 5, paragraph 1(3)(b).
[96] PDPA, First Schedule, Part 5, paragraph 1(3)(c).
[97] PDPA, First Schedule, Part 5, paragraph 1(5)(a). An "**existing customer**" is an individual who purchases, hires or uses, or has purchased, hired, or used, any goods or services provided by the corporation (PDPA, First Schedule, Part 5, paragraph 2).
[98] PDPA, First Schedule, Part 5, paragraph 1(5)(b). A "**prospective customer**" is an individual who, at the relevant time, has expressed an interest in, or is conducting negotiations with a view to, purchasing, hiring, or using any goods or services provided by the corporation (PDPA, First Schedule, Part 5, paragraph 2).
[99] PDPA, First Schedule, Part 5, paragraph 1(4)(a).
[100] PDPA, First Schedule, Part 5, paragraph 1(4)(b).

- the disclosure of that personal data by *A* to another organization (*B*);[101]
- the collection and use of that personal data by *B*;[102] and
- the disclosure of that personal data by *B* to another organization,[103]

where reasonably necessary for the conclusion of the contract between *P* and *A*.

Similarly, where an individual (*P*) enters into a contract with an organization (*A*) and provides personal data to *A* pursuant to, or in relation to, that contract, *P* is deemed to consent to:

- the disclosure of that personal data by *A* to another organization (*B*), where the disclosure is reasonably necessary for the performance of the contract between *P* and *A* or the conclusion of a contract between *A* and *B* which is entered into on *P*'s request or which a reasonable person would consider to be in *P*'s interest;[104]
- the collection and use of that personal data by *B*;[105]
- the disclosure of that personal data by *B* to another organization.[106]

This rule does not affect any provision of the contract between *P* and *A* that specifies or restricts:

- the personal data provided by *P* that *A* may disclose to another organization;[107] or
- the purposes for which *A* may disclose the personal data provided by *P* to another organization.[108]

10.3. Research purpose

An individual's personal data may be used[109] or disclosed[110] without consent for a research purpose (including historical or statistical research) if:

- the research purpose cannot reasonably be accomplished unless the personal data is used in an individually identifiable form;
- there is a clear public benefit to using the personal data for the research purpose;
- the results of the research will not be used to make any decision that affects the individual; and
- in the event that the results of the research are published, the organization publishes the results in a form that does not identify the individual.

An individual's personal data may also be collected, used, or disclosed without consent if such collection, use, or disclosure is solely for archival or historical purposes, if a reasonable person would not consider the personal data to be too sensitive to the individual to be collected, used, or disclosed at the proposed time.[111]

These general provisions are combined with sectoral provisions. Thus, for instance, the PDPA does not expressly cover health research, but the HBRA governs various aspects of biomedical research in Singapore, including the taking of consent, and would supersede the PDPA in the event of any inconsistency.[112]

---

[101] PDPA, s 15(3)(a).
[102] PDPA, s 15(3)(b).
[103] PDPA, s 15(3)(c).
[104] PDPA, s 15(6)(a).
[105] PDPA, s 15(6)(b).
[106] PDPA, s 15(6)(c).
[107] PDPA, s 15(9)(a).
[108] PDPA, s 15(9)(b).
[109] PDPA, Second Schedule, Part 2, Division 3.
[110] PDPA Second Schedule, Part 3, Division 2.
[111] PDPA, First Schedule, Part 2, paragraph 4.
[112] PDPA, s 4(6).

10.4. Carrying out a task in the public interest and matters affecting the public

Several provisions of the PDPA address collection, use, and disclosure of personal information without consent for the purpose of carrying out tasks in the public interest as well as other matters affecting the public.

Firstly, an individual's personal data may be *collected*, *used*, or *disclosed* without the individual's consent if such collection, use, or disclosure is in the national interest.[113] The PDPA's definition of the term "national interest" includes national defense, national security, public security, the maintenance of essential services, and the conduct of international affairs.[114]

Secondly, an individual's personal data may be *used* without the individual's consent if the personal data was disclosed by a public agency, and the organization's use of the personal data is consistent with the purpose of the disclosure by the public agency.[115]

Thirdly, an individual's personal data may also be *disclosed* to a public agency without the individual's consent where the disclosure is necessary in the public interest.[116]

10.5. Law enforcement, defense, or national security

An individual's personal data may be disclosed to a prescribed law enforcement agency without the individual's consent, upon production of written authorization signed by the head or director of that prescribed law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.[117]

Where an organization discloses personal data to a prescribed law enforcement agency under the PDPA, the organization must not inform the individual.[118]

10.6. Publicly available personal data

An individual's personal data that is publicly available may be collected, used, or disclosed without the individual's consent.[119] Personal data is considered publicly available under the PDPA if it is generally available to the public—this includes personal data collected by reasonably expected means at a location or event that is open to the public and at which the individual appears.[120]

10.7. Vital interests of the individual

Part 1 to the First Schedule of the PDPA provides 4 situations in which an individual's personal data may be collected, used, or disclosed without consent in relation to the vital interests of individuals.

Firstly, such collection is permitted where necessary for any purpose which is clearly in the individual's interests, and:

- consent for the collection, use, or disclosure cannot be obtained in a timely way;[121] or
- the individual would not reasonably be expected to withhold consent.[122]

---

[113] PDPA, First Schedule, Part 2, paragraph 2.
[114] PDPA, s 2(1).
[115] PDPA, Second Schedule, Part 2, Division 1.
[116] PDPA, Second Schedule, Part 3, Division, paragraph 1.
[117] PDPA, Second Schedule, Part 3, paragraph 4.
[118] PDPA, s 21(4).
[119] PDPA, First Schedule, Part 2, paragraph 1.
[120] PDPA, s 2(1).
[121] PDPA, First Schedule, Part 1, paragraph 1(1)(a).
[122] PDPA, First Schedule, Part 1, paragraph 1(1)(b).

Where the organization collects, uses, or discloses personal data about the individual pursuant to the above conditions, the organization must, as soon as is practicable, notify the individual of the collection, use, or disclosure and the purpose for the collection, use or disclosure.[123]

Secondly, such collection is permitted where necessary to respond to an emergency that threatens the life, health, or safety of the individual or another individual.[124]

Thirdly, such collection is permitted where:

- consent for the collection, use, or disclosure cannot be obtained in a timely way;[125] and
- there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected.[126]

Finally, such collection is permitted where it is for the purpose of contacting the next-of-kin or a friend of any injured, ill, or deceased individual.[127]

The PDPC has clarified in an advisory notice on contact tracing for COVID-19 that during the COVID-19 pandemic, relevant personal data can be collected, used, and disclosed without consent in the event of a COVID-19 case to carry out contact tracing and other response measures, as this is necessary to respond to an emergency that threatens the life, health, or safety of other individuals.[128]

10.8. Business asset transactions

Broadly, this exception permits use and disclosure of personal data without consent in the context of a prospective or finalized transaction for merger or acquisition between two or more organizations.[129]

Prospective parties to such a transaction may share personal data without consent where necessary for the purpose of determining whether to proceed with the transaction,[130] and where the relevant parties have entered into an agreement only to use the shared data for this purpose.[131]

Once the relevant parties have entered into the transaction, they must notify affected individuals of the transaction and of the disclosure of those individuals' personal data,[132] and the parties to whom personal data is disclosed may only use or disclose it for the purpose(s) for which the original owner would have been entitled to use or disclose the data.[133]

If the transaction does not proceed or is not completed, then the parties to whom the personal data is disclosed must destroy or return the data.[134]

10.9. Others

The collection, use, or disclosure of an individual's personal data without consent is also permitted where collection, use, or disclosure is for artistic or literary purposes[135] or is undertaken by a news organization solely for its news activity.[136]

---

123 PDPA, First Schedule, Part 1, paragraph 1(2).
124 PDPA, First Schedule, Part 1, paragraph 2.
125 PDPA, First Schedule, Part 1, paragraph 3(a).
126 PDPA, First Schedule, Part 1, paragraph 3(b).
127 PDPA, First Schedule, Part 1, paragraph 4.
128 PDPC, "Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry" (4 January 2022), available at https://www.pdpc.gov.sg/help-and-resources/2021/05/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing
129 PDPA, First Schedule, Part 4, paragraph 3.
130 PDPA, First Schedule, Part 4, paragraphs 1(3)(a), 2(2)(a)(i), and 2(2)(b)(i).
131 PDPA, First Schedule, Part 4, paragraphs 1(3)(b), 2(2)(a)(ii), and 2(2)(b)(ii).
132 PDPA, First Schedule, Part 4, paragraphs 1(4)(c) and 2(3)(c).
133 PDPA, First Schedule, Part 4, paragraphs 1(4)(a) and 2(4).
134 PDPA, First Schedule, Part 4, paragraphs 1(5) and 2(3)(a).
135 PDPA, First Schedule, Part 2, paragraph 3.
136 PDPA, First Schedule, Part 2, paragraphs 5 and 6.

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