ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Malaysia

Status of Consent for Processing Personal Data

JULY 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

Deepak Pillai

Partner, Christopher & Lee Ong

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Catherine Shen.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION 1

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PDPA 2

2.1. PDPA amendments 2

3. SECTORAL LAWS AND REGULATIONS 3

3.1. Banking and financial services sectors 3

3.2. Healthcare sector 3

4. PERSONAL DATA PROTECTION CODES OF PRACTICE ("PDP CODE OF PRACTICE") 3

5. CONDITIONS FOR CONSENT 4

5.1. Definition and forms of consent 4

5.2. Withdrawal of consent 5

5.3. Bundled consent 5

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA 5

6.1. Children 6

6.2. Cookie, Internet of Things, online tracking 6

6.3. Direct marketing 6

6.4. Biometric and genetic data 7

6.5. Financial information 7

6.6. Statistics and research 8

6.7. Pseudonymized data 8

6.8. Location data 8

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS 8

8. TRANSPARENCY AND NOTICE 9

9. SANCTIONS AND ENFORCEMENT 9

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT 10

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

11.1. Collecting, using, and disclosing non-sensitive personal data 10

a. "Vital interests" 10

11.2. Collecting, using, and disclosing sensitive personal data 11

11.3. Transferring personal data across borders without consent 12

11.4. Exemptions from the General Principle 12

11.5. Sectoral regulations 13

11.6. Rule of interpretation 13

11.7. COVID-19 14

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Malaysia'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 Personal Data Protection Act 2010 ("**PDPA**")[1] is the main data protection legislation in Malaysia and is enforced and administered by the Personal Data Protection Commissioner ("**PDP Commissioner**").

The 7 Data Protection Principles ("**PDP Principles**"), which are set out in Sections 6 to 12 of the PDPA, establish the default rules governing collection, use, and disclosure of personal data.[2]

The **General Principle**:

- prohibits a data user[3] (i.e., data controller) from processing[4] personal data[5] without the consent of a data subject; and
- requires that the processing of personal data must be:
  - for a lawful purpose which is:
    - directly related to an activity of the data user; or
    - necessary or directly related to the purpose for which personal data was collected; and
  - not excessive in relation to the purpose for which it was collected.[6]

The **Notice and Choice Principle** requires a data user to:

- notify the data subject of several matters relating to the personal data that is being processed by or on behalf of the data user; and
- provide means of choice to the data subject.[7]

The **Disclosure Principle** prohibits the disclosure of a data subject's personal data:

- for any purpose other than the purpose that was disclosed at the time of collection, or a purpose directly related to that purpose; or
- to any party other than the class of third parties disclosed to the data subject under the Notice and Choice Principle.[8]

The **Security Principle** requires data users to take measures to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, and alteration or destruction during its processing.[9]

---

[1] Available at https://www.pdp.gov.my/jpdpv2/akta-709/personal-data-protection-act-2010/

[2] PDPA, s 5.

[3] Note that a "**data user**" is defined as a person who alone, jointly, or in common with other persons processes any personal data, has control over, or authorizes the processing of personal data (PDPA, s 4).

[4] Note that "**processing**" is broadly defined under the PDPA and includes, among others, the collection of personal data (PDPA, s 4). Therefore, the requirement to obtain consent under the General Principle would apply at the point of initial collection.

[5] "**Personal data**" is defined as any information in respect of commercial transactions which: (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information, whether alone or in combination with other information (PDPA, s 4). Note that information processed for the purpose of credit reporting is excluded from this definition.

[6] PDPA, s 6.

[7] PDPA, s 7.

[8] PDPA, s 8.

[9] PDPA, s 9.

The **Retention Principle** provides that personal data should not be retained for longer than necessary to fulfill the purpose for which it was collected and requires the data user to destroy or permanently delete all personal data which is no longer required.[10]

The **Data Integrity Principle** requires a data user to take steps to ensure that all personal data is accurate, complete, not misleading, and kept up to date.[11]

The **Access Principle** confers on data subjects a right of access to their own personal data and to correct it if it is inaccurate, incomplete, misleading, or outdated.[12]

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PDPA

Consent plays a central role in the PDP Principles and is the default basis for processing personal data under the PDPA.

Pursuant to the General Principle and Notice and Choice Principle, data users are prohibited from processing a data subject's personal data unless they inform the data subject how they will process the data, and the data subject consents to the processing.

However, the PDPA recognizes certain exceptions where personal data can be processed without the consent of the data subject. A data user may process personal data without the data subject's consent if the processing falls under one of the types of processing considered "necessary" under Section 6(2) of PDPA or if one of the exceptions under Section 45 of the PDPA applies (see below).

2.1. PDPA amendments

The Malaysian Government has not made any public statements explaining the rationale for including consent-based provisions in data protection law. However, when the PDPA was first drawn up in 1998, then-Secretary-General of the Ministry of Energy, Communications and Multimedia, Datuk Noraizah Abdul Hamid announced that Malaysia would be enacting a comprehensive data protection law based on the OECD Guidelines and the EU Data Protection Directive, modelled on legislation in the UK, Hong Kong SAR, and New Zealand.[13]

Since then, there has been discussion in Malaysia as to the real value of consent. The main criticisms against the current notice and consent model are that it has failed to provide data subjects with real choices in managing their data, and that it places an undue burden on data subjects to read through and understand privacy notices. Another argument raised in the discussion is that existing notice and consent mechanisms are ineffective and inappropriate in the context of increased personal data collection through ambient computing devices. Discussion on these issues has brought attention to alternatives to the consent model and the need to provide greater protection to the rights of data subjects.

Most recently, in February 2020, the PDP Commissioner issued a public consultation paper, Public Consultation Paper No. 01/2020 on Review of the PDPA ("**Public Consultation Paper**"),[14] which identifies general areas where the PDPA may need to be amended. One such area is Section 6 of the PDPA, which outlines the PDPA's consent requirements. The Public Consultation Paper proposes to

---

[10] PDPA, s 10.

[11] PDPA, s 11.

[12] PDPA, s 12.

[13] Md. Toriqul Islam, Mohammad Ershadul Karim, *A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia*, Sejarah: Journal of History Department, University of Malaya: No. 28 (2) 2019: 169-186, available at https://www.researchgate.net/publication/338689408_A_BRIEF_HISTORICAL_ACCOUNT_OF_GLOBAL_DATA_PRIVACY_REGULATIONS_AND_THE_LESSONS_FOR_MALAYSIA

[14] Available at https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf

retain the PDPA's existing consent-based model but provide greater clarity as to the conditions for consent.

Additionally, in February 2021, the Malaysian Government launched the MyDigital initiative and the Malaysia Digital Economy Blueprint ("**MDEB**"),[15] which set out plans for digital transformation and stimuli to bolster Malaysia's digital economy. According to the MDEB, the Malaysian Government aims to review the PDPA by 2025. It remains to be seen whether this review will reconsider the role of consent, notice, and choice in Malaysia's personal data protection framework.

3. SECTORAL LAWS AND REGULATIONS

3.1. Banking and financial services sectors

The Financial Services Act 2013 ("**FSA**")[16] and the Islamic Financial Services Act 2013 ("**IFSA**")[17] contain banking secrecy provisions which prohibit a financial institution or any of its any directors, officers, or agents from disclosing any document or information relating to the affairs or account of any customer of the financial institution to another person.

Disclosures of customer information are only permissible where the disclosure falls within the list of permitted disclosures under Schedule 11 of, respectively, the FSA or the IFSA[18]—for example, where permitted by the customer.[19]

3.2. Healthcare sector

Generally, the Private Healthcare Facilities and Services Act 1998[20] and its subordinate regulations provide for the confidentiality of patient data.

In addition, medical practitioners registered under the Medical Act 1971 are also required to comply with regulations, codes, and guidelines issued by the Malaysian Medical Council ("**MMC**"),[21] which has issued several ethical codes and guidelines relating to the issue of consent and confidentiality.[22]

In particular, the MMC's Confidentiality Guidelines provide that patients have the right to expect that their personal data will not be disclosed by a medical practitioner in the course of the practitioner's professional duties, unless the patient in question consents to disclosure of the data.[23]

4. PERSONAL DATA PROTECTION CODES OF PRACTICE ("PDP CODE OF PRACTICE")

Pursuant to Sections 21 and 23 of the PDPA, the PDP Commissioner has approved and registered seven sector-specific Personal Data Protection Codes of Practice ("**PDP Code of Practice**"), which take into account the industry practices of the specific sector and set out more detailed requirements to be met in order to comply with the PDPA:

---

[15] Available at https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf
[16] Available at https://www.bnm.gov.my/documents/20124/35ed2b4c-1995-f91d-3891-75d69d247d55
[17] Available at https://www.bnm.gov.my/documents/20124/8102422b-e6dd-d149-8db0-e3637e89ed5c
[18] FSA, ss 133 and 134; IFSA, ss 145 and 146. See also the Central Bank (*Bank Negara Malaysia*, or "**BNM**")'s Policy Document on Management of Customer Information and Permitted Disclosure which sets out further conditions that must be complied with in relation to the list of permitted disclosures set out in Schedule 11 of the FSA and the IFSA, respectively.
[19] FSA, Schedule 11, paragraph 1; IFSA, Schedule 11, paragraph 1.
[20] Available at https://www.moh.gov.my/index.php/database_stores/attach_download/317/27
[21] See Medical Act 1971, s 29(1).
[22] The full list of ethical codes and guidelines issued by the MMC is available at https://mmc.gov.my/laws-regulations/
[23] The MMC's Confidentiality Guidelines are available at https://mmc.gov.my/wp-content/uploads/2019/11/Confidentiality-guidelines.pdf

- **Code of Practice for the Insurance and Takaful Industry**[24] – which applies to all insurance company/takaful operators licensed under the FSA or the IFSA, and insurance/takaful intermediaries;
- **Code of Practice for the Banking and Financial Sector**[25] – which applies to all banks and financial institutions licensed under the FSA, IFSA, and the Development Financial Institution Act 2002;
- **Code of Practice for the Aviation Sector**[26] – which applies to all licensees and/or permit holders under the Malaysian Aviation Commission Act 2015;
- **Code of Practice for the Communications Sector**[27] – which applies to licensees under the Communications and Multimedia Act 1998;
- **Code of Practice for the Utilities Sector (Electricity)**[28] – which applies to Tenaga Nasional Berhad, Syarikat SESCO Berhad, and Sabah Electricity Sdn. Bhd;
- **Code of Practice for the Utilities Sector (Water)**[29] – which applies to water utilities companies specifically listed under the Personal Data Protection (Class of Data Users) Order 2013;[30] and
- **Code of Practice for Private Hospitals in the Healthcare Industry**[31] – which applies to all private healthcare facilities licensed as private hospitals under the Private Healthcare Facilities and Services Act 1998.

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

Neither the PDPA nor its subsidiary regulations provide a definition of "consent." The PDPA also does not contain any express requirements that consent must be freely given, affirmative, clear, or unambiguous.[32]

Further guidance on consent requirements is instead found in the Personal Data Protection Regulations 2013 ("**PDP Regulations**"),[33] which clarify that:

---

[24] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Code_of_Practice_Insurance_and_Takaful_2016.r1.pdf

[25] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/170816-ABM-Code-Of-Practice-CLOcv04-FINAL_CLEAN.pdf

[26] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Code_of_Practice_For_Aviation_Sector.pdf

[27] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP-1.pdf

[28] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/COP-English-JUNE-2016-13072016-amendment-clean-copy-to-JPDM.pdf

[29] Available at https://www.pdp.gov.my/jpdpv2/assets/2022/02/COP_CODE-OF-PRACTICE-Personal-Data-Protection-Water.pdf

[30] These data users include Air Kelantan Sdn Bhd; LAKU Management Sdn. Bhd.; Perbadanan Bekalan Air Pulau Pinang Sdn. Bhd.; Syarikat Bekalan Air Selangor Sdn. Bhd.; Syarikat Air Terengganu Sdn. Bhd.; Syarikat Air Melaka Sdn. Bhd.; Syarikat Air Negeri Sembilan Sdn. Bhd.; Syarikat Air Darul Aman Sdn. Bhd.; Pengurusan Air Pahang Berhad.; Lembaga Air Perak.; Lembaga Air Kuching.; Lembaga Air Sibu.; Pengurusan Air Selangor Sendirian Berhad.

[31] Available at https://www.pdp.gov.my/jpdpv2/assets/2022/02/COP_-CODE-OF-PRACTICE-FOR-PRIVATE-HOSPITALS-APHM.pdf

[32] However, the PDP Code of Practice for Private Hospitals in the Healthcare Industry requires "explicit consent" to be freely given, specific and unambiguous (see "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA" below).

[33] Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Peraturan-peraturan_Perlindungan_Data_Peribadi.pdf

- consent can take any form that can be recorded and that the data user can properly maintain;[34] and
- consent for a specific form of processing of personal data must be distinguishable from other matters in the consent form.[35]

Apart from the above, the PDPA and its subsidiary regulations make no further mention of other forms that consent may take (e.g., express, implied, deemed consent) under the PDPA.

However, it appears from the PDP Codes of Practice that both express and implied consent (in written or verbal form) *may* be acceptable forms of consent under the PDPA, provided that the consent is capable of being recorded and maintained by the data user.

Specifically, the PDP Code of Practice for the Banking and Financial Sector provides that the following forms of consent are acceptable under the PDPA:

- signatures or ticks indicating consent;
- opt-in consent;
- deemed consent; and
- verbal consent.[36]

Further, the PDP Code of Practice for the Banking and Financial Sector defines "deemed consent" to refer to instances where the data subject:

- does not object to the data user processing his/her personal data;
- proceeds to volunteer his/her personal data; or
- proceeds/continues to use the facility/service of the data user.[37]

A similar position is also found in the other PDP Codes of Practice, including those for the Utilities (Electricity) Sector and the Communications Sector.

5.2. Withdrawal of consent

The PDPA provides that a data subject may withdraw his/her consent to the processing of his/her personal data by giving written notice to the data user. Upon receiving such a notice, the data user must cease processing the data subject's personal data.[38]

Failure of the data user to comply with the notice of withdrawal of consent is a criminal offense punishable with a fine not exceeding RM100,000 and/or imprisonment for a term not exceeding 1 year.[39]

5.3. Bundled consent

Under the PDPA, there are no express provisions that prohibit the use of "bundled consent" or making access to a service conditional on users' consent to specific collection/use of their personal data.

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The PDPA recognizes a subset of personal data known as "sensitive personal data," which comprises any personal data relating to a data subject's:

- physical or mental health or condition,

---

[34] PDP Regulations 2013, Regulation 3(1).
[35] PDP Regulations 2013, Regulation 3(2).
[36] PDP Code of Practice for the Banking and Financial Sector, paragraph 3.1.5.
[37] PDP Code of Practice for the Banking and Financial Sector, paragraph 3.1.6.
[38] PDPA, s 38(2).
[39] PDPA, s 38(4).

- political opinions,
- religious beliefs or other beliefs of a similar nature, and
- commission or alleged commission of any offense.[40]

The above categories are not fixed, as the Minister of Communications and Multimedia has the power to declare any other personal data as sensitive personal data by order in the Federal Gazette. However, to date, no such order to that effect has been made.

The PDPA requires "explicit consent" to be obtained for the processing of sensitive personal data.[41] However, note that the PDPA does not define "explicit consent" or clarify the scope of this term.[42]

6.1. Children

Children's personal data is not categorized as sensitive personal data under the PDPA.

However, the PDP Regulations 2013 provide that in order to process the personal data of any data subject under the age of 18, the data user is required to obtain the consent of the parent, guardian, or other person who has parental responsibility over the data subject.[43]

6.2. Cookie, Internet of Things, online tracking

The PDPA and its subsidiary regulations currently do not impose any specific restrictions on the use of cookies, Internet of Things devices, or other online tracking technologies.

6.3. Direct marketing

The PDPA currently adopts an opt-out regime in relation to the processing of personal data for "direct marketing" purposes (defined as the communication, by whatever means, of any advertising or marketing materials, which is directed to particular data subjects[44]).

Specifically, the PDPA provides that a data subject may issue a written notice to a data user requiring that the data user either should not begin processing the data subject's personal data for direct marketing purposes, or if the data user has already begun to process personal data for direct marketing purposes, that the data user should cease such processing.[45]

The data user must comply with the notice within such period as is reasonable in the circumstances. If the data user fails to do so, the data subject may submit an application to the PDP Commissioner.[46] The PDP Commissioner is granted certain powers to require the data user to take steps to comply with the notice,[47] failing which the data user would face criminal liability.[48]

The PDP Commissioner has previously issued two sets of public consultation papers that address the topic of direct marketing.

Public Consultation Paper (No. 1/2014) titled the *Guide in Dealing with Direct Marketing Under Personal Data Protection Act (PDPA) 2010* ("**Direct Marketing Public Consultation Paper**") provides that a data user is not allowed to use electronic communications for direct marketing except where the following conditions are met:

---

[40] PDPA, s 4.
[41] PDPA, s 40(1).
[42] However, the PDP Code of Practice for Private Hospitals in the Healthcare Industry sets out further guidance on "explicit consent," which is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her (PDP Code of Practice for Private Hospitals in the Healthcare Industry, paragraph 3).
[43] PDP Regulations 2013, Regulation 3(3).
[44] PDPA, s 43(5).
[45] PDPA, s 43(1).
[46] PDPA, s 43(2).
[47] PDPA, s 43(3).
[48] PDPA, s 43(4).

- the data subject has been informed of the identity of the direct marketing organization(s), the purpose for collection of the personal data, and the persons to whom the said personal data may be disclosed;
- the data subject has given explicit consent for his/her personal data to be used for direct marketing;
- the data subject's personal data was obtained in the course of sale of products or services;
- direct marketing materials only relate to similar products and services; and
- the materials provide a means for the data subject to refuse use of his/her personal data for direct marketing purposes.

Further, in the Direct Marketing Public Consultation Paper, the PDP Commissioner also indicated that it was considering issuing guidelines on mechanisms for digital and electronic marketing, which would include providing a clear method for data subjects to unsubscribe from online services. However, these proposals have not translated into law, and the PDP Commissioner has not issued any formal guidelines or guidance after receiving public feedback.

6.4. Biometric and genetic data

The PDPA currently does not specifically regulate biometric data and genetic data. Nevertheless, biometric data and genetic data would generally fall under the umbrella of sensitive personal data (which includes information relating to the physical or mental health or condition of a data subject). As such, the processing of biometric and genetic data would require "explicit consent" under Section 40 of the PDPA.

6.5. Financial information

The PDPA neither defines financial information nor imposes stricter conditions for financial information than those for other forms of personal data.

However, the PDP Code of Practice for the Banking and Financial Sector sets out guidance and requirements for processing of personal data by the following kinds of institutions:

- licensed banks and licensed investment banks under the FSA;
- licensed Islamic banks and licensed international Islamic banks under the IFSA; and
- development financial institutions under the Development Financial Institution Act 2002.

These institutions must obtain "explicit consent" of their customers for collection of information relating to the customers' National Registration Identity Card ("**NRIC**")[49] and comply with the requirements prescribed under the the Central Bank of Malaysia, *Bank Negara Malaysia* ("**BNM**")'s Guidelines on Product Transparency and Disclosure, which specify additional matters that must be included in these institutions' privacy notices to their customers.[50]

Financial institutions which handle personal information are also subject to a higher degree of regulation under the FSA and the IFSA. These laws prohibit the disclosure of any document or information relating to the affairs or account of any of these financial institutions' customers to another person, unless the disclosure falls within the list of permitted disclosures under Schedule 11 of the FSA and the IFSA,[51] which include disclosure based on written consent from the customer.[52]

---

[49] PDP Code of Practice for the Banking and Financial Sector, paragraph 4.2.4.
[50] PDP Code of Practice for the Banking and Financial Sector, paragraphs 4.4.11 to 4.4.16
[51] FSA, ss 133 and 134; IFSA, ss 145 and 146. See also the BNM's Policy Document on Management of Customer Information and Permitted Disclosure which sets out further conditions that must be complied with in relation to the list of permitted disclosures set out in Schedule 11 of the FSA and the IFSA.
[52] FSA and IFSA, Schedule 11, paragraph 1.

6.6. Statistics and research

The PDPA provides an exemption from several of the PDP Principles (including the General Principle, the Notice and Choice Principle, and the Disclosure Principle) for data users that process personal data for the purpose of preparing statistics or carrying out research.

However, this is subject to the proviso that the personal data may not be processed for any other purpose, and the output of the statistics or research may not be made available in a form which identifies the data subject.[53]

6.7. Pseudonymized data

The PDPA does not make specific provisions for pseudonymized data, and the PDP Commissioner has not issued any official guidance on anonymized or pseudonymized personal data.

However, it is likely that if a given pseudonymization technique is not reversible (i.e., if re-identification of the data subject is no longer possible), then data that has been pseudonymized using such a technique would no longer qualify as "personal data" under the PDPA.

6.8. Location data

The PDPA does not make specific provisions for location data.

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

The default rule under the PDPA is that cross-border data transfers are prohibited unless the transfer is to a jurisdiction that the Minister of Communications and Multimedia has declared as providing an adequate level of protection of personal data or having in place a substantially similar data protection law to the PDPA.[54] To date, the Minister has made no such declaration.

However, the PDPA also provides a list of exceptions to this general prohibition. Cross-border data transfers are permitted where, among others, the data subject has consented to the transfer.[55] However, the PDPA is silent as to the specific form and type of consent required for transfer of personal data out of Malaysia.

In practice, consent for cross-border data transfers is obtained through the data user's privacy notice (together with the consent obtained for all other forms of processing carried out by the data user), or in contracts between the data user and the data subject, via contractual clauses which provide that the data subject consents to the processing of his/her personal data, including the transfer of his/her personal data outside the country.

The approach above has been recognized in several of the PDP Codes of Practice, including the PDP Codes of Practice for the Aviation Sector,[56] the Banking and Financial Sector,[57] and the Communications (Licensees under the Communications and Multimedia Act 1998) Sector.[58]

Additionally, the MDEB states that the Government targets to complete the review and enhancement to cross-border data transfer provisions under the PDPA and its implementation mechanism by 2025. Further, the Government has also stated that it will incorporate cross-border data protection elements in all future trade agreements.

---

[53] PDPA, s 45(2)(c).
[54] PDPA, ss 129(1) and 129(2).
[55] PDPA, s 129(3)(a).
[56] PDP Code of Practice for the Aviation Sector, paragraph 4.3.
[57] PDP Code of Practice for the Banking and Financial Sector, paragraph 4.10.
[58] PDP Code of Practice for the Communications Sector, Part 4, paragraph 7.

8. TRANSPARENCY AND NOTICE

The minimum information that must be included in a written privacy notice under the PDPA and the PDP Regulations 2013 is as follows:

- a description of the personal data that is being processed by the data user;[59]
- the purposes for which the personal data is being or is to be collected and further processed; [60]
- such information as is available to the data user regarding the source of the personal data;[61]
- the existence of data subjects' rights to request access to, and correction of, their personal data and how to exercise these rights;[62]
- information on how to contact the data user with any inquiries or complaints in respect of the personal data (minimally, the designation of the data user's contact person and the data user's phone number);[63]
- the class of third parties to whom the data user may disclose the personal data;[64]
- the choices and means by which the data subject may limit the processing of his/her personal data and personal data relating to other persons who may be identified from that personal data;[65]
- whether it is obligatory or voluntary for data subjects to supply the personal data;[66] and
- where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he/she fails to supply the personal data.[67]

In addition to the above, the PDPA also requires the privacy notice to be provided in both English and the national language, *Bahasa Malaysia*.[68]

9. SANCTIONS AND ENFORCEMENT

Contravention of any of the PDP Principles, including the General Principle, is a criminal offense punishable with a fine not exceeding RM 300,000 and/or imprisonment for a term not exceeding 2 years.[69]

In practice, enforcement of the PDPA's notice and consent requirements is uncommon. Since the PDPA came into force in 2013, there has only been one publicly reported enforcement action for breach of the consent requirement in Section 5(2) of the PDPA. In 2017, the PDP Commissioner imposed a fine of RM 10,000 or 8 months' imprisonment on a hotel for processing personal data without a valid certificate of registration and without the data subjects' consent.[70]

Details as to the facts of this case and the PDP Commissioner's reasoning are limited as the PDP Commissioner typically only makes available information about the penalty imposed on the offender in its enforcement actions, rather than publishing a comprehensive decision for each action.

---

[59] PDPA, s 7(1)(a).
[60] PDPA, s 7(1)(b).
[61] PDPA, s 7(1)(c).
[62] PDPA, s 7(1)(d).
[63] PDP Regulations 2013, regulation 4.
[64] PDPA, s 7(1)(e).
[65] PDPA, s 7(1)(f).
[66] PDPA, s 7(1)(g).
[67] PDPA, s 7(1)(h).
[68] PDPA, s 7(3).
[69] PDPA, s 5(2).
[70] See https://www.pdp.gov.my/jpdpv2/berita_terkini/pengguna-data-yang-telah-dikenakan-tindakan-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709/?lang=en

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

The Malaysian data protection regime does not provide for the concept of "legitimate interests" in relation to the processing of personal data. Rather, as explained earlier, the PDPA operates on a consent-based model pursuant to the General Principle, which provides that personal data can only be processed with the consent of data subjects by default.[71] Neither the PDP Commissioner nor the Malaysian Government has provided reasons for omitting to include a "legitimate interests" basis in the PDPA.

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

11.1. Collecting, using, and disclosing non-sensitive personal data

A data user may process personal data (other than sensitive personal data) without the consent of the data subject if the processing is necessary:

- for the performance of a contract to which the data subject is a party;[72]
- for the taking of steps at the request of the data subject with a view to entering into a contract;[73]
- for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;[74]
- in order to protect the vital interests of the data subject;[75]
- for the administration of justice;[76] or
- for the exercise of any functions conferred on any person by or under any law.[77]

a. "Vital interests"

The PDP Codes of Practice have provided some clarification on processing which is necessary for the "vital interests" of the data subject.

- The **PDP Code of Practice for the Aviation Sector** provides that this exception would apply where the data user discloses names and nationalities in search and rescue operations in the event of an aircraft incident.[78]
- The **PDP Code of Practice for the Banking and Financial Sector** provides that this exception would apply where a data user discloses the personal data of the data subject to relevant third parties, such as the police or the data subject's next-of-kin, in matters relating to life, death, or security of the data subject.[79]

---

[71] PDPA, s 6(1).
[72] PDPA, s 6(2)(a).
[73] PDPA, s 6(2)(b).
[74] PDPA, s 6(2)(c).
[75] PDPA, s 6(2)(d). Note that "vital interests" are defined as matters relating to life, death or security of a data subject (PDPA, s 4).
[76] PDPA, s 6(2)(e).
[77] PDPA, s 6(2)(f).
[78] PDP Code of Practice for the Aviation Sector, paragraph 2.15.
[79] PDP Code of Practice for the Banking and Financial Sector, paragraph 3.12.

- The **PDP Code of Practice for the Utilities (Electricity) Sector** provides that this exception applies where the processing is due to the request by the Royal Malaysian Police or the data subject's immediate family in matters relating to life, death, or security of the data subject.[80]
- The **PDP Code of Practice for Private Hospitals in the Private Healthcare Sector** provides that this exception applies where medical treatment is administered to accident victims using information from personal documents such as a national registration identity card, or to treat psychiatric patients who are incapable of giving consent.[81]

11.2. Collecting, using, and disclosing sensitive personal data

Processing of sensitive personal data generally requires the explicit consent of the data subject.[82]

However, the PDPA provides that sensitive personal data may be processed without the explicit consent of the data subject if the processing is necessary:

- for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;[83]
- in order to protect the vital interests of the data subject or another person, in a case where:
  - consent cannot be given by or on behalf of the data subject;[84] or
  - the data user cannot reasonably be expected to obtain the consent of the data subject;[85]
- in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;[86]
- for medical purposes[87] and where the personal data is processed by—
  - a healthcare professional;[88] or
  - a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;[89]
- for the purpose of, or in connection with, any legal proceedings;[90]
- for the purpose of obtaining legal advice;[91]
- for the purpose of establishing, exercising or defending legal rights;[92]
- for the administration of justice;[93]
- for the exercise of any functions conferred on any person by or under any written law;[94] or
- for any other purposes as the Minister of Communications and Multimedia thinks fit.[95]

---

80 PDP Code of Practice for the Electricity (Utilities) Sector, paragraph 3.4.5.
81 PDP Code of Practice for Private Hospitals in the Private Healthcare Sector, paragraph 6.1.1(b).
82 PDPA, s 40(1)(a).
83 PDPA, s 40(1)(b)(i).
84 PDPA, s 40(1)(b)(ii)(A).
85 PDPA, s 40(1)(b)(ii)(B).
86 PDPA, s 40(1)(b)(iii).
87 "Medical purposes" is defined to include purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services (PDPA, s 40(4)).
88 PDPA, s 40(1)(b)(iv)(A).
89 PDPA, s 40(1)(b)(iv)(B).
90 PDPA, s 40(1)(b)(v).
91 PDPA, s 40(1)(b)(vi).
92 PDPA, s 40(1)(b)(vii).
93 PDPA, s 40(1)(b)(viii).
94 PDPA, s 40(1)(b)(ix).
95 PDPA, s 40(1)(b)(x).

Additionally, the requirement to obtain explicit consent for the processing of sensitive personal data is also dispensed with, where the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.[96]

11.3. Transferring personal data across borders without consent

The PDPA provides that personal data may be transferred outside of Malaysia without the consent of the data subject under the following circumstances, many of which align with the exceptions to consent for processing of personal data under Section 6(2) of the PDPA:

- the transfer is necessary for the performance of a contract between the data subject and the data user;[97]
- the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which is—
  - entered into at the request of the data subject;[98] or
  - in the interests of the data subject;[99]
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising, or defending legal rights;[100]
- the data user has reasonable grounds for believing that in all circumstances of the case:
  - the transfer is for the avoidance or mitigation of adverse action against the data subject;[101]
  - it is not practicable to obtain the consent in writing of the data subject to that transfer;[102] and
  - if it was practicable to obtain such consent, the data subject would have given consent;[103]
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA;[104]
- the transfer is necessary in order to protect the vital interests of the data subject;[105] or
- the transfer is necessary as being in the public interest in circumstances as determined by the Minister of Communications and Multimedia.[106]

11.4. Exemptions from the General Principle

The PDPA also provides for certain instances where data processing activities are exempted from the consent requirement under the General Principle, i.e., where personal data is processed:

- for the prevention or detection of crime or for the purpose of investigations;[107]
- for the apprehension or prosecution of offenders;[108]
- for the assessment or collection of any tax or duty or any other imposition of a similar nature;[109]

---

96 PDPA, s 40(1)(c).
97 PDPA, s 129(3)(b).
98 PDPA, s 129(3)(c)(i).
99 PDPA, s 129(3)(c)(ii).
100 PDPA, s 129(3)(d).
101 PDPA, s 129(3)(e)(i).
102 PDPA, s 129(3)(e)(ii).
103 PDPA, s 129(3)(e)(iii).
104 PDPA, s 129(3)(f).
105 PDPA, s 129(3)(g).
106 PDPA, s 129(3)(h).
107 PDPA, s 45(2)(a)(i).
108 PDPA, s 45(2)(a)(ii).
109 PDPA, s 45(2)(a)(iii).

- to prepare statistics or carry out research, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;[110]
- for the purpose of or in connection with any order or judgement of a court;[111]
- for the purpose of discharging regulatory functions;[112]
- for journalistic, literary or artistic purposes, provided that:
  - the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;[113]
  - the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest;[114] and
  - the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.[115]

In addition to the above, the Minister of Communications and Multimedia has the power to make further exemptions on the application of all or any of the provisions of the PDPA by way of an order published in the Federal Gazette.[116]

11.5. Sectoral regulations

Schedule 11 of the FSA and the IFSA respectively outlines circumstances in which customers' consent is not required for the disclosure of their documents or information.

The list of permitted disclosures in Schedule 11 are subject to the BNM's Policy Document on Management of Customer Information and Permitted Disclosure which sets out further conditions that must be complied with before customer information may be disclosed.[117]

11.6. Rule of interpretation

The PDP Commissioner and the Malaysian courts have not provided any official guidance or decisions on the adoption of a rule of interpretation for the PDPA provisions which operate as exceptions to the consent requirement in the PDPA.

Regarding general legal principles, Malaysian courts have endorsed the view that an exemption in legislation should be strictly interpreted, i.e., that the situation or circumstances in question must fall squarely within the words employed in the exemption.[118] However, this approach has not yet been applied to interpretation of the PDPA.

In any event, the strict interpretation of exemption or exception provisions is subject to the general rules of statutory interpretation set out in the Interpretation Acts 1948 and 1967, and case law which requires a provision to be construed in a manner that would give a fair, reasonable, and just meaning to

---

[110] PDPA, s 45(2)(c).
[111] PDPA, s 45(2)(d).
[112] PDPA, s 45(2)(e).
[113] PDPA, s 45(2)(f)(i).
[114] PDPA, s 45(2)(f)(ii).
[115] PDPA, s 45(2)(f)(iii).
[116] PDPA, s 46.
[117] https://www.bnm.gov.my/documents/20124/938039/PD+Management+of+Customer+Info.pdf/0822334e-95b2-0cd9-ecdc-1fbf275a27a2?t=1592247605654
[118] See, for example, *Enra Engineering and Fabrication Sdn Bhd v Gemula Sdn Bhd* [2020] 7 MLJ 482 in the context of the Construction Industry Payment and Adjudication (Exemption Order) 2014 and the Construction Industry Payment and Adjudication Act 2012.

the provision in order to avoid a manifestly gross absurdity and a grave and obvious injustice in the application of the provision.[119]

11.7. COVID-19

In May 2020, the PDP Commissioner issued an Advisory on the Handling Guidelines for Collection, Processing and Retention of Personal Data by Business Premises during the Conditional Movement Control Order (CMCO) ("**COVID-19 Advisory Guidelines**").[120]

However, this document was fairly limited and merely identified the requirements on businesses that were permitted to operate during the CMCO period when recording customers' or visitors' contact details for contact tracing purposes. This included guidance on the applicable requirements under the PDP Principles (for example, the types of information that can be collected for contract tracing, the need for clear notices to be displayed to visitors regarding the purpose for collection of their personal data, the data collected to be retained up to 6 months after the end of the CMCO period, etc.).

Other than the above, the PDP Commissioner has issued no further guidance regarding the collection of personal data during the COVID-19 pandemic, and whether processing in the context of COVID-19 pandemic would fall under any of the legal exemptions to the requirement to obtain consent (e.g., vital interest of the data subject, compliance with a legal obligation, research, public interest, etc.).

More broadly, the PDP Code of Practice for Private Hospitals in the Healthcare Industry provides more detailed guidance on exceptions to consent requirements which would apply to processing personal data in the context of COVID-19. In particular, insofar as sensitive personal data relates to a communicable disease, such data may be shared with the Ministry of Health ("**MOH**") pursuant to the legal basis for exercising functions conferred by written law.[121] Further, a hospital may disclose personal data pursuant to its obligation to notify MOH of notifiable diseases (which include COVID-19) on the basis that the hospital is required to or authorized to do so by law, notwithstanding that such disclosure is not within the purposes for disclosure which the data subject had consented to under the Disclosure and Notice and Choice Principles.[122]

---

[119] *Mudajaya Corp Bhd v Leighton Contractors (M) Sdn Bhd* [2015] 10 MLJ 745; *Andrew Lee Siew Ling v United Overseas Bank (M) Sdn Bhd* [2013] 1 MLJ 449; *Dirkje Peiternella Halma v Mohd Noor bin Baharom & Ors* [1990] 3 MLJ 103; and *United Hokkien Cemeteries Penang v Majlis Perbandaran Pulau Pinang* [1979] 2 MLJ 121.

[120] Available at https://ammi.com.my/wp-content/uploads/2020/06/2020-May-KKMM-PDPA-Guidelines-English.pdf

[121] PDP Code of Practice for Private Hospitals in the Healthcare Industry, paragraph 6.1.1(b).

[122] PDP Code of Practice for Private Hospitals in the Healthcare Industry, paragraph 4.4.3.

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