ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Macau SAR China

Status of Consent for Processing Personal Data

AUGUST 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Graça Saraiva

Assistant General Counsel and Data Protection Officer, Sands China

ACKNOWLEDGEMENTS

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 the data protection framework of the Special Administrative Region of Macau, China ("**Macau SAR**") and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

The main data protection legislation in Macau SAR is the Personal Data Protection Act (Law No. 8/2005) ("**PDPA**"),[1] which was passed in 2005.

The PDPA is intended to establish a comprehensive regime for processing and protection of personal data in Macau SAR,[2] based on the general principle that personal data should be processed transparently with strict respect for privacy and other fundamental rights, freedoms, and guarantees set out in the Basic Law of Macau SAR, instruments of international law, and legislation in force.[3]

The PDPA was significantly influenced by European data protection legislation – notably, Portugal's Law No. 68/98 on the Protection of Personal Data,[4] which implemented EU Directive 95/46/EC[5] (the predecessor to the GDPR). The PDPA's legal bases for processing of personal data[6] are therefore identical to those provided in Article 7 of Directive 95/46/EC and very similar to those in Article 6 of the GDPR. Under the PDPA, a controller[7] or processor[8] may process[9] personal data[10] with the consent of the data subject or where processing is necessary in other specific circumstances.

2. ROLE OF THE OFFICE OF PERSONAL DATA PROTECTION ("OPDP")

The PDPA empowers a public authority, the Office of Personal Data Protection ("**OPDP**"), to – among others – issue codes of conduct to guide implementation of the PDPA in specific sectors[11] and to register non-binding codes of conduct drawn up by professional associations and other bodies representing categories of controllers.[12]

---

[1] Note that the official languages of Macau SAR are Chinese and Portuguese. The original text of the PDPA is available in Chinese at https://www.gpdp.gov.mo/zh_cn/relevant_laws.html and in Portuguese at https://www.gpdp.gov.mo/pt/relevant_laws.html.
An unofficial English translation is available at https://www.gpdp.gov.mo/en/relevant_laws.html.

[2] PDPA, Article 1.

[3] PDPA, Article 2.

[4] Available in Portuguese at https://dre.pt/dre/detalhe/lei/69-1998-239806.

[5] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[6] PDPA, Article 6.

[7] A "**controller**" is defined as a natural or legal person, public entity, agency, or any other body which alone or jointly with others determines the purpose and means of processing (PDPA, Article 4(1)(5)).

[8] A "**processor**" is defined as a natural or legal person, public entity, agency, or any other body which processes personal data on behalf of the controller (PDPA, Article 4(1)(6)).

[9] "**Processing of personal data**" or "**processing**" is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (PDPA, Article 4(1)(3)).

[10] "**Personal data**" is defined as any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity (PDPA, Article 4(1)(1)).

[11] PDPA, Article 26.

[12] PDPA, Article 27.

The OPDP has published several sets of guidelines[13] which provide insight into how the OPDP interprets the PDPA's requirements in specific contexts, namely:

- "Principles concerning the protection of personal data in the workplace: Guidelines for Employee Monitoring" (September 2007) ("**Guidelines for Employee Monitoring**");
- "Notes for Attention: Practices for employment agencies to process customers' personal data" (July 2008);
- "Issues relating to Using Fingerprint/Hand Geometry Devices to Check on Work Attendance" (December 2008) ("**Guidelines on Using Fingerprint/Hand Geometry Devices**");
- "Opinion on the retention period of public archives containing personal data" (February 2009);
- "On using facial identification attendance control systems" (September 2009) ("**Guidelines on Facial Identification**");
- "On using attendance devices of biometric technologies other than fingerprint or hand-geometry identification" (September 2009) ("**Guidelines on Other Forms of Biometric Identification**");
- "The right to information in indirect collection of personal data" (August 2010);
- "Guidelines on publication of personal data on the Internet" (January 2011);
- "General notes on handling personal data by non-tertiary education institutions" (November 2012) ("**Education Guidelines**");
- "Guidelines on Merchants' Processing of Identification Documents of Payment Cardholders" (April 2013);
- "Guidelines on personal data processing for election campaigns" (May 2013); and
- "Guidelines for Apps Development" (September 2014).

3. SECTORAL LEGISLATION

Certain sectoral laws impose confidentiality obligations over customers'/users' information, which may include their personal data. These confidentiality obligations usually may only be waived with the consent of a customer/user or by court order. Examples of these laws include:

- **banking and financial services** – Financial System Act (Law No. 32/1993) ("**FSA**");[14]
- **telecommunications** – Basic Telecommunications Law (Law No. 14/2001[15] and the Law to Combat Computer Crime (Law No. 11/2009);[16] and
- **healthcare** – Law on Prevention and Fight Against Infectious Diseases (No. 2 /2004).[17]

---

[13] The original text of these guidelines is available in Chinese at https://www.gpdp.gov.mo/zh_cn/legal_guidelines.html and in Portuguese at https://www.gpdp.gov.mo/pt/legal_guidelines.html.
Unofficial English translations of these guidelines are available at https://www.gpdp.gov.mo/en/legal_guidelines.html.

[14] The FSA is available in Chinese at https://bo.io.gov.mo/bo/i/93/27/declei32_cn.asp and in Portuguese at https://bo.io.gov.mo/bo/i/93/27/declei32.asp. An unofficial English translation is available at https://bo.io.gov.mo/bo/i/93/27/declei32_en.asp.

[15] Available in Chinese at https://bo.io.gov.mo/bo/i/2001/34/lei14_cn.asp and in Portuguese at https://bo.io.gov.mo/bo/i/2001/34/lei14.asp. An unofficial English translation is available at https://bo.io.gov.mo/bo/i/2001/34/lei14_en.asp.

[16] Available in Chinese at https://bo.io.gov.mo/bo/i/2009/27/lei11_cn.asp#11 and in Portuguese at https://bo.io.gov.mo/bo/i/2009/27/lei11.asp.

[17] Available in Chinese at https://bo.io.gov.mo/bo/i/2004/10/lei02_cn.asp# and in Portuguese at https://bo.io.gov.mo/bo/i/2004/10/lei02.asp.

4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PERSONAL DATA PROTECTION ACT, LAW 8/2005 ("PDPA")

Consent is one of several legal bases for processing personal data[18] and sensitive personal data[19] under the PDPA but in practice, is the primary legal basis relied on by controllers and processors in Macau SAR.

Consent also functions as one of several legal bases for transferring personal data out of Macau SAR and can be used to legitimize transfer to a jurisdiction which does not ensure an adequate level of data protection.[20]

The PDPA prescribes various administrative and criminal offenses for breaching consent requirements.[21]

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

The PDPA defines consent of the data subject as any freely given, specific, and informed indication of the data subject's wishes by which the data subject signifies agreement to processing of personal data relating to him/her.[22]

The PDPA also requires that consent for the processing[23] and cross-border transfer[24] of personal data should be "unambiguous." While these requirements would likely permit express consent, it is possible that they could also permit consent to be inferred from the data subject's words or conduct, at least in certain circumstances.

The PDPA also permits processing of sensitive personal data[25] where the data subject has given "explicit" consent to such processing.[26] This appears to preclude reliance on inferred consent for most processing of sensitive personal data. That said, the PDPA does recognize inferred consent for this category of personal data in a very limited context: sensitive personal data may be processed when the data subject has manifestly made such data public, and the data subject's consent can be inferred from his/her declarations.[27]

5.2. Withdrawal of consent

The PDPA does not expressly state that consent may be withdrawn. However, based on the nature of the consent in any civil law system, it is likely that consent may be withdrawn at any time. This interpretation is consistent with the OPDP's Education Guidelines, which state a data subject can withdraw consent to processing of his/her personal data, and that a data controller must respect the data subject's "right" to do so.[28]

---

[18] PDPA, Article 6.
[19] PDPA, Articles 7(2)(3), 7(3)(2), and 7(3)(3).
[20] PDPA, Article 20(1). See "CONSENT FOR CROSS-BORDER DATA TRANSFERS" below.
[21] See "SANCTIONS AND ENFORCEMENT" below.
[22] PDPA, Article 4(1)(9).
[23] PDPA, Article 6.
[24] PDPA, Article 20.
[25] See "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA" below.
[26] PDPA, Article 7(2)(3)
[27] PDPA, Article 7(3)(3).
[28] Education Guidelines, section III.1.

Note that the PDPA also provides a right to object to processing on compelling legitimate grounds related to the data subject's particular situation.[29] If the data subject's objection is justified, the controller would be prevented from processing the data in question.[30]

5.3. Bundled consent

The PDPA does not expressly provide for bundled consent or whether provisions of goods or services may be conditional on a data subject giving consent.

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The PDPA recognizes a category of "sensitive personal data," which refers to personal data:

- revealing a person's philosophical or political beliefs, political association or trade-union membership, religion, privacy, and racial or ethnic origin;
- concerning a person's health or sex life; or
- including a person's genetic data.[31]

Sensitive personal data about a data subject may be processed either where the data subject explicitly consents to such processing or subject to guarantees of non-discrimination and implementation of security measures specified in Article 16 of the PDPA, where another legal basis for such processing exists.[32]

However, note that the PDPA requires controllers and processors to obtain authorization from the OPDP before processing sensitive personal data[33] and/or personal data relating to:

- persons suspected of illegal activities, criminal, and administrative offenses;[34] or
- the credit and the solvency of data subjects.[35]

6.1. Children

The PDPA does not specifically provide for the processing of children's data.

However, note that pursuant to the Civil Code,[36] the age of majority in Macau SAR is 18.[37] Persons below the age of 18 lack capacity to exercise legal rights (including giving consent)[38] but may be represented by their parents or legal guardians.[39]

6.2. Direct marketing

The OPDP's enforcement decisions[40] have consistently taken the position that consent is required for processing of personal data for direct marketing purposes.[41] However, these decisions do not state the rationale for this position.

---

[29] PDPA, Article 12(1).
[30] PDPA, Article 12(1).
[31] PDPA Article 7(1).
[32] PDPA, Article 7(2).
[33] PDPA, Article 22(1)(2).
[34] PDPA, Article 22(1)(1).
[35] PDPA, Article 22(1)(2).
[36] Available in Chinese at https://bo.io.gov.mo/bo/i/99/31/codcivcn/default.asp and in Portuguese at https://bo.io.gov.mo/bo/i/99/31/codcivpt/default.asp
[37] Civil Code, Article 111.
[38] Civil Code, Article 112.
[39] Civil Code, Article 113.
[40] Available at https://www.gpdp.gov.mo/en/abstract.html.
[41] See, for example, Case No. 0003/2012/IP, Case No. 0076/2014/IP, Case No. 0187/2014/IP, Case No. 0006/2015/IP, and Case No. 0014/2015/IP.

The PDPA also provides data subjects with certain rights where the controller anticipates that these data subjects' personal data will be processed for the purposes of direct marketing or other forms of commercial research. Specifically, data subjects have rights to:

- object, on request and free of charge, to processing of their personal data for such purposes;
- be informed the first time that their personal data is either disclosed to third parties, or used on behalf of third parties, for such purposes — in this case, data subjects must be offered an express right to object, free of charge, to such use or disclosure.[42]

6.3. Biometric data

Though the PDPA does not specifically provide for biometric data, the OPDP has released several guidelines on use of biometrics.

The Guidelines on Using Fingerprint/Hand Geometry Devices provide that fingerprint and handprint data qualify as personal data and that their use for monitoring employees' attendance would generally require unambiguous consent from the employee (which could be expressed in an employment contract).[43] Similar principles apply to other forms of biometric data collected for identification purposes, such as voice prints and iris scans.[44]

By contrast, the Guidelines on Facial Identification provide that facial images would likely qualify as sensitive personal data as they tend to be indicative of racial and ethnic origin, and collection of such data in the workplace would therefore likely require explicit consent from employees.[45]

6.4. Genetic data

The PDPA expressly provides that genetic data qualifies as sensitive personal data.[46]

6.5. Financial information

Financial information does not qualify as sensitive personal data under the PDPA.

However, the FSA imposes a duty on financial institutions to maintain confidentiality over information concerning the relationship between the financial institution and its customers and only permits disclosure of such information with the customers' consent or by court order.[47]

The PDPA also requires authorization from the OPDP for processing of personal data on credit and the solvency of data subjects.[48]

6.6. Statistics and research

The PDPA does not specifically provide legal bases for processing personal data for statistical or research purposes.

However, processing of personal data for these purposes may be exempted from certain of the PDPA's requirements under specific conditions. Specifically, personal data that is used for historical, statistical, or scientific purposes may be stored for periods longer than is strictly necessary for the purpose of collection or further processing.[49] Additionally, a controller's obligations to provide data subjects with information on,[50] and access to,[51] personal data about them which the controller has collected may be waived if the data in question is processed for statistical purposes or for the purposes of historical or scientific research.

---

[42] PDPA, Article 12.
[43] Guidelines on Using Fingerprint/Hand Geometry Devices, page 2.
[44] Guidelines on Other Forms of Biometric Identification, pages 3-5.
[45] Guidelines on Facial Identification, page 2.
[46] PDPA Article 7(1).
[47] FSA, Article 80.
[48] PDPA, Article 22(1)(2).
[49] PDPA, Article 5(2).
[50] PDPA, Article 10(5)(3).
[51] PDPA, Article 11(6).

6.7. Pseudonymized data

The PDPA does not specifically provide for pseudonymized data.

6.8. Location data

The PDPA does not specifically provide for location data.

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

Consent is one of several exceptions[52] to the default rule in the PDPA that personal data may only be transferred to a jurisdiction that provides an adequate level of data protection,[53] as determined by the OPDP.[54]

However, the OPDP has not issued a list of countries that are deemed adequate to date, and therefore, in practice, consent currently functions as the main legal basis for transferring personal data out of Macau SAR. As discussed above, consent for cross-border data transfers must be "unambiguous." [55]

8. TRANSPARENCY AND NOTICE

As discussed above, consent under the PDPA must, by definition, be informed.[56]

To that end, the PDPA requires a controller or its representative to provide the following information to data subjects at the time of data collection:[57]

- the identity of the controller and its representative, if any;[58]
- the controller's purpose(s) for processing the personal data;[59]
- the recipients or categories of recipients (if any) of the personal data;[60]
- whether the data subject is required to provide the personal data and the possible consequences if the data subject does not provide the data;[61] and
- the existence of the data subject's rights to access and rectify personal data about him/her and the conditions for exercising these rights.[62]

Any documents supporting the collection of personal data must contain the above information.[63] Hence, the above information is the minimum set of information that should be made available to data subjects in notices and consent forms.

A controller or its representative is not required to provide the above information:

- where the data subject already has the information;[64]
- where non-provision of the information is permitted by law;[65]
- on the grounds of security and preventing or investigating crimes;[66]

---

[52] PDPA, Article 20(1).
[53] PDPA, Article 19(1).
[54] PDPA, Article 19(3).
[55] PDPA, Article 20(1).
[56] PDPA, Article 4(1)(9).
[57] PDPA, Article 10(1).
[58] PDPA, Article 10(1)(1).
[59] PDPA, Article 10(1)(2).
[60] PDPA, Article 10(1)(3)(i).
[61] PDPA, Article 10(1)(3)(ii).
[62] PDPA, Article 10(1)(3)(iii).
[63] PDPA, Article 10(2).
[64] PDPA, Article 10(1).
[65] PDPA, Article 10(5)(1).
[66] PDPA, Article 10(5)(2).

- where processing is for statistical purposes or for purposes of historical or scientific research, and:
  - providing the information would be impossible or would involve disproportionate effort;[67] or
  - collection or disclosure is expressly laid down by law or administrative regulation, and the controller or its representative has notified the OPDP;[68] or
- where processing is for journalistic purposes or for the purpose of artistic or literary expression.[69]

In addition, if data is collected on an open network, the data subject must be informed that personal data relating to him/her may be circulated on the network without security measures and may be seen or used by third parties.[70]

9. SANCTIONS AND ENFORCEMENT

The PDPA provides various administrative and criminal offenses for breach of the PDPA, including breaches of provisions on consent and other legal bases for processing.

The OPDP generally investigates breaches of the PDPA in response to complaints, but there have also been instances where it has launched *ex officio* investigations. The OPDP publishes case notes of its numerous decisions on its website.[71]

9.1. Administrative offenses

A person who processes personal data (including sensitive personal data) or transfers such data out of Macau SAR without consent or another legal basis under the PDPA faces a fine of between MOP 8,000 and MOP 80,000.[72]

Further, a person who fails to provide a data subject with information at the time of data collection or first disclosure of the data, as required under Article 10 of the PDPA, faces a fine of between MOP 4,000 and MOP 40,000.[73]

9.2. Criminal offenses

A person who, by any means, accesses personal data without authorization faces up to one year's imprisonment or a fine.[74] The punishment doubles if the access:

- was achieved by violating technical security rules;[75]
- allowed the offender or a third party to obtain knowledge of the personal data;[76] or
- provided the offender or a third party with a benefit or material advantage.[77]

A person who is bound by professional secrecy according to the law[78] and without just cause and without due consent reveals or discloses personal data, totally or in part, faces up to two years' imprisonment or a fine.[79] The punishment doubles if the offender:

- is a civil servant (or equivalent);[80]

---

[67] PDPA, Article 10(5)(3).
[68] PDPA, Article 10(5)(3).
[69] PDPA, Article 10(6).
[70] PDPA, Article 10(4).
[71] Available at https://www.gpdp.gov.mo/en/abstract.html.
[72] PDPA, Article 33(2).
[73] PDPA, Article 33(1).
[74] PDPA, Article 38(1).
[75] PDPA, Article 38(2)(1).
[76] PDPA, Article 38(2)(2).
[77] PDPA, Article 38(2)(3).
[78] Note that under the PDPA, controllers and persons who, in carrying out their functions, obtain knowledge of personal data are bound by professional secrecy, even after such functions terminate (PDPA, Article 18(1)).
[79] PDPA, Article 41(1).
[80] PDPA, Article 41(2)(1).

- acts with the intention of obtaining a material advantage or other unlawful gain;[81] or
- adversely affects the reputation, honor and esteem, or privacy of another person.[82]

9.3. Civil liability

The PDPA expressly provides that any person who has suffered damage as a result of unlawful processing or any act which is incompatible with the PDPA or other laws and regulations in the area of personal data protection is entitled to receive compensation from the controller for damage suffered.[83]

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

10.1. Processing personal data under the PDPA

The PDPA recognizes a legal basis for processing personal data (but not sensitive personal data) where necessary for the purpose of pursuing a legitimate interest of the controller or of a third party to whom the data is disclosed. This basis is subject to a balancing test: processing is only permitted if the legitimate interest relied upon is not overridden by the fundamental rights, freedoms, and guarantees of the data subject.[84]

The PDPA does not elaborate on how this balancing test should be applied or which factors should be taken into consideration. However, the OPDP has published numerous decisions on its website[85] which have applied the legitimate interests basis. These decisions do not elaborate on how the balancing test should be applied in practice but have recognized that data controllers in Macau SAR could rely on the legitimate interests basis in at least the following circumstances:

- publishing of personal data in exercise of freedom of the press;[86]
- using personal data contained in publicly available business registration information to send a letter of demand to the administrator and shareholder of a company at that person's residential address;[87]
- processing personal data for contract and bill settlement purposes;[88]
- sharing court documents containing personal data with persons who had an interest in a case related to those court documents;[89]
- collecting personal data to prevent fraud, including:
  - recording credit card numbers in full to prevent credit card fraud;[90]
  - collecting a person's full name, identity card number, and driver's license number in a public car park to prevent parking coupon fraud;[91] and
  - petrol station staff recording customers' car license plate numbers on credit card receipts to avoid fraudulent credit card transactions;[92]
- employee monitoring to ensure safety and monitor attendance, including:

[81] PDPA, Article 41(2)(2).
[82] PDPA, Article 41(2)(3).
[83] PDPA, Article 14(1).
[84] PDPA, Article 6(5).
[85] Available at https://www.gpdp.gov.mo/en/abstract.html.
[86] Case No. 0001/2011/IP.
[87] Case No. 0185/2016/IP.
[88] Case No. 0028/2009/IP.
[89] Case No. 0018/2013/IP.
[90] Case No. 0120/2015/IP.
[91] Case No. 0066/2014/IP.
[92] Case No. 0092/2015/IP.

  - maintaining a list of staff members' names, identity card numbers, and mobile numbers which staff members had to sign for purposes of timekeeping, protection of company property, ensuring venue security, and calculation of staff salary;[93] and
  - installing and collecting personal data via closed-circuit television (CCTV) cameras in a workplace for purposes of ensuring security and monitoring employees;[94]
- collecting personal data of visitors to a building for purposes of ensuring the safety of owners and tenants and their property;[95] and
- an airline collecting passengers' personal data for immigration purposes, security checks, and for reference in the event of an emergency.[96]

The Guidelines for Employee Monitoring state that it is legitimate under the PDPA for an employer to conduct employee monitoring within the scope of business and accountability to guarantee the operation and general interests of the institution.[97] While these guidelines do not expressly refer to the legitimate interests basis, they list a number of relevant considerations to be considered in assessing the legitimacy of the purpose, method, and scope of measures to monitor employees within the workplace.

Note that neither the PDPA nor any guidance issued by the OPDP to date provides specifically for data protection impact assessments.

10.2. Combining personal data under the PDPA

Except where otherwise provided by law, the PDPA only permits combination of personal data where the OPDP has given authorization[98] and where such combination is necessary for pursuing the legal or statutory purposes and legitimate interests of the controller.[99]

This legal basis is also subject to a balancing test: the combination of personal data must not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects,[100] and the party seeking to combine the data take account of the type of data subject to combination[101] and implement adequate security measures.[102]

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

11.1. Processing personal data without consent under the PDPA

In addition to the legitimate interests basis discussed in the previous section, the PDPA permits processing of personal data without the data subject's consent where processing is necessary:

- for the performance of a contract to which the data subject is a party;[103]
- in order to take steps at the request of the data subject prior to entering into a contract or where the data subject has declared that he/she is willing to negotiate a contract;[104]

---

[93] Case No. 0085/2015/IP. See also Case No. 0020/2011/IP.
[94] Case No. 0142/2014/IP.
[95] Case No. 0002/2008/IP; Case No. 0025/2009/IP; Case No. 0049/2014/IP; Case No. 0032/2015/IP; Cases Nos. 0107/2015/IP and 0108/2015/IP; and Case No. 0091/2017/IP.
[96] Case No. 0026/2016/IP.
[97] Guidelines for Employee Monitoring, page 3.
[98] PDPA, Article 9(1).
[99] PDPA, Article 9(2)(1).
[100] PDPA, Article 7(2)(2).
[101] PDPA, Article 7(2)(4).
[102] PDPA, Article 7(2)(3).
[103] PDPA, Article 6(1).
[104] PDPA, Article 6(1).

- for compliance with a legal obligation to which the controller is subject;[105]
- in order to protect the vital interests of a data subject who is physically or legally incapable of giving consent;[106] or
- to carry out a task in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data has been disclosed;[107]

11.2. Processing sensitive personal data without consent under the PDPA

The PDPA permits processing of sensitive personal data without the need to obtain consent from the data subject where the controller or processor has given a guarantee of non-discrimination and complies with the security measures in Article 16 of the PDPA, and the processing of sensitive personal data is:

- explicitly authorized by law or regulation;[108] or
- essential, on important public interest grounds, for exercising the legal or statutory rights of the controller and is authorized by the OPDP;[109]
- necessary to protect the vital interests of the data subject or of another person, and the data subject is physically or legally incapable of giving consent;[110]
- in the ordinary course of legitimate activities undertaken by a legal person or a not-for-profit body with a political, philosophical, religious, or trade union aim and relates solely to members of that body or persons who have regular contact with it, in connection with its purposes, and the data is not disclosed to a third party without the data subject's consent;[111]
- in respect of personal data which has manifestly been made public by the data subject, where the data subject's consent to processing of his/her data can be clearly inferred from the data subject's declarations;[112] or
- necessary for the establishment, exercise or defense of legal claims and is exclusively carried out for that purpose.[113]

Additionally, sensitive personal data relating to a data subject's health, sex life, or genetic data may be processed without the data subject's consent where necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided that:

- the data is processed by a health professional bound by professional secrecy or by another person who is subject to an equivalent obligation of secrecy;
- processing is notified to the OPDP under Article 21 of the PDPA; and
- suitable safeguards are implemented.[114]

[105] PDPA, Article 6(2).
[106] PDPA, Article 6(3).
[107] PDPA, Article 6(4).
[108] PDPA, Article 7(2)(1).
[109] PDPA, Article 7(2)(2).
[110] PDPA, Article 7(3)(1).
[111] PDPA, Article 7(3)(2).
[112] PDPA, Article 7(3)(3).
[113] PDPA, Article 7(3)(4).
[114] PDPA, Article 7(4).

11.3. Transferring personal data across borders without consent under the PDPA

The PDPA permits transfer of personal data out of Macau SAR to a jurisdiction which does not ensure an adequate level of protection as determined by the OPDP, without the data subject's consent, where the controller notifies the OPDP of the transfer,[115] and the transfer is:

- necessary:
  - for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;[116]
  - for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;[117] or
  - to protect the vital interests of the data subject;[118]
- necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;[119] or
- made from a register which is intended to provide information to the public and which is open to consultation either by the public or any person who can demonstrate a legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.[120]

11.4. COVID-19

The primary legal documents that empower public authorities to take measures to address the COVID-19 pandemic are the Law on Prevention and Fight Against Infectious Diseases (No. 2 /2004)[121] and the health authority's guidelines on prevention of COVID-19.[122]

The OPDP has issued three authorizations exempting data controllers from the obligation to notify the regulator, defining the scope of data to be collected, retention periods and security measures to be applied in relation to data collection and processing in compliance with the recommendations and guidelines of other public bodies.

[115] PDPA, Article 20(1).
[116] PDPA, Article 20(1)(1).
[117] PDPA, Article 20(1)(2).
[118] PDPA, Article 20(1)(4).
[119] PDPA, Article 20(1)(3).
[120] PDPA, Article 20(1)(5).
[121] Available in Chinese at https://bo.io.gov.mo/bo/i/2004/10/lei02_cn.asp# and in Portuguese at https://bo.io.gov.mo/bo/i/2004/10/lei02.asp.
[122] Available in English at https://www.ssm.gov.mo/apps1/PreventCOVID-19/en.aspx#clg22916.

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