Personal Data Protection

Macau has developed its own legal regime on data protection, distinct from the framework in mainland China. The growth of online transactions, digital transformation, and cross-border data flows has heightened the relevance of personal data protection. Both local businesses and foreign entities operating in Macau must therefore navigate the territory's data protection requirements to ensure lawful handling of personal information and avoid regulatory pitfalls.

1. Background

Data protection is provided in the Macau Basic Law (article 30), the Macau Civil Code (article 79) and primarily by Law no. 8/2005 (the Personal Data Protection Act or the "PDPA"). The PDPA defines 'personal data' as any information of any type, in any format, including sound and image, related to a specific or identifiable natural person ("data subject"). An identifiable natural person is anyone who can be identified, directly or indirectly, in particular by reference to a specific number or to one or more specific elements related to his or her physical, physiological, mental, economic, cultural or social identity. Furthermore, "sensitive personal data" is any personal data revealing political persuasion or philosophical beliefs, political and joint trade union affiliation, religion, private life, racial or ethnical origin or data related to health or sex life, including genetic data.

The PDPA is applicable whenever there are personal data processing activities in Macau. '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, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. The Personal Data Protection Bureau ("PDPB") is the Macau regulatory authority responsible for supervising and coordinating the implementation of the PDPA.

2. Data Processing

Personal data may be processed only if the data subject has given his or her unequivocal consent or if processing is deemed necessary for:

1. Execution of an agreement where the data subject is a party, or, at the data subject's request, negotiation in relation to such an agreement;
2. Compliance with a legal obligation to which the data controller is subject;
3. Protection of vital interests of the data subject if he or she is physically or legally unable to give his or her consent;
4. Performance of a public interest assignment or exercise of public authority powers vested in the data controller or in a third party to whom the personal data is disclosed; or
5. Pursuing a data controller's legitimate interest (or the legitimate interest of a third party to whom the data is disclosed), provided that the data subject's interests or rights, liberties and guarantees do not prevail.

In the event personal data of sensitive nature is processed, the data controller requires the data subject's explicit consent to legitimately process the data. The data controller may also rely on one of the following circumstances to legitimately process personal data of sensitive nature:

- When the processing of the data referred to in the preceding paragraph is given explicit authorisation by a legal provision or by a provision of a regulation of an organic nature;
- When, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller, and authorised by the public authority;
- When it is 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 his consent;
- When it is carried out with the data subject's consent in the course of its legitimate activities by a legal person or non-profit seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
- When it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
- When it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

The data controller should provide the following information to the data subject (regardless if the former is processing data of sensitive nature or not): identification of the data controller, the purpose of processing, and the means and forms available to the data subject for accessing, amending and deleting his or her personal data. Moreover, if applicable, the data subject should also be informed of the possibility of their data being transferred to a jurisdiction outside of Macau.

3. Data Subjects' Rights
Data subjects enjoy various rights under the GDPR including the right of access, right to rectify, erasure or blocking of data (which processing does not comply with the PDPA), right to object and right not to be subject to automated individual decisions, and the general right to compensation in the event the data subject suffers any damages from unlawful processing activities.

4. Data Protection Officer
The PDPA does not require data controllers to appoint a data protection officer.

5. Transfer of Data
The transfer of personal data outside Macau can only take place if the recipient country ensures an adequate level of personal data protection, unless the data subject has provided clear consent or the required legal conditions have been met, and the required filings have been made with the PDPB.

In view of the close relationship with Mainland China and the extraterritorial effect of the Chinese Personal Information Protection Law ("PIPL"), the PDPB has urged local data controllers and processors to be aware of the data transfer requirements pursuant to the PIPL, including to proceed / take part in a data security assessment prior to the transfer of data from Mainland China to Macau.

6. Notification and Authorization Requirements
The PDPB must be notified of any processing of personal data by a data controller, within 8 days from the commencement of the processing activity, unless an exemption applies.

For certain data categories (e.g. certain sensitive personal data, data regarding illicit activities or criminal and administrative offenses or credit and solvency data) and certain specific personal data processing, data controllers must obtain prior authorization from the PDPB.

7. Security
The data controller must implement adequate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a security level appropriate to the risks represented by the personal data processing and the nature of the personal data, taking into consideration the state of the art and costs of the measures.

Notwithstanding the foregoing, the PDPA does not require data controllers to notify either the PDPB or data subjects about any personal data breach. However, the Law on Cybersecurity implemented a requirement to notify the Cybersecurity Incident Alert and Response Center (CARIC) and respective regulatory authority, in the event of a system breach. This obligation is, however, limited to operators of critical infrastructures.

8. Marketing Communications
Under the PDPA, data subjects have the right to object, upon their request and free of charge, to the processing of their personal data for direct marketing purposes, to be informed before their personal data is disclosed or used by third parties for the purpose of direct marketing and to be expressly offered, also free of charge, the right to object to such disclosure or use.

9. Penalties
Violations of the PDPA are subject to civil liability and administrative and criminal sanctions, including fines and/or imprisonment. The maximum administrative fine under the PDPA is MOP 200,000.

Key Contact:

JOSÉ LEITÃO, PARTNER
jose.leitao@mdme.com