

PANORAMIC

DATA PROTECTION & PRIVACY

Macau

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: October 5, 2026

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2026 Law Business Research

Contents

Data Protection & Privacy

LAW AND THE REGULATORY AUTHORITY

- Legislative framework
- Data protection authority
- Cooperation with other data protection authorities
- Breaches of data protection law
- Judicial review of data protection authority orders

SCOPE

- Covered uses of PI
- Exempt sectors and institutions
- Interception of communications and surveillance laws
- Other laws
- PI formats
- Extraterritoriality

LEGITIMATE PROCESSING OF PI

- Legitimate processing – grounds
- Legitimate processing – types of PI

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

- Transparency
- Exemptions from transparency obligations
- Data accuracy
- Data minimisation and purpose limitation
- Data retention

SECURITY

- Security obligations
- Notification of data breach

INTERNAL CONTROLS

- Accountability
- Data protection officer
- Record-keeping
- Risk assessment
- Design of PI processing systems

REGISTRATION AND NOTIFICATION

- Registration

Other transparency duties

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

Restrictions on third-party disclosure

Cross-border transfer

Further transfer

Localisation

RIGHTS OF INDIVIDUALS

Access

Other rights

Compensation

Enforcement

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

SPECIFIC DATA PROCESSING

Cookies and similar technology

Electronic communications marketing

Targeted advertising

Children's data

Age verification

Sensitive personal information

Profiling

Automated decision-making

Cloud services

UPDATE AND TRENDS

Key trends and future developments

Contributors

Macau

MdME

MdME

José Leitão

Daniela Guerreiro

jose.leitao@mdme.com

daniela.guerreiro@mdme.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Personal data is protected in Macau through the following statutes:

- article 32 of the Macau Basic Law guarantees the freedom and privacy of communications of residents and provides the constitutional foundation for personal data and privacy protection, subject only to lawful limitations for specific public interests.
- article 79 of the Macau Civil Code safeguards personal data by granting individuals rights to access and correct their data, requiring collection for clear and defined purposes, and subjecting third-party access to authorisation by the competent authority.

The Personal Data Protection Act (Law No. 8/2005) (PDPA) is the principal data protection law in Macau, setting out the core principles for personal data processing, the rights of data subjects, and the obligations of data controllers, drawing inspiration from the former EU Data Protection Directive and Portuguese data protection law.

Law stated - 7 September 2026

Data protection authority

Which authority is responsible for overseeing the data protection law?
What is the extent of its investigative powers?

The Directorate of Personal Data Protection Services (DSPDP) is the supervisory authority responsible for overseeing compliance with Macau's personal data protection framework and enforcing the PDPA. It has exclusive competence to monitor compliance, propose data protection policies and measures, and exercise supervisory and enforcement powers.

Within the DSPDP, the Supervision Department handles complaints and inquiries, conducts investigations, and initiates administrative sanctioning proceedings. It is empowered to inspect data-processing activities and keep official records of PDPA administrative offences.

Law stated - 7 September 2026

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Yes. Administrative Regulation No. 42/2023 expressly requires the DSPDP to cooperate with other data protection authorities, both within Macau and internationally. The Department of Verification, Administration and Finance is tasked with promoting cooperation and information exchange, while the Verification Division prepares and proposes cooperation agreements with foreign counterparts.

While this framework establishes a clear legal basis for cooperation through bilateral or multilateral arrangements, it does not provide a formal mechanism for resolving divergent interpretations or enforcement approaches, relying instead on coordination through cooperation agreements.

Law stated - 7 September 2026

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes. Breaches of Macau data protection law may result in administrative sanctions, corrective orders, and criminal penalties, depending on the seriousness of the infringement.

The DSPDP is empowered to investigate violations, either following a complaint or on its own initiative, and may issue binding orders to cease unlawful processing or require remedial measures. Where a breach involves sensitive personal data or data relating to criminal or administrative offences, administrative fines ranging from 4,000 to 40,000 patacas may be imposed on controllers that fail to implement appropriate safeguards. Ancillary measures may also apply, including the blocking, erasure, or destruction of data, temporary or permanent prohibitions on processing, publication of the decision, or public censure.

The PDPA also establishes criminal offences, including unauthorised access to personal data and unauthorised destruction or alteration of data, which are prosecuted through the judicial system and may lead to imprisonment or fines.

The PDPA itself does not require data breach notifications, but separate notification obligations may apply under the Cybersecurity Law where the breach qualifies as a cybersecurity incident and the controller is an operator of critical infrastructure.

Law stated - 7 September 2026

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

While the concept of PI owner is not recognised under Macau law (as the PDPA solely refers to data controllers, processors and recipients), Macau law allows the data controller and other affected parties to appeal to the courts against binding orders, decisions, or sanctions issued by the DSPDP. Acts of the DSPDP constitute administrative acts and are thus subject to judicial review under Macau's administrative litigation framework. An appeal may be filed before the competent administrative courts, typically by way of a contentious administrative appeal (*recurso contencioso*), challenging the legality of

the decision, including its compliance with the law (based on manifest error or total unreasonableness in the exercise of discretionary powers), and adherence to procedural requirements. The court has the authority to annul, uphold, or otherwise rule on the challenged measure in accordance with general principles of administrative law.

Law stated - 7 September 2026

SCOPE

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Macau Personal Data Protection Act (Law No. 8/2005) (PDPA) applies to all personal data processing carried out in Macau, regardless of the type of processing activity. It does not recognise the concept of a 'data owner', but instead distinguishes between data controllers (who determine the purposes and means of processing), data processors (who process data on the controller's behalf), and data recipients (to whom personal data are disclosed).

Law stated - 10 June 2026

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation, or are some sectors or institutions outside its scope?

The Macau PDPA applies as a general rule across all sectors and types of organisations, including both public and private entities, and serves as the core data protection framework in Macau.

Certain areas of activity are, however, subject to specific statutory regimes that may complement, qualify, or limit the application of the PDPA, in particular:

- Law relating to the defence of state security (Law No. 2/2009) establishes a special regime for activities relating to the protection of State security and grants competent authorities enhanced powers to collect, use, access, and retain personal data for national security purposes. In this context, certain PDPA safeguards and data subject rights may be restricted to the extent strictly necessary.
- Law on the protection of state secrets (Law No. 21/2023) governs the classification and handling of information designated as state secrets. Where personal data form part of or are linked to state secrets, strict confidentiality, access, and security obligations apply, which may override general PDPA requirements.
- Legal framework for the interception and protection of communications (Law No. 10/2022) regulates the interception of communications and the retention and disclosure of communications and user data for criminal investigation purposes. While it expressly refers to the PDPA, it introduces specific powers and obligations applicable to telecommunications operators and service providers that qualify the general data protection regime.

- Cybersecurity Law (Law No. 13/2019) establishes a mandatory cybersecurity framework for operators of critical infrastructures. Where personal data is processed in the context of cybersecurity obligations – such as incident prevention, monitoring, and reporting – specific duties of cooperation and disclosure toward competent authorities apply alongside, and in some cases limit, the PDPA framework.
- In the financial sector, the Monetary Authority of Macau issues sector-specific guidance, regulations, and supervisory requirements applicable to financial institutions under its oversight. Such guidance typically addresses governance, risk management, outsourcing, cybersecurity, anti-money laundering, and operational resilience, and routinely includes expectations relating to the protection, security, and confidentiality of customer and employee personal data.
- In the gaming sector, the Gaming Inspection and Coordination Bureau issues binding instructions applicable to gaming concessionaires and other gaming-related entities. This guidance may address the handling of player data, including the cross-border transfer of gaming-related information.

Notwithstanding these sector-specific regimes, the PDPA remains the baseline data protection law in Macau, and continues to apply unless its application is expressly excluded or modified by special legislation.

Law stated - 10 June 2026

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Macau PDPA applies to electronic marketing and to the monitoring and surveillance of individuals, but it does not specifically regulate the interception of communications, which is instead governed by Law no. 10/2022. That law establishes a strict legal framework for the interception of communications in the context of criminal proceedings, limiting such measures to serious crimes and subjecting them to judicial authorisation, time limits, and procedural safeguards, as well as regulating the retention and disclosure of communications and user data by service providers.

In relation to electronic marketing, the PDPA requires a valid legal basis—typically the data subject’s unambiguous consent—and grants data subjects the right to object, free of charge, to the use of their personal data for direct marketing. Transparency obligations also apply where data are disclosed or used by third parties for marketing purposes.

As regards monitoring and surveillance, the PDPA applies to video surveillance involving identifiable individuals. In addition, Law no. 2/2012 provides a specific framework for video surveillance in public spaces by authorities with police powers, restricting such measures to defined public-interest purposes and imposing requirements relating to authorisation, proportionality, access controls, retention limits, and safeguards against misuse.

Law stated - 10 June 2026

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The Directorate of Personal Data Protection Services (DSPDP) has issued several guidelines in multiple topics, including on employee monitoring, practices for employment agencies, the use of diverse technology to check on employee attendance, app development, the publication of personal data on the internet, among others.

Certain sectors may have additional regulations: for instance, the Monetary Authority of Macau has issued guidance on Cloud Outsourcing Controls, Technology and Cyber Risk Management, as well as enhancement of security control for mobile banking and mobile payment application. Furthermore, the Macau Gaming Inspection and Coordination Bureau has also issued directives to gaming concessionaires and other entities under its supervision, regarding data processing activities in the gaming sector.

Law stated - 10 June 2026

PI formats

What categories and types of PI are covered by the law?

The Macau PDPA applies to the processing of personal data relating to identified or identifiable natural persons, regardless of the format or medium, and expressly covers both automated processing and manual filing systems. It does not apply to personal data processed by individuals for purely personal or household purposes, provided that the data are not systematically disclosed to third parties.

Law stated - 10 June 2026

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Macau PDPA applies territorially to all personal data processing carried out in Macau. While its scope is based on territorial criteria, the PDPA may also apply to controllers without a physical presence in Macau where personal data are processed through activities taking place in the territory, such as the use of local communication networks or service providers established in Macau.

Law stated - 10 June 2026

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes. Under the Macau Personal Data Protection Act (Law No. 8/2005) (PDPA), the processing of personal information must be based on a legitimate legal ground, and the applicable grounds depend on whether the data are non-sensitive or sensitive.

For non-sensitive personal data, processing may be justified on a range of legal bases, including the data subject's unambiguous consent, the performance or negotiation of a contract, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest or under official authority, or the pursuit of the controller's legitimate interests.

For sensitive personal data, more restrictive conditions apply. Processing is generally permitted only where there is the data subject's explicit consent or another specific legal basis, such as statutory authorisation, necessity for important public interest reasons, protection of vital interests, processing by certain organisations (ie, political or trade-union bodies) within limited contexts, data manifestly made public by the data subject, or where necessary for the establishment, exercise, or defence of legal claims.

Law stated - 10 June 2026

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Yes. The Macau PDPA requires controllers to apply enhanced protection to personal data of a sensitive nature (ie, personal data revealing philosophical or political beliefs, political association or trade-union membership, religion, privacy and racial or ethnic origin, data concerning health or sex life, including genetic data).

These heightened protection standards are reflected, in particular, in the stricter conditions and limited legal grounds under which sensitive personal data may be processed. In addition, the Macau PDPA requires data controllers to implement reinforced technical and organisational security measures, including controls over physical access to processing premises, protection of data media, prevention of unauthorised input, access, use, transmission, and transport of personal data, as well as mechanisms to ensure traceability and ex post verification of data processing activities.

Law stated - 10 June 2026

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Macau Personal Data Protection Act (Law No. 8/2005) (PDPA) imposes a general transparency obligation on data controllers, requiring them to inform data subjects about key aspects of their personal data processing activities, including the controller's identity, processing purposes, recipients of the data, data subject rights, and any cross-border data transfers. Additional information must be provided where data are collected via open networks. This information must be made available to data subjects prior to the commencement of processing and may be provided through an appropriate format, such as a privacy notice or privacy policy.

Law stated - 10 June 2026

Exemptions from transparency obligations

When is notice not required?

The Macau PDPA permits the information obligation to be waived in limited circumstances, including where authorised by law, necessary for security or criminal investigations, or where personal data are processed for statistical, historical, or scientific research and informing data subjects would be impossible or disproportionate. The duty to inform also does not apply to processing carried out solely for journalistic, artistic, or literary purposes.

Law stated - 10 June 2026

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. The Macau PDPA establishes data quality as a core principle, requiring personal data to be accurate, complete, and kept up to date, and obliges controllers to rectify or erase inaccurate or incomplete data. Data subjects have the right to request rectification, which must be handled without excessive delay or expense. The PDPA does not define specific timelines or costs, leaving these to be assessed on a case-by-case basis.

Law stated - 10 June 2026

Data minimisation and purpose limitation

Does the law restrict the types or volume of PI that may be collected?

The Macau PDPA requires that personal data be adequate, relevant, and not excessive in relation to the purposes of processing, reflecting the principles of necessity and proportionality. As the law does not define what constitutes 'excessive' data, this assessment is made case by case, taking into account the processing purpose, context, and the data subject's legitimate expectations. Controllers are, therefore, expected to limit data collection to what is strictly necessary and to periodically review the scope of data processed.

Law stated - 10 June 2026

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The Macau PDPA requires that personal information be kept no longer than necessary for the purposes for which it was collected or further processed. However, it does not set specific limits on the amount of personal data that may be held or prescribe fixed retention periods.

Data controllers must therefore determine appropriate data minimisation and retention periods on a case-by-case basis, taking into account factors such as the purpose of processing, the nature of the data, and applicable legal or regulatory obligations. In practice, sector-specific legislation may impose minimum retention requirements. For example, employee-related data must generally be retained for at least three years under the Labour Relations Law, while anti-money laundering and counter-terrorist financing rules in the banking sector typically require relevant records to be retained for at least five years following the completion of a transaction or the end of a business relationship.

Law stated - 10 June 2026

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Yes. The Macau Personal Data Protection Act (Law No. 8/2005) (PDPA) requires controllers to implement appropriate technical and organisational security measures to protect personal data, particularly where sensitive data or data relating to criminal or administrative offences are involved. These measures may include physical security, access controls, secure data transmission, protection of data media, and mechanisms ensuring traceability of processing.

Where controllers engage processors, they must ensure that processors provide adequate security guarantees and comply with equivalent data protection obligations. This must be documented in a binding contract or legal instrument, under which the processor acts solely on the controller's instructions.

Law stated - 10 June 2026

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Macau PDPA does not impose any obligation to notify personal data breaches, either to the supervisory authority or to affected individuals.

However, separate notification obligations arise under the Macau Cybersecurity Law for operators of critical infrastructures, who must report cybersecurity incidents to the Cybersecurity Incident Alert and Response Center (CARIC) and the relevant sectoral authorities.

'Cybersecurity Incident' is understood as any situation that constitutes an unauthorised act and, in general, any event with a real adverse effect on the security of computer networks, systems, and data. The notification to CARIC should be made in writing, by using a specific form which can be emailed to CARIC or faxed. Reporting timelines depend on the severity of the incident, with serious incidents requiring notification within two hours, followed by updates and a final report.

In addition, sector-specific regimes may impose further reporting requirements. For example, financial institutions must report 'Major Emergencies' to the Monetary Authority of Macau, often subject to accelerated notification timelines and follow-up reporting obligations. 'Major Emergencies' include system malfunction, operational disruption of Internet/mobile banking services, distributed denial of service (DDoS) attacks, fraudulent websites, natural disasters, outbreak of infectious diseases, acts of terrorism and other incidents that could lead to major operational disruption in the financial institutions.

Where a financial institution is affected by a major emergency, it is subject to multiple reporting requirements, including an initial notification to be made within one hour of the occurrence or detection of the incident, and a final report to be submitted within one month thereafter.

Law stated - 10 June 2026

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Under the Macau Personal Data Protection Act (Law No. 8/2005) (PDPA), controllers and processors are not subject to a specific accountability regime requiring specific internal control frameworks. However, they are required to implement appropriate technical and organisational measures to ensure that the processing of personal information complies with the PDPA and to remain responsible for such compliance. In practice, this means that organisations must put in place internal controls, procedures, and safeguards appropriate to the nature, scope, and risks of the processing activities. While the PDPA does not expressly require formal documentation, audits, or compliance reports, controllers must be able to demonstrate compliance when challenged by the supervisory authority, particularly in the context of investigations or complaints.

Law stated - 10 June 2026

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

No. The PDPA does not require the appointment of a data protection officer (DPO), nor does it define a DPO role or prescribe related qualifications or responsibilities.

However, under the Macau Cybersecurity Law, operators of critical infrastructures are required to appoint a principal person responsible for cybersecurity, as well as a designated substitute. While this role does not fully correspond to a DPO as understood in other data protection regimes, it may indirectly encompass responsibilities relevant to the protection of personal data, insofar as such data are processed within information and cybersecurity systems.

The person responsible for cybersecurity must have adequate suitability and professional experience and be habitually resident in Macau. Operators are expected to consult the Judiciary Police regarding the suitability of the proposed appointees, although the Cybersecurity Law does not further define the required professional experience.

Their responsibilities include overseeing the operator's cybersecurity management framework, supervising its implementation, managing and assessing cybersecurity incident response, promoting staff awareness and training, and ensuring ongoing availability for contact by the CARIC.

Law stated - 10 June 2026

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

No, not generally. The Macau PDPA does not require controllers or processors to maintain internal records of personal information comparable to formal records of processing activities under other regimes.

However, record-keeping obligations may arise under other laws. In particular, the Cybersecurity Law requires operators of critical infrastructures to maintain records relating to cybersecurity management, incident handling, and system security logs, which may include personal data. In addition, sector-specific legislation, such as financial services regulations and anti-money laundering requirements, may impose separate record-keeping duties involving customer and transaction data.

Law stated - 10 June 2026

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The Macau PDPA does not impose a specific obligation on controllers or processors to carry out formal risk assessments. However, risk assessments may be required in practice in certain situations, including:

- Processing subject to prior authorisation by the Directorate of Personal Data Protection Services (DSPDP), such as the processing of sensitive data without statutory authorisation, data interconnection, or processing operations that may pose risks to data subjects' rights, where controllers must explain the associated risks and safeguards.
- Implementation of security measures, where controllers are expected to assess processing risks in order to determine appropriate technical and organisational safeguards.
- Cross-border transfers of personal data requiring prior DSPDP authorisation, where controllers must demonstrate the necessity, proportionality, and risk mitigation measures applicable to the transfer.

Law stated - 10 June 2026

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The Macau PDPA does not provide for a specific obligation for controllers or processors to apply a formal 'privacy by design' or 'privacy by default' approach. Notwithstanding the foregoing, while the PDPA appears to be very general in nature, it still requires processing systems to be designed and implemented in a manner that embeds data protection principles, including security, proportionality, purpose limitation and retention control.

However, sectoral rules may provide for additional rules. For instance, in the financial sector, the Monetary Authority of Macau guidelines on technology and cyber-risk management, electronic banking, and cyber resilience require authorised financial institutions to design and implement systems with embedded safeguards, including robust access controls, data confidentiality and integrity protections, logging and monitoring mechanisms, and security measures proportionate to the sensitivity of the data and the associated risks. As a result, data processing systems in the financial sector must be architected from the outset to ensure secure, controlled and purpose-limited processing throughout the data life cycle, in line with both regulatory expectations and PDPA requirements.

Law stated - 10 June 2026

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Yes. Under the Macau Personal Data Protection Act (Law No. 8/2005) (PDPA), data controllers are generally required to notify the DSPDP of their personal data processing activities carried out in Macau, regardless of whether the controller has an establishment in Macau. Controllers without a local presence must appoint a local representative. Notification must be submitted within eight days from the commencement of processing, using the prescribed form, and approved notifications are made publicly accessible by the Directorate of Personal Data Protection Services (DSPDP).

Failure to notify constitutes an administrative offence, punishable by fines ranging from 2,000 to 20,000 patacas (natural persons) or 10,000 to 100,000 patacas (legal persons), with higher penalties where prior authorisation is required.

Exemptions apply to certain routine processing activities, subject to strict conditions, such as limited employee data processing, administrative HR management, recruitment data (with capped retention periods), and basic vendor or service-provider data.

Law stated - 10 June 2026

Other transparency duties

Are there any other public transparency duties?

There are no other transparency obligations under Macau law.

Law stated - 10 June 2026

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Under the Macau Personal Data Protection Act (Law No. 8/2005) (PDPA), the sharing of personal data with entities that provide outsourced processing services is permitted but strictly regulated, with the data controller remaining ultimately responsible for compliance with the PDPA. The main requirements on the sharing of personal data are as follows:

- the controller should only engage processors that provide sufficient guarantees with respect to technical and organisational security measures;
- the processor may only process personal data pursuant to the purposes determined by the controller, and in strict compliance with the controller's instructions;
- the relationship between controller and processor should be governed by a written contract or other legally binding instrument; and
- where the sharing of personal data requires cross-border data transfer, additional requirements may apply.

Additional requirements may apply in different sectors; for instance, in the financial sector, the Monetary Authority of Macau has issued a Guideline on Outsourcing, which requires outsourced service providers to implement adequate confidentiality, data protection and

security measures. Furthermore, outsourcing arrangements should be governed by written contracts clearly defining the scope of the services, data protection responsibilities, access controls, and audit and supervision rights.

Law stated - 10 June 2026

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The Macau PDPA does not provide for any specific restrictions on sharing personal data with recipients that are not processors or service providers, beyond the general requirements of notice, choice or purpose limitation.

Furthermore, Macau law does not recognise or regulate the 'sale' of personal information as a distinct concept, nor does it impose specific rules or prohibitions on sharing personal information for online targeted or behavioural advertising.

Law stated - 10 June 2026

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Yes. The Macau PDPA restricts the transfer of personal information outside Macau. As a general rule, cross-border transfers are permitted only where the receiving jurisdiction ensures an adequate level of data protection, as assessed by the Directorate of Personal Data Protection Services (DSPDP) on a case-by-case basis.

However, transfers may proceed without an adequacy assessment, subject to notification to the DSPDP, where a valid legal basis applies. These include the data subject's unambiguous consent, necessity for the performance or negotiation of a contract, important public interests or legal proceedings, protection of the data subject's vital interests, or transfers from public registers open to consultation under law.

Law stated - 10 June 2026

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Macau PDPA's restrictions apply equally to transfers to service providers and to onward transfers, but only at the level of the Macau controller's responsibility. While the PDPA does not apply directly to a transfer occurring wholly outside Macau, the Macau controller remains ultimately accountable for ensuring that any onward transfer by a service provider or recipient is authorised, contractually controlled, and consistent with the safeguards or authorisation underpinning the original transfer from Macau.

Law stated - 10 June 2026

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No, the Macau PDPA does not impose a general data-localisation requirement, nor does it require personal information or copies thereof to be retained in Macau once such data are lawfully transferred or accessed from outside the jurisdiction. While sector-specific frameworks (including in the financial sector) may require controllers to make records available to competent regulators upon request, in line with cooperation and supervisory obligations, there are no rules mandating that such records be stored or maintained locally in Macau.

Law stated - 10 June 2026

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, data subjects are entitled to exercise their right of access under the Macau Personal Data Protection Act (Law No. 8/2005) (PDPA). The scope of this right includes the following:

- confirmation as to whether or not data relating to the data subject are being processed, as well as the information on the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;
- communication, in an intelligible form, of the personal data undergoing processing and of any available information regarding the source of such data; and
- information on the logic involved in any automated processing of personal data concerning the data subject.

Data subjects should be able to exercise this right without excessive delay or expense. The Macau PDPA, however, does not provide specific guidance on what constitutes 'excessive' delay or expense, and this will therefore depend on the circumstances of each case, including the nature of the request and the scope of the personal data concerned.

Law stated - 10 June 2026

Other rights

Do individuals have other substantive rights?

Yes, the PDPA provides for other rights to the data subject, including:

- the right to request rectification, erasure or blocking of data which processing is not compliant with the PDPA (including where the data are incomplete or inaccurate);
- the right to object to marketing communications, upon request and free of charge;
- the right to object to the processing activities on compelling legitimate grounds relating to the data subject's particular situation;
- the right not to be subject to automated individual decisions; and
- the right to compensation where the data subject suffers damage as a result of unlawful processing of their personal data.

Law stated - 10 June 2026

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, the PDPA provides for the right to compensation, where the data subject suffers damages as a result of unlawful processing of their personal data. As a general rule, the data subject must be able to demonstrate actual damage resulting from the breach. This may include material (financial) loss and, in principle, non-material damage (such as moral or reputational harm), assessed in accordance with the general rules on civil liability under Macau law.

Law stated - 10 June 2026

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights are exercisable through both the judicial system and the supervisory authority. Data subjects may lodge complaints to the Directorate of Personal Data Protection Services (DSPDP), which has competence to investigate alleged breaches, order corrective measures, and impose administrative sanctions where appropriate.

Data subjects may also enforce their rights through the courts, in particular by bringing civil claims for compensation for damage suffered as a result of PDPA infringements.

Law stated - 10 June 2026

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Yes. Certain data subject rights may be restricted where processing is necessary for the prevention, investigation, detection, or prosecution of criminal offences, or for the conduct of judicial proceedings, in accordance with applicable laws.

Furthermore, such rights may also be restricted for reasons of public security, national security, defence, or other important public interests, to the extent provided by law.

Law stated - 10 June 2026

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The Macau Personal Data Protection Act (Law No. 8/2005) (PDPA), and the Macau legal framework more generally, does not provide for specific rules on the use of 'cookies' or equivalent technology. However, the use of cookies is indirectly regulated under the PDPA to the extent that cookies involve the processing of personal data.

Law stated - 10 June 2026

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Macau does not have a specific or standalone regime governing marketing by email, fax, telephone, or other electronic channels (such as social media). However, such marketing activities are regulated indirectly under the Macau PDPA. In particular, pursuant to the PDPA, the data subject has the right to object to marketing communication upon request and free of charge.

Law stated - 10 June 2026

Targeted advertising

Are there any rules on targeted online advertising?

Macau does not have a specific or standalone regime governing targeted advertising. However, such activities are regulated indirectly under the Macau PDPA. In particular, pursuant to the PDPA, the data subject has the right to object to marketing communication upon request and free of charge.

Law stated - 10 June 2026

Children's data

Are there any specific rules relating to the use of children's PI?

The Macau PDPA does not provide for specific rules relating to the use of children's PI.

Law stated - 10 June 2026

Age verification

Are there any specific rules relating to the use of PI for age verification purposes online?

The Macau PDPA does not provide for specific rules relating to the use of PI for age verification purposes.

Law stated - 10 June 2026

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Yes, the PDPA provides for more stringent rules on the processing of personal data, deemed to be of a sensitive nature.

Law stated - 10 June 2026

Profiling

Are there any rules regarding the use of PI for individual profiling?

The Macau PDPA does not provide rules specifically for profiling; however, the PDPA foresees some requirements related to automated decision-making.

Law stated - 10 June 2026

Automated decision-making

Does the law restrict the use of PI in automated decision making that affects individuals without human intervention?

Yes. The Macau PDPA restricts automated decision-making without human involvement where such decisions produce legal effects or significantly affect individuals. Data subjects have the right not to be subject to decisions based solely on automated processing, particularly where personal aspects such as performance, creditworthiness, or behaviour are evaluated.

Automated decisions may nevertheless be permitted where they are necessary for entering into or performing a contract, provided appropriate safeguards exist (including the right to

express a viewpoint), or where they are expressly authorised by law and accompanied by measures protecting the data subject's legitimate interests.

Law stated - 10 June 2026

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The Macau PDPA does not contain cloud-specific rules, nor has the Directorate of Personal Data Protection Services (DSPDP) issued dedicated guidance on cloud computing. Accordingly, the use of cloud services is assessed under the PDPA's general data protection principles, such as lawfulness and security, where personal data is processed.

However, sector-specific rules may apply. In particular, the Monetary Authority of Macau treats cloud computing as a form of outsourcing for regulated financial institutions, subjecting it to risk-based regulatory oversight, including requirements for due diligence, risk assessments, and appropriate technical and organisational security safeguards.

Law stated - 10 June 2026

UPDATE AND TRENDS

Key trends and future developments

Are there any emerging trends or hot topics in data protection in your jurisdiction, and are there any proposed changes to the current legislation?

One of the current hot topics in Macau data protection is the ongoing harmonisation of Macau's regulatory framework with the data protection and data governance rules of mainland China, particularly in relation to cross-border transfers of personal data within the Guangdong–Hong Kong–Macau Greater Bay Area (GBA). In this context, the Macau Government has been actively participating in regional initiatives aimed at facilitating the safe and orderly cross-boundary flow of data, while maintaining appropriate safeguards. Notably, Macau authorities have introduced facilitation measures such as the GBA Standard Contract for the Cross-boundary Flow of Personal Information, promoted through the Macau Economic and Technological Development Bureau, which seeks to streamline compliance requirements for data transfers between Macau and mainland China within the GBA framework.

Law stated - 10 June 2026