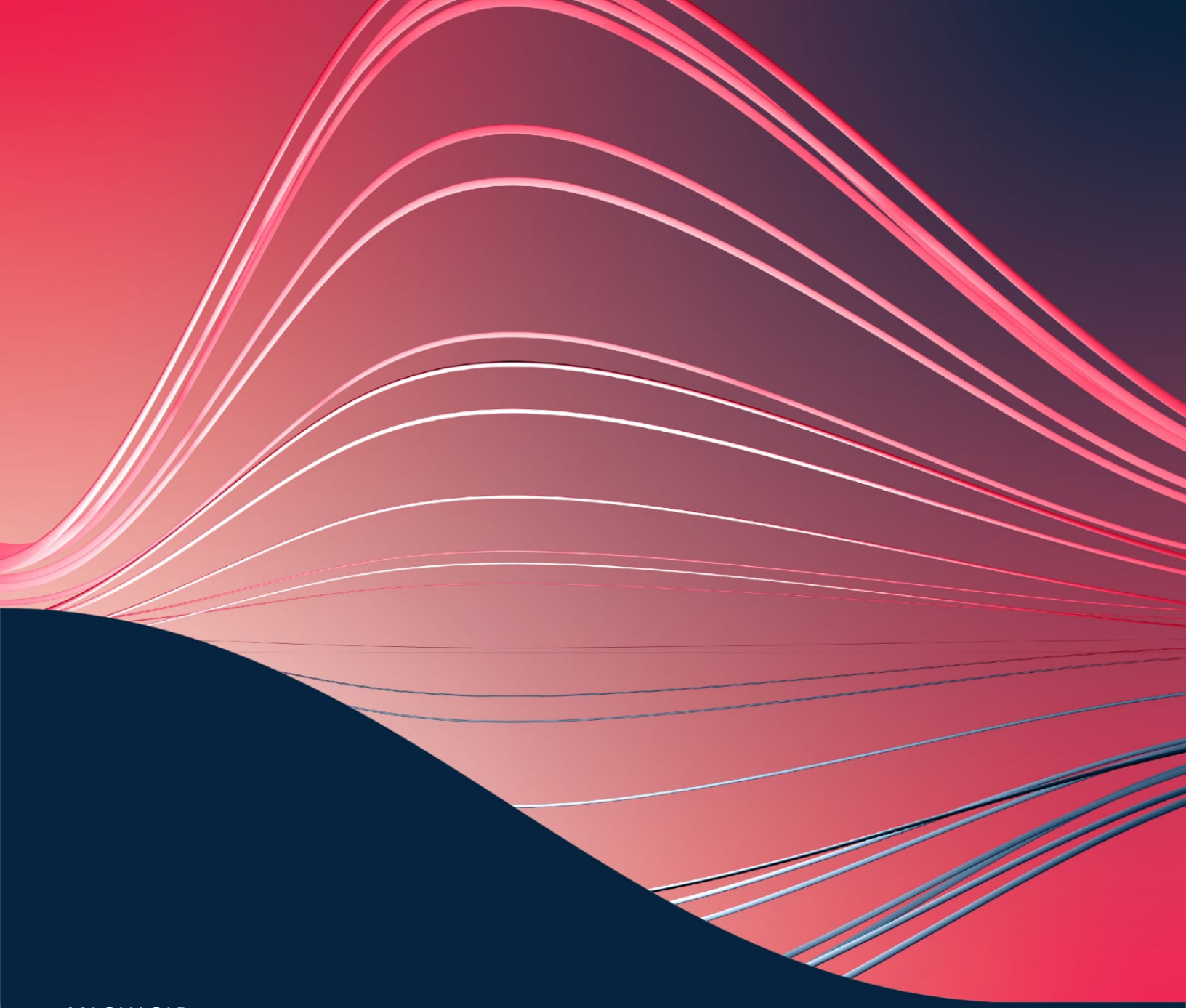


MACAU SAR

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

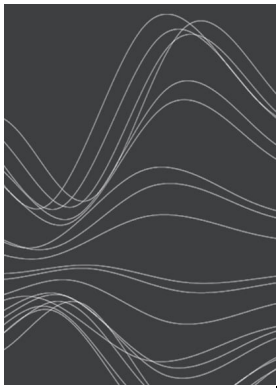
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

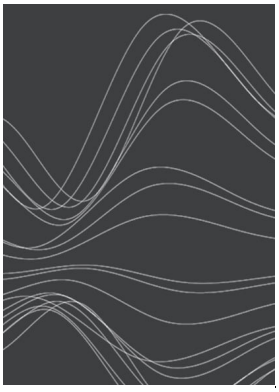
Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Macau SAR

LAST MODIFIED 19 DECEMBER 2023

Data protection laws

Macau Personal Data Protection Law no. 8/2005 of August 22nd (Law).

Definitions

Definition of personal data

The Law 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.

Definition of sensitive personal data

The Law defines sensitive personal data as 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.

National data protection authority

The Office for Personal Data Protection (OPDP) is the Macau regulatory authority responsible for supervising and coordinating the implementation of the Law.

Registration

The OPDP 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 OPDP.

The OPDP provides (official) forms that must be submitted regarding personal data processing, either in Portuguese or Chinese language, along with the following information (if applicable):

- Identification and contact details of the data controller and its representatives;
- The personal data processing purpose;
- Identification and contact details of any third party carrying out the personal data processing;
- The commencement date of the personal data processing;
- The categories of personal data processed (disclosing whether sensitive personal data, data concerning the suspicion of illicit activities, criminal and / or administrative offenses or data regarding credit and solvency are to be collected);
- The legal basis for processing personal data;
- The means and forms available to the data subject for updating his or her personal data;
- Any transfer of personal data outside Macau, along with the grounds for, and measures to be adopted with, the transfer;
- Personal data storage time limits;
- Interconnection of personal data with third parties; and
- Security measures adopted to protect the personal data.

Data protection officers

There is no legal requirement to appoint a data protection officer in Macau.

Collection and processing

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

- 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;
- Compliance with a legal obligation to which the data controller is subject;
- Protection of vital interests of the data subject if he or she is physically or legally unable to give his or her consent;

- 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
- 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.

The data subject must be provided with all relevant processing information, including the 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.

Transfer

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 OPDP.

In view of the close relationship with Mainland China and the entry into force of the Chinese Personal Information Protection Law ("**PIPL**") with extraterritorial effect, the Macao Office for Personal Data Protection (OPDP) 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 Macao.

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.

Breach notification

The Law does not require data controllers to notify either the OPDP or data subjects about any personal data breach.

However, a new Law on Cybersecurity came into effect in 2019, which implemented the 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.

Enforcement

Violations of the Law are subject to civil liability and administrative and criminal sanctions, including fines and / or imprisonment.

Electronic marketing

Under the Law, 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.

Online privacy

The Law also applies in the online environment.

For example, a Macau company that collects personal data from Macau residents through its website (e.g. through cookies) must fulfil all obligations under the Law imposed on data processors. In particular, the Macau company must inform data subjects of the personal data processing purpose and notify the OPDP about the personal data processing.

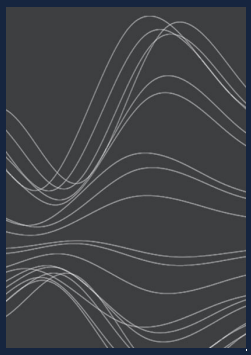
Data protection lawyers

José Leitão
Partner
MdME
jose.leitao@mdme.com
View bio

Daniela Guerreiro
Associate
MdME
daniela.guerreiro@mdme.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com