

## LEGAL ALERT

### CYBERSECURITY LAW

In keeping with latest regulatory trends, Macau has passed Law No. 13/2019 on 24 June 2019, regulating local legal requirements for Cybersecurity (the “**Cybersecurity Law**”), which creates public departments and private entities in order to maintain the security of the city’s “*critical infrastructure*” in respect of information technology.

By setting out various obligations and duties, the Cybersecurity Law requires key infrastructure operators to properly manage their information networks and formulate an information network management system, including proper management of information related to the public, to raise awareness of prevention and protect the privacy of the public. The Cybersecurity Law creates a preventive and remediation framework, as opposed to the existing law on computer crimes (Law No. 11/2009), which punishes computer crimes.

#### CRITICAL INFRASTRUCTURE

- **Public Sector:** All public departments, bodies and entities;
- **Private Sector:** Important industries in the society, such as water and electricity supply, telecommunications, internet services, television and radio broadcasting, hospitals, public transportation, waste collection and disposal, gaming concessionaires, financial and insurance institutions.

#### CYBERSECURITY SYSTEM

Under the Cybersecurity Law, the local Cybersecurity System is composed by the following:

- The Cybersecurity Committee, which is chaired by the Macau Chief Executive;

- The Cybersecurity Incidents Alert and Response Centre, under the coordination of the Macau Judiciary Police; and
- The Cybersecurity Supervisory Entities.

## **DUTIES AND OBLIGATIONS**

### For Private Entities

- Creation of internal cybersecurity procedures;
- Appointment of cybersecurity officers;
- Creation of procedural, preventive and reactive methods
- Self-assessment and reporting obligations; and
- Cooperation duties.

### For Public Entities

- Appointment of a manager responsible for implementing the necessary and relevant measures;
- Creation of procedural, preventive and reactive, self-assessment cooperation mechanisms;
- Review and implementation of contracts for the provision of cybersecurity services with private entities.

## **PENALTIES**

### Fines

- From a range of MOP50,000 to MOP5,000,000.

### Additional sanctions (maximum period of up to two years)

- Prohibition of participating in public tenders for the acquisition of goods or services by public authorities; or
- Suspension of benefits or financial aids.

[José Leitão \[+info\]](#)

[João Faria \[+info\]](#)

***Disclaimer: The information contained herein is for informational purposes only and is not intended to constitute legal advice. As legal advice must be tailored to the specific circumstances of each case, nothing provided herein should be used as a substitute for advice of a qualified lawyer in Macau.***