Overview of the personal data protection and cybersecurity laws in Macao

Cebu, December 2019

Personal Data Protection Act

General Information

- Legal system in Macao: civil law system
- Law no. 8/2005 (PDPA) established the legal regime on the processing and protection of personal data
- Effective from Feb. 2006
- Similar to the then Portuguese PDPA (Law No. 67/98), thus closely related to the EU Directive 95/46/EC
- The supervisory authority: Office for Personal Data Protection (OPDP)

Some Key Features

- Sensitive Data
- Cross-border data flow
- Notification and authorization scheme
- Enforcement

Sensitive Data

Conditions of Legitimacy - sensitive data

- The processing of sensitive personal data is prohibited
  1. philosophical or political beliefs
  2. political society or trade union membership,
  3. Religion
  4. privacy
  5. racial or ethnic origin
  6. data concerning health or sex life, including genetic data
- Derogations specified in Article 7 (explicit consent, legal provisions, OPDP authorizations, among others).

CROSS-BORDER DATA FLOWS

Restriction on cross-border data flows

- A system similar to that of EU
- Requirement of an adequate level of data protection (Article 19), but White List not available yet
- Derogations (Article 20): by notification or authorization, under strict conditions

Derogations - Notification

It may be allowed on condition that the public authority is notified, and that the data subject has given his consent unambiguously to the proposed transfer, or if that transfer:

(1) 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;

(2) is necessary 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;

(3) is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims;

(4) is necessary in order to protect the vital interests of the data subject;

(5) is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

Derogations - Authorization

the public authority may authorise a transfer or a set of transfers of personal data to a destination in which the legal system does not ensure an adequate level of protection within the meaning of No. 2 of the previous article, provided the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses.

Derogations - Others

A transfer of personal data which is necessary for the protection of defence, public security and public health, and for the prevention, investigation and prosecution of criminal offences, shall be governed by special legal provisions or by the international conventions and regional agreements to which the MSAR is party.

Notification and authorization scheme

What requires a notification?

Basic: the automatic processing of personal data [Article 21(1)]

- The controller or his representative, if any, must notify the public authority in written form within eight days after the initiation of any wholly or partly automatic processing operations or set of such operations intended to serve a single purpose or several related purposes.

Others:

- Some kinds of sensitive data processing [Article 21(5)]
- Some exemptions from the obligation to provide information [Article 10(5)]
- Some kinds of transferring personal data outside the MSAR [Article 20(1)]

What requires an authorization?

1. Processing sensitive data, on important public interest grounds and such processing is essential for exercising the legal or statutory rights of the controller. (Article 22(1)(1))
2. Processing credit and solvency data (Article 22(1)(2))
3. Combination of data (Article 22(1)(3))
4. Change of purpose (Article 22(1)(4))
5. Extending the data preservation period (Article 5(2))
6. Transferring personal data outside the MSAR, without the conditions for a notification (Article 20(2))
7. Transitional provision for manual filing systems existed before the date the PDPA coming into force(i.e., February 19th, 2006) (Article 45(3)).

Transparency –
Registration and its publication [Article 25(1)]

- When personal data processing is not covered by a legal provision or statutory regulations with organizational nature, and must be authorised or notified, it shall be set down in a public authority register open to consultation by any person.

The register shall include the following information: [Article 25(2)]

- the name and address of the controller and of his representative, if any;
- the purposes of the processing;
- a description of the category or categories of data subjects and of the data or categories of personal data relating to them;
- the recipients or categories of recipients to whom the data might be disclosed and in what circumstances;
- proposed transfers of data to third countries;

simplification or exemption [(Article 20(2)]

- The public authority may authorize the simplification of or exemption from notification for particular categories of processing which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of the data subjects and to take account of criteria of speed, economy and efficiency.

- (Please check our website for more information about these decision on simplification or exemption)

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
個人資料保護辦公室
Gabinete para a Protecção de Dados Pessoais

公開資料（個人資料處理登記）

Informações para consulta pública (Tratamento de dados pessoais)

登記編號： Registo n.º：	R0093/2018/GPDP	
負責處理資料的實體： Nome do responsável pelo tratamento：	中文 Chinês：	治安警察局
	葡文 Português：	Corpo de Polícia de Segurança Pública
	英文 Inglês：	Macao Public Security Police Force
實體的地址： Endereço：	澳門十月一號前地治安警察局總部大樓	
處理的目的： Finalidades do tratamento：	(1)輔助執法； (2)監督及檢討人員執法過程。	
資料當事人類別： Categorias de titulares dos dados：	本局人員若配置隨身攝錄機執勤時當開啟錄制模式下，在錄影及錄音範圍內之人士。	
個人資料種類： Categorias dos dados：	- 懷疑從事不法行為、刑事或行政違法行為的資料 - 有監察性質的資料	- Suspeitas de actividades ilícitas, infracções penais e infracções administrativas - Dados com natureza de fiscalização
資料的通告： Comunicação de dados：	接收者或接收者的類別： Destinatários ou categorias de destinatários：	告知資料的條件： Condições de comunicação：
	執法機關	涉及違反犯罪之調查或應執法機關要求
	負責刑法，行政，紀律，投訴卷宗調查之人員	涉及刑事，行政，紀律，投訴卷宗之調查
將個人資料轉移到澳門特區以外的地方： Transferência de dados pessoais para local situado fora da RAEM：	沒有轉移	Não existe transferência
歷史記錄： Historial do ficheiro：	登記日期： 2018-05-21	Registado em： 2018-05-21

Enforcement

Violation of the PDPA

- Administrative Offense: fine up to MOP 200,000 (GPDP is responsible for the investigation and imposing sanctions)
- Crime: up to 4 years imprisonment (Public Prosecutor)

Case 1 – Google Street-view (0013/2010/IP)

- Capture of images without consent, including some inside the residence.
- Collection of Wi-Fi data.

Violations:

1. Illegal collection of sensitive data (MOP $10000)
2. Illegal collection of Wi-Fi data (MOP $10000)
3. Illegal transfer of data (MOP $10000)

Case 2 – A beauty center (0041/2010/IP)

A beauty center used the image data (before and after plastic surgery)of a client, who is also its former employee, collected for surgery purposes, for printing promotional leaflets. It is unclear when and why the outsourced company in mainland China downloaded the photos from its computer.

Violations:

1. Illegal utilization of sensitive data (not sanctioned, data collected before law enactment).
2. Lack of data security (MOP $4000)
3. Illegal transfer of data (MOP $8000)

Cybersecurity Law

General Information

- Law no. 13/2019
- Effective from Dec. 21, 2019
- Administrative Regulation no. 35/2019 further defines the functioning of the governance system
- The objectives: to establish and regulate the cybersecurity system, to protect the network, system and data of the critical infrastructure operators

Some Key Features

- Critical infrastructure
- governance system
- Obligations
- Enforcement / Sanction

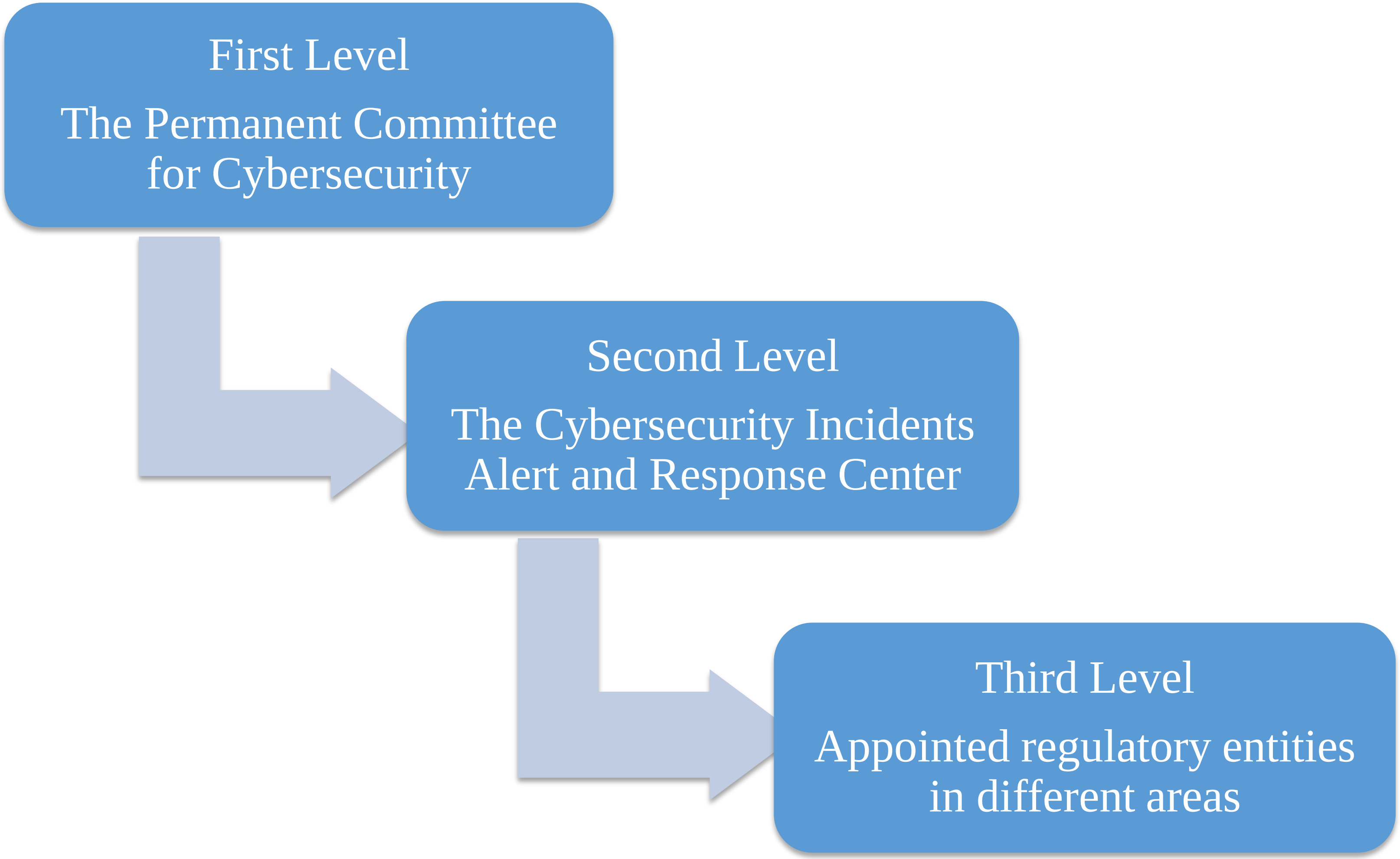
critical infrastructure and its operators

- Critical infrastructure: entity’s assets, networks and computer systems that if disrupted, disclosed, suspended, or significantly slowed down, would potentially endanger public welfare, safety, or order.

(banking, finance, insurance, gambling, telecommunication or healthcare, etc..)

- Critical infrastructure operators: public and private entities operating the critical infrastructure.

Cybersecurity governance system



First Level

The Permanent Committee for Cybersecurity

Second Level

The Cybersecurity Incidents Alert and Response Center

Third Level

Appointed regulatory entities in different areas

First Level: Permanent Committee for Cybersecurity

Led by the Chief Executive. Its roles are:

- Defining the guidelines, objectives and strategies towards cybersecurity goals.
- Supervising the related entities’ activities inside the cybersecurity system.
- Suggesting government to have agreement with public and private entity to protect local cybersecurity.

- The coordinator of OPDP is a member of this Committee.

Second Level: Cybersecurity Incidents Alert and Response Center

Composed of the Judiciary Police (Coordinator), the Public Administration & Civil Service Bureau, and the Macao Post and Telecommunications Bureau. Its roles are:

- Collecting information about cybersecurity incidents.
- Developing cybersecurity incident response plan.
- Providing technical support.
- Responsible for monitoring the traffic pattern of data transmission between networks of the critical infrastructure operators and the internet.

Third Level: Appointed regulatory entities in different areas

- A: Public Administration & Civil Service Bureau: supervising public critical infrastructure operator.
- B: Another 11 government departments: supervising private critical infrastructure operator.
- Their roles: Supervising critical infrastructure operators activities and enforcing of the law (in the relevant area)

Obligation of private critical infrastructure operators

Organizational obligations

- Establish and run a cybersecurity management unit capable to implement internal security measures relating cybersecurity.
- Appoint / set up delegated and competent cybersecurity officer (with Macao residency) / to manage IT security.
- Ensure that the cybersecurity officer can be reached by the Cybersecurity Incidents Alert and Response Center.
- Establish a complaint and reporting mechanism for cybersecurity.

Procedural, preventive and contingency obligations

- Develop and adopt cybersecurity management system and operational procedures, and internal measures for security incident monitoring and response.

- Inform (the Cybersecurity Incidents Alert and Response Center / the relevant regulatory entity) about cybersecurity incidents, including examination and recording of status of the information network.

Self - assessment and reporting obligations

- Engaged internal / external professionals to conduct cyber security assessment / audit.
- Submit cybersecurity report, including annual incident report (if applicable) to relevant regulatory entities.

Cooperative obligation

- Cooperate with and provide support to the Cybersecurity Incidents Alert and Response Center / the relevant regulatory entity (i.e. regulators) for their inspection and investigation.

Enforcement/Sanction for non-compliance:

- Issuing Warnings

- If the private critical infrastructure operator could fix mistakes within the required period set by the regulator.

- Administrative offense : Monetary Penalty

- two levels Monetary Fines (minor and severe)
- First level: from MOP 50,000 to 150,000
- Second level: from MOP 150,000 to 5,000,000

From the perspective of OPDP as the PDPA regulator on PD security

- It complements and reinforces the data security requirements (Article 15 of PDPA, data controllers must implement appropriate security measures)
- Indirectly it brings new requirements of Compulsory Data Breach Notification for those CI operators
- No direct effect for non-CI operators

Thank you!

www.gpdp.gov.mo