CROSS-BORDER DATA FLOWS IN MACAO

Personal Data Protection Act

- Law no. 8/2005
- Effective from Feb. 2006
- Similar to the Portuguese PDPA, thus closely related to the EU Directive 95/46/EC
- Legal system in Macao: Romano-Germanic law system (civil law system)
- The supervisory authority: Office for Personal Data Protection (GPDP)

Restriction on cross-border data flows

- A system similar to that of EU
- Requirement of an adequate level of data protection
- Derogations: by notification or authorization, under strict conditions

Article 19
Principles

- 1 - The transfer of personal data to a destination outside the MSAR may only take place subject to compliance with this Act and provided the legal system in the destination to which they are transferred ensures an adequate level of protection.
- 2 – The adequacy of the level of protection referred to in the previous number shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the place of origin and place of final destination, the rules of law, both general and sectoral, in force in the destination in question and the professional rules and security measures which are complied with in that destination.
- 3 – It is for the public authority to decide whether a legal system ensures an adequate level of protection referred to in the previous number.

Article 20
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.

Article 20
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.

Article 20
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.

Practical Problems

- The WHITE LIST is not available
- The common and frequent cross-border data flows in reality

Common cross-border data flows

For Data controllers in Macao

- Data processor outside Macao – outsourcing, servers and service providers outside Macao, remote IT support, cloud computing;
- Data recipient outside Macao – the third party, the parent company;

Common cross-border data flows

For Data controllers outside Macao

- Collecting / processing data in Macao
- Data processor inside Macao

Complaint from businesses

- Bureaucratic procedures
- Inefficiency
- Not effective in data protection
- Lack of ways to deal with legacy

From a supervising authority's view

- Data protection as fundamental human rights.
- Necessary in this digital world – one second to the whole world, undeletable.
- The core problems are always the incompliance in data processing legitimacy and data security, rather than that in the procedure. The latter is always a way to find out the former.

Conditions of Legitimacy - General

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

(1) for the performance of a contract or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate;

(2) for compliance with a legal obligation to which the controller is subject to;

(3) in order to protect the vital interests of the data subject if the latter is physically or legally incapable of giving his consent;

(4) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

(5) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

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.

Additional concern

- Data security
- The nature of legal obligations in foreign jurisdiction
- The loss of control over data, while obligations regarding data protection remain

Case 1 – Google Street-view

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

Case 1 – Google Street-view

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

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.

Case 2 – A beauty center

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)

Case 3 – A hotel

A hotel disclosed the information of its clients, including accommodation and consumption details, to an investigator came from its parent company in US, investigating a director of the parent company.

Case 3 – A hotel

Violations:

1. Illegal disclosure of sensitive data (MOP $10000)
2. Illegal transfer of data (MOP $10000)

Case 4 – A company

A company sent raw data of its employees, clients, etc, to its parent company in US, to prepare a possible lawsuit.

Case 4 – A company

Violations:

1. Illegal disclosure of data (pre-trial discovery in this case is not recognized as legitimate in Macao) (MOP $20000)
2. Illegal transfer of data (MOP $20000)

Case 5 – A school's enquiry

- A school intends to purchase from an Indian company its cloud-computing services, but server locations unidentified.
- The contract between the two parties may make the school a surrender of legal protection on data security.
- The school will remain the ultimate responsible party for the data breaches.
- Some school data may be sensitive.
- There seems no way for the school to keep the data secure under this arrangement.
- GPDP does not recommend.

Conclusion

- When data protection problems arise in cross-border data flows, the most important issues always originate from the legitimacy of personal data processing rather than the procedural requirements.
- Data security also plays an important role.
- Obligations to protect data remain.

Practical suggestions to business

- Always focus on the legitimacy of data processing
- Always pay attention to data security
- When legitimate and secure, it is not very difficult to find a solution in cross-border data transfer – notification or authorization
- Notification is always the priority

Challenges to GPDP

- The white list
- APEC CBPR not feasible