Features of Macao’s Personal Data Protection Regime and Culture
PART I – Brief Notes on Macao

PART II – Personal Data Protection Act of Macao

PART III – Evolution of “Personal Data Protection” in Macao

PART IV – Future Prospects and challenges
PART 1

BRIEF NOTES ON MACAO
MACAO
Special Administrative Region of the People’s Republic of China
General Information:

- **Location:** Western end of the Pearl River delta
- **Area:** 30.5 KM$^2$
- **Population:** 648,000, with composition of Chinese being the majority
Political/Legal Background:

- Under Portuguese administration before 1999
- Portuguese matrix evolving under local conditions
- Public administration structure and judiciary system in European style
- Handover to People’s Republic of China in 1999
- “Localization” arrangements brought smooth transition

East–Meet–West Culture
Under “One Country, Two Systems” principle, the Socialist System doesn’t apply.

- Widely known for casinos and gambling business
- Gambling had long been its economic pillar particularly after the decline of local manufacturing industry in the 80’s
- Monopoly Gambling system ended in 2002 when concessions were granted to six companies and foreign capital largely invested into gambling-related tourism business
Social Condition:

- Positioning as World Centre of Tourism and Leisure
- Heading to transformation into a “Smart City”
- Gambling related tourism being the mainstays of economy and support of labour force
- In 2016, visitors reaching 31 million, of which 28 million came from mainland China
- Residents inhabit the unique culture of “East-meet-West”
PART II

PERSONAL DATA PROTECTION ACT OF MACAO
General Legal Background:

Macau Special Administrative Region of P. R. China

“One Country Two Systems”

“Macao people ruling Macao”

“High Degree of Autonomy”
Basic Law stipulations:

- Executive Power
  - Legislative Power
  - Independent Judicial Power [final adjudication]

Political autonomy includes: finances, taxation, currency, separate customs, culture, tourism, science, sports

excludes: foreign affairs, defense
Personal Data Protection in different levels:

- **Constitutional Protection under the Basic Law (1993)**
  - Right to the privacy of private and family life (art. 30)
  - The freedom and privacy of communication (art. 32)

- **Fundamental Protection under «Civil Code» (1999):**
  - Right of Access (art. 79/1)
  - Principles of Data Collection (art. 79/2)
  - Enforcement by a Public Authority (art. 79/3)

- **Fundamental Protection under «Criminal Code»:**
  - Penalty to infringement of private life (art. 186)
  - Penalty to infringement of personal data (art. 187)

- **Principal Protection under «Personal Data Protection Act» (2005)**
Enforcement Agency

Established by Dispatch of Chief Executive no. 83/2007

OFFICE FOR PERSONAL DATA PROTECTION

- operates independently
- accountable towards Chief Executive
- exercises the legal competence in supervising and coordinating the public implementation of and compliance with the Personal Data Protection Act in both public and private sectors
Main duties and tasks of OPDP:

- Supervises personal data processing through submissions of notification and application for authorisation
- Addresses requests for opinions
- Handles complaints against misconduct on data processing
- Carries out investigations and imposes sanctions whenever administrative offenses are detected
- Assists different sectors to establish corresponding codes of conduct
- Launches promotions and educations to foster the implementation of the data processing regime
International and Regional Participation of OPDP:

- Member of APPA
- Member of GPEN
- Observer of ICDPPC
The stipulations of PDPA were mostly drawn from the Portuguese law 68/98 that transposed the EU Directive 95/46/CE.
Features of the Personal Data Protection Act (PDPA)

- Notification
- Authorisation
- Combination of Personal Data
- Transfer of Personal Data outside the MSAR
Article 21 - Obligation of notification

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

2. The public authority may authorise 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.

3. The authorisation shall be published in the *Official Gazette* of the MSAR and must specify the purposes of the processing, the data or category of data to be processed, the category or categories of data subjects, the recipients or categories of recipients to whom the data may be disclosed and the length of time the data are to be stored.

4. Processing whose sole purpose is the keeping of a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest shall be exempted from notification.

5. The non-automatic processing of the personal data provided for in paragraph 1 of Article 7 shall be subject to notification when they are processed under subparagraph (1) of paragraph 3 of that Article.
Data controller shall notify OPDP in writing within 8 days of the initiation of data processing in situations as listed below:

- Automatic processing of personal data - Article 21(1) of the PDPA
- Processing of sensitive data - Articles 7(3)(1) and Article 21(5) of the PDPA
- Exemption from the obligation to provide information - Article 10(5) of the PDPA
- Transferring personal data outside the MSAR - Article 20(1) of the PDPA
Applications for OPDP’s authorisation needed to be made prior to the data processing under any of these conditions:

- Processing sensitive data - Article 22(1)(1) of the PDPA
- Processing credit and solvency data - Article 22(1)(2) of the PDPA
- Combination of data - Article 22(1)(3) of the PDPA
- Change of purpose - Article 22(1)(4) of the PDPA
- Extending the data preservation period - Article 5(2) of the PDPA
- Transferring personal data outside the MSAR - Article 20(2) of the PDPA
## Authorisations about notification obligation

<table>
<thead>
<tr>
<th>Authorization No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/2014</td>
<td>Simplified Notification for the Personal Data Processed by vehicle Positioning Systems and Devices</td>
</tr>
<tr>
<td>02/2013</td>
<td>Exemption from the Notification Obligation Data Processing for the Purpose of Election Campaign</td>
</tr>
<tr>
<td>01/2013</td>
<td>Simplification of Notification Obligation The Processing of Personal Data by Video Surveillance System for Security purposes</td>
</tr>
<tr>
<td>02/2011</td>
<td>Exemption from the Notification Obligations Processing of Admission Data by Educational Institutes</td>
</tr>
<tr>
<td>01/2011</td>
<td>Exemption from the Notification Obligations Processing of Recruitment Data</td>
</tr>
<tr>
<td>04/2008</td>
<td>Exemption from the Obligation of Notification Data Registration and Processing Relating to Registration of Entries and Exits of Visitors</td>
</tr>
<tr>
<td>Authorization No.</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>03/2008</td>
<td>Exemption from the Obligation of Notification Personal Data Processing Relating to Users of Libraries and Archives</td>
</tr>
<tr>
<td>02/2008</td>
<td>Exemption from the Obligation of Notification Personal Data Processing by Educational Institutions Relating to Students</td>
</tr>
<tr>
<td>01/2008</td>
<td>Exemption from the Obligation of Notification Personal Data Processing Relating to Billing and Contact Information of Clients, Suppliers and Service Providers</td>
</tr>
<tr>
<td>03/2007</td>
<td>Exemption from the Obligation of Notification Data Processing Relating to Non-Profit Legal Person’s Collection of Membership Fees or Contact with Members</td>
</tr>
<tr>
<td>02/2007</td>
<td>Exemption from the Obligation of Notification Data Processing Relating to Administration of Employees and Service Providers</td>
</tr>
<tr>
<td>01/2007</td>
<td>Exemption from the Obligation of Notification Data Processing Relating to Remunerations, Payments and Welfare Benefits</td>
</tr>
</tbody>
</table>
Combination of Personal Data
(Article 9)

1. The combination of personal data not provided for in a legal provision or a provision of a regulation of an organic nature shall be subject to the authorisation of the public authority, requested by the controller or jointly by the corresponding controllers under paragraph 1 of Article 22.

2. The combination of personal data must:
   (1) be necessary for pursuing the legal or statutory purposes and legitimate interests of the controller;
   (2) not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects;
   (3) be covered by adequate security measures; and
   (4) take account of the type of data to be combined.
74 authorizations for combination of Personal Data Processing have been granted until June 2017, 67 of which remain in force.

- **54** involve Public Sector entities only
- **1** involves a Public Entity and a private Hospital
- **12** involve Private Sector controllers
<table>
<thead>
<tr>
<th>Authorization No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/A/2016/GPDP</td>
<td>Combination of identity and medical information of the participants of the eHR Pilot Scheme, between the Health Bureau and the Kiang Wu Hospital</td>
</tr>
<tr>
<td>01/A/2015/GPDP</td>
<td>The Labour Affairs Bureau (DSAL) receives information of the beneficiaries and employers of the social security system from the Social Security Fund (FSS) through data combination</td>
</tr>
<tr>
<td>02/A/2015/GPDP</td>
<td>The Courts of Macao Special Administrative Region receives information of the beneficiaries and employers of the social security system from the Social Security Fund (FSS) through data combination</td>
</tr>
<tr>
<td>03/A/2015/GPDP</td>
<td>The Industrial and Commercial Development Fund (FDIC) receives information of the data subjects recorded in the Business Registry from the Legal Affairs Bureau (DSAJ) through data combination</td>
</tr>
<tr>
<td>04/A/2015/GPDP</td>
<td>The Social Welfare Bureau receives the data of the beneficiaries of the social security system from the Social Security Fund through data combination</td>
</tr>
</tbody>
</table>
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 preceding paragraph 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 preceding paragraph.
1. A transfer of personal data to a destination in which the legal system does not ensure an adequate level of protection within the meaning of paragraph 2 of the preceding Article 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 where one of the following conditions is met:

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

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

(5) it 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.

2. Without prejudice to paragraph 1 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 paragraph 2 of the preceding 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.

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

EVOLUTION OF “PERSONAL DATA PROTECTION” IN MACAO
1980’s

- Small city of little population
- Relatively close interpersonal relationship
- Social situation rather stable and conservative
- Concept of privacy and of personal data protection amongst people not yet appeared

1990’s

- Population grew due to increase of immigrants from Mainland China
- Modernization of society through common use of computerised and digital products
- Lifestyle underwent enormous change as social media and instant messaging software popularized
- Concept of privacy amongst people began to be recognised while most people moved to flats from blockhouse
2000’s

• Accelerating economic growth contributed from gambling concessions
• Sudden sharp rise in demand for foreign labour and brought in a diversification of lifestyle in harmony
• Social situation changed to be more internationalized and open
• Concept of right of data protection amongst people gradually formed and later on legalized following its rapid development in Europe and Asia

2010’s

• Internet and AI technology take the dominant and leading position
• BIG DATA is the key to success
• Right of data protection is emphasized and highlighted as never before
• Conflict between Right of Data protection and Freedom of Information Flow always in discussion
• Data Protection becomes a global issue
Investigations

No. of Cases

- 2007: 22
- 2008: 35
- 2009: 47
- 2010: 63
- 2011: 86
- 2012: 118
- 2013: 141
- 2014: 194
- 2015: 155
- 2016: 224
The ongoing ascending figure of requests and investigations demonstrates, on one hand, the **actual demands** of stronger implementation of the Personal Data Protection Act, and, on the other, the rising awareness and concerns about personal data protection, to which constant publicity and promotion works on the Act contribute the most.
While OPDP invests greatest efforts to combat data breaching incidents, the office values prevention and public education its core tasks and endeavors to enhance public awareness of personal data protection through publicity and promotion works in a broad area:

- Organising Training Courses, Seminars, Campaigns and Events
- Producing Announcements and Advertisements via video, audio as well the internet channels
- Distributing Publication of printed materials
- E-Training made available at website
- Offering degaussing service to all public departments and Non-Tertiary Education institutions for free
Case Sharing

Case I - Personal Photos publicized on a social networking site
Case II - Personal data transfer to foreign servers
Case III - Inappropriate use of images captured by a clinic’s surveillance system
Case IV - Private CCTV cameras installed by flat owner
Complainants A together with B lodged a complaint against C, who established and managed Page Y of a social website. Photos that showed both A and B were publicized in the said page without their prior consent. Negative comments were also found in that publicly accessible post as a way to condemn their improper behaviour and to draw public attention.

Complainants requested investigation to the case.

Investigation File no.: (0104/2014/IP)
Case I – Result

- Imposed a penalty on C of MOP$8000 according to Article 33(2) of the PDPA, and
- Ordered C to remove the said posts of Page Y, as an additional penalty based on Article 43(1) of the same Law.
Complainant A earlier signed up for an activity held by Organization B.

A then found out that the server of B’s online application system was located outside Macao and suspected data of applicants being transferred outside Macao without their prior consent.

Investigation File no.: (0158/2014/IP)
OPDP imposed on Organization B a penalty of MOP$12,000 according to Article 33(2) of the PDPA for violation of transborder data flows.
Complainant A filed a report to OPDP, stating that Newspaper B published photos that showed his family member and himself when they were visiting Clinic C for therapy. The photos, according to the Complainant, were taken from the Clinic’s surveillance system, and thus, A believed that this was a violation of PDPA and wanted an investigation.

Investigation File no.: (0077/2015/IP)
Considering that the publication on Newspaper B created rather significant impact to the Complainant; but considering Clinic C’s cooperation during the investigation and that this was their first violation being a negligent, rather than intentional, act, the OPDP decided to impose a penalty of MOP$ 10, 000 to Clinic B, based on Article 33(1) and 35(1) of the PDPA.
Case IV – Description

This case stemmed from the installation of a number of CCTV cameras along the bottom edge of B’s balcony. These cameras, as the Complainant A claimed, pointed towards a public street and collected excessive data, therefore A asked OPDP’s investigation.

Investigation File no.: (0128/2015/IP)
B installed cameras in balcony for household security purpose while some excessively captured images of his neighbours and the public street. Being without proper consideration of the interests and rights of other data subjects, the data processing of these cameras could not be legitimimized under Article 6(5) of PDPA.

OPDP asked B to remove all the cameras that were contrary to the PDPA requirements and the case was closed after the removal.
PART IV

FUTURE PROSPECTS AND CHALLENGES
While being the independent enforcement agency, the Office for Personal Data Protection, established in 2007, is still defined as a project team, temporary in nature, and successively extended.

The Office was not established by an Act and operates without a permanent legal basis.

The lack of a status of permanent independence may sometimes hinder our ability to fully cooperate with foreign enforcement agencies during practical investigation work.

Absence of permanent statutory independence confines our participations in global activities.
Bill for an Organic Law is ready to move forward for legislative procedures

New premises for the Office, improved hardware equipment and facilities, allowing for future development of OPDP

Critical challenges expected during the development of the upcoming Smart City projects

Work together and emerge stronger from those challenges ahead by turning them into opportunities for the development of data protection
“We are going from an interconnection world to an interdependent one.

We’re moving into a world where machines and software can analyze (see patterns that were always hidden before); optimize (tell a plane which altitude to fly each mile to get the best fuel efficiency); prophesize (tell you when your elevator will break and fix it before it does); customize (tailor any product or service for you alone) and digitize and automate just about any job.” (Aug. 2, 2017, The New York Times)
We come together and create that interdependent world, by connecting walls of personal data protection built by every jurisdiction. A regulatory system makes the biggest contribution when many of them netted together as a whole holistically form the barrier for data breach and mend those loopholes.
Office for Personal Data Protection

P.O. Box: P.O. Box 880, MACAU
Tel: (853) 28716006
Fax: (853) 28716116
Email: info@gpdp.gov.mo

For more information, visit us at www.gpdp.gov.mo
THANK YOU!