Office for Personal Data Protection

Annual Report

2012

Unofficial English Translation

Disclaimer

This is an unofficial English translation of some major chapters in the Annual Report 2012 of the Office for Personal Data Protection. It does not include any legal documents published in the Annual Report, namely Opinions and Authorisations. Please visit the Office’s website www.gpdp.gov.mo to get some of their available translations.

We regret that a full English translation of the Annual Report is not provided. Please note that the official languages in Macao SAR are Chinese and Portuguese. You should not act or rely on any unofficial English translation of legal documents without seeking legal advice when appropriate.

Office for Personal Data Protection
Government of Macao SAR
July, 2013
Preface

The Office for Personal Data Protection (GPDP) has gone through five years since its inception in 2007. Due to the inadequate awareness of the Personal Data Protection Act (PDPA) by the public at the beginning, as well as limited human resources, GPDP has encountered some challenges in respects of law enforcement and law promotion. Thanks to the full support of the Chief Executive, the active cooperation of many public and private institutions and the persistent efforts by all GPDP’s staff, we have been able to push the work ahead steadily, both in terms of case investigations or law promotion.

The GPDP has always been proceeding along the line of “awareness and education first, penalty second” in our work; however, appropriate disclosure of cases involving punishment for violations of the PDPA not only helps improve the transparency of our work, but also warns the residents to carefully handle personal data of their own and others to avoid suffering damages or breaking the law inadvertently. At a press conference held in early 2012, we released the investigation outcome and decisions of several cases, including the case of Google Street View Cars collecting imaginary and Wi-Fi network information in Macao; a public department recorded phone calls without obtaining callers’ consent, in order to alert the society.

In addition to initiating case investigations and announcing the results of such cases, the GPDP also offered opinions on issues relating to the PDPA. For example, prior to the formulation of Law 2/2012—the Legal Regime of Video Surveillance in Public Spaces—by the Legislative Assembly, the GPDP offered opinions on personal data protection. After the enforcement of the Law, GPDP formulated the opinion document *The Basic Principles to be Observed When Video Surveillance Systems Are Installed in Public Spaces.*

As the regulatory authority in charge of the implementation of the PDPA in Macao, GPDP is deeply convinced that promoting public awareness of this law is as important as its implementation. Since its inception in 2007, GPDP has held more than 310 presentation seminars, lectures and training courses, attracting more than 14,000 participants. In terms of law publicity in the future, we will continue the constant work in order to enhance citizens’ awareness of the PDPA at different levels. At the same time, GPDP has been conducting law promotion in various forms and through various channels to adapt to different targets. During 2012, new attempts have been made, for instance, the first four-panel cartoon competition on the Personal Data Protection Act, in a bid to promote personal data protection through cartoon; publicity information put up on the outside of buses of the three bus companies, communicating the PDPA to a large audience of the public; cooperation with the *Companhia de Electricidade de Macao* (CEM) to send leaflets to all local merchants and citizens, in order to deepen their awareness of personal privacy protection.

Furthermore, in order to safeguard their lawful interests, reduce the risks and costs of litigations and establish goodwill, the GPDP will assist the professional sectors to establish their own code of practice, which help promote their data
protection self-discipline work. For this purpose, in 2012 the GPDP published the document General notes on handling personal data by non-tertiary education institution, in order to more effectively protect the legitimate rights and interests of education institutions and their data subjects. On the other hand, to further simplify the administrative procedures and to optimize services, the GPDP developed the online query system for personal data processing registration, which aimed to facilitate residents accessing the database and to improve the transparency of public and private institutions in their personal data processing. In the future, the GPDP will continue to promote and improve the registration system of personal data processing in Macao, assist public and private institutions improving their personal data processing policies and to protect the citizens’ personal data according to the laws.

In addition to steadily promoting personal data protection in Macao and considering the frequent cross-border transfer of data, the GPDP actively participated, as an observer, in international conferences and exchange programs on personal data protection, so as to establish effective communication channels with personal data protection authorities of other countries or regions for greater cooperation and deeper exchanges. On the other hand, GPDP has regularly shared the development and law enforcement work of privacy protection of other neighboring countries and regions, exploring possibilities for cross-border cooperation and establishing joint investigations of illegal cross-border transfer of personal data and violation of personal data privacy.

It should be noted that after years of efforts the GPDP finally, in July 2012, became a member of both the Global Privacy Enforcement Network (GPEN) and the Asia Pacific Privacy Authorities (APPA). Although Macao is a small jurisdiction, it has the most stringent personal data protection law in the Asia Pacific region. The international community has been paying attention to Macao's enforcement of personal data laws. The fact of being an official member of international organizations not only allows the international community to know Macao better but also helps improve the protection of personal data through reinforced contact.

Overseas exchanges and participation in international conferences undoubtedly help the development of personal data protection in Macao. In mid-June 2012, GPDP took the opportunity of the 37th Asia Pacific Privacy Authorities Forum in Hong Kong and invited representatives of participants to Macao to participate the two events organized by the GPDP and the Legal Affairs Bureau on June 15th and 16th — Seminar on Policy and Practice of Personal Data Protection, and International Experience on Personal Data Protection Seminar. During the two events, members of the Portuguese National Data Protection Commission and academics from the Mainland introduced, to the staff of public and private institutions and legal professionals and academics in Macao, the personal data protection systems and experience in the Mainland, Europe, Portugal and the Asia Pacific region (including Hong Kong, Australia, New Zealand, Japan, Canada, Mexico, etc.). The participants further conducted in-depth exchanges and thus expanded their international visions, promoting the development of personal data protection in Macao.

In terms of connection with the neighboring areas, as direct marketing has become more active and local or overseas marketing calls or text messages have become more common, the GPDP, for better regulations of direct marketing and
privacy, organized the seminar Direct Marketing and Personal Data Protection in early November 2012. Experts and academics, officials and representatives of regulatory and law enforcement agencies from Mainland, Hong Kong and Macao were invited as keynote speakers, in order to share their experience and provide in-depth discussions with the respective local sector representatives.

Looking forward to 2013, GPDP, will fully utilize its resources to expand its network for international and regional cooperation, and committed to monitoring the implementation of the PDPA in Macao, pushing ahead the work relating to personal data protection. GPDP, however, is still a temporary organization without clear mandate and legal competence, and it could only act according to the PDPA and posed difficulties to its work. We hope that through the enactment of its organization law, GPDP will become an official data protection supervisory authority, so as to highlight the effectiveness of the law and duly protect the basic rights of the local residents’ data protection.

Coordinator

Chan Hoi Fan
Major events

2/2012

- Attending the Data Protection Awareness Seminar in Kuala Lumpur and the opening ceremony of the Malaysian Department of Personal Data Protection.

3/2012

- Press conference announcing investigation outcome.

6/2012

- Attending the 37th Asia Pacific Privacy Authorities Forum as an observer.
- The International Experience on Personal Data Protection Seminar organized by the GPDP.
- Representatives of the Caritas Macao - Suicide Prevention Services visiting the GPDP.

7/2012

- Visiting the Chinese Educators Association of Macao.
- Representatives of the Macao Catholic Schools Association visiting the GPDP.

9/2012

- Consultation meeting on the guidance document *General Notes on Handling Personal Data by Non-Tertiary Education Institution*.

10/2012

- Holding consultations on the Guidelines on Merchants’ Processing of Identification Documents of Payment Cardholders.
11/2012

- Direct Marketing and Personal Data Protection Seminar.
- Reviewing the four-panel cartoon competition on the Personal Data Protection Act.
- Participation in the IT Week 2012.

12/2012

- Attending the 38th Asia Pacific Privacy Authorities Forum as a member for the first time.
- Awards ceremony for the four-panel cartoon competition on the Personal Data Protection Act.
Processing of enquiries and complaints

I. Enquiries about law

In 2012, the GPDP received a total of 990 enquiries about personal data (excluding those regarding procedures), of which 989 were concluded. A majority (40.9%) of those applications involved legitimacy in personal data processing, followed by the rights of the data subjects, accounting for 23.5%. The enquiries were mainly made by phone, accounting for 87.6%. With regard to the categories of enquirers, public and private institutions accounted for the majority, in a total of 27.9% and 56.7% respectively.

As the GPDP carried out its work further, with a growing sense of personal data protection among the citizens, the recent years saw a huge increment in the number of enquiries. In 2011, the rate of the number of enquiries increased was 33.8%.

Figure 1 – Categories of enquiries by nature

<table>
<thead>
<tr>
<th>Nature of cases</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of application and definitions of the Personal Data Protection Act</td>
<td>190</td>
</tr>
<tr>
<td>Nature and principles of data processing</td>
<td>214</td>
</tr>
<tr>
<td>Legitimacy of data processing</td>
<td>405</td>
</tr>
<tr>
<td>Rights of data subjects</td>
<td>233</td>
</tr>
<tr>
<td>Security and confidentiality of data processing</td>
<td>58</td>
</tr>
<tr>
<td>Data combination</td>
<td>10</td>
</tr>
<tr>
<td>Data transfer</td>
<td>43</td>
</tr>
<tr>
<td>Notifications and authorizations</td>
<td>194</td>
</tr>
<tr>
<td>Consequences of violations of laws</td>
<td>25</td>
</tr>
<tr>
<td>Guidelines prepared by the GPDP</td>
<td>72</td>
</tr>
<tr>
<td>Rights to privacy provided for by other laws</td>
<td>26</td>
</tr>
<tr>
<td>Others</td>
<td>98</td>
</tr>
</tbody>
</table>

Note: Some enquiries involved more than one of categories listed above.

Figure 2 – Means of enquiry

<table>
<thead>
<tr>
<th>Means of enquiry</th>
<th>Number of cases</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>867</td>
<td>87.6%</td>
</tr>
<tr>
<td>Internet (Online Enquiry and E-mail)</td>
<td>82</td>
<td>8.3%</td>
</tr>
<tr>
<td>Personal visits</td>
<td>39</td>
<td>3.9%</td>
</tr>
<tr>
<td>Mail/fax</td>
<td>2</td>
<td>0.2%</td>
</tr>
</tbody>
</table>
Figure 3 – Categories of enquirers

<table>
<thead>
<tr>
<th>Categories of enquirers</th>
<th>Number of enquiries</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public institutions</td>
<td>153</td>
<td>15.4%</td>
</tr>
<tr>
<td>Private institutions</td>
<td>276</td>
<td>27.9%</td>
</tr>
<tr>
<td>Individuals</td>
<td>561</td>
<td>56.7%</td>
</tr>
</tbody>
</table>

Figure 4 – Increment of enquiries

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>43</td>
</tr>
<tr>
<td>2008</td>
<td>207</td>
</tr>
<tr>
<td>2009</td>
<td>602</td>
</tr>
<tr>
<td>2010</td>
<td>704</td>
</tr>
<tr>
<td>2011</td>
<td>740</td>
</tr>
<tr>
<td>2012</td>
<td>990</td>
</tr>
</tbody>
</table>
II. Case investigation

The GPDP identified a total of 118 cases to investigate in 2012, a 37.2% rise over the 86 cases in 2011. With the 59 cases from 2011, the GPDP investigated 177 cases, of which 118 were concluded (57 cases carried over from 2011, and 61 from 2012). Of the 118 new cases opened in 2012, 56.8% was regarding cases in which processing legitimacy has not been established, 36.4% about violations of data processing principles, and 42.4% in regard data subjects’ complaints. Of the parties investigated, the majority is private institutions, accounting for 65.3%. Of the 118 cases concluded, 49.2% involved penalty or recommendations given.

Figure 5 – Investigated cases by nature

<table>
<thead>
<tr>
<th>Nature of cases</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involving breach of confidentiality obligations</td>
<td>6</td>
</tr>
<tr>
<td>Involving lack of security precautions</td>
<td>17</td>
</tr>
<tr>
<td>Involving failure to secure data subjects’ rights</td>
<td>20</td>
</tr>
<tr>
<td>Found breaching data processing principles</td>
<td>43</td>
</tr>
<tr>
<td>Found lacking legitimacy in data processing</td>
<td>67</td>
</tr>
<tr>
<td>Improper access</td>
<td>3</td>
</tr>
<tr>
<td>Others</td>
<td>4</td>
</tr>
</tbody>
</table>

Note: Some of the investigated cases were of mixed nature.

Figure 6 – Investigated cases by ways of instigation

<table>
<thead>
<tr>
<th>Investigated cases by ways of instigation</th>
<th>Number of cases</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints</td>
<td>50</td>
<td>42.4%</td>
</tr>
<tr>
<td>Reports</td>
<td>44</td>
<td>37.3%</td>
</tr>
<tr>
<td>Referral</td>
<td>11</td>
<td>9.3%</td>
</tr>
<tr>
<td>Voluntary intervention</td>
<td>13</td>
<td>11%</td>
</tr>
</tbody>
</table>

Figure 7 – Categories of investigated parties

<table>
<thead>
<tr>
<th>Categories of investigated parties</th>
<th>Number and frequency / person-time</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public institutions</td>
<td>30</td>
<td>20.1%</td>
</tr>
<tr>
<td>Private institutions</td>
<td>93</td>
<td>62.4%</td>
</tr>
<tr>
<td>Individuals</td>
<td>26</td>
<td>17.4%</td>
</tr>
</tbody>
</table>

Note: Some of the investigated cases involved more than one party being investigated.
### Figure 8 – Categories of investigated private institutions

<table>
<thead>
<tr>
<th>Categories of investigated private institutions</th>
<th>Number of institutions involved in the investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial enterprises</td>
<td>Public enterprises (excluding telecommunication and media organizations)</td>
</tr>
<tr>
<td>Gaming</td>
<td>4</td>
</tr>
<tr>
<td>Hotel</td>
<td>6</td>
</tr>
<tr>
<td>Finance</td>
<td>4</td>
</tr>
<tr>
<td>Insurance</td>
<td>3</td>
</tr>
<tr>
<td>Telecommunication</td>
<td>7</td>
</tr>
<tr>
<td>Health and hygiene</td>
<td>3</td>
</tr>
<tr>
<td>Education</td>
<td>4</td>
</tr>
<tr>
<td>Media</td>
<td>1</td>
</tr>
<tr>
<td>Information services</td>
<td>1</td>
</tr>
<tr>
<td>Promotion and consultancy</td>
<td>19</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2</td>
</tr>
<tr>
<td>Wholesale and retail</td>
<td>12</td>
</tr>
<tr>
<td>Personal service</td>
<td>11</td>
</tr>
<tr>
<td>Other commercial enterprises</td>
<td>5</td>
</tr>
<tr>
<td>Associations, non-profit organizations and the likes</td>
<td>9</td>
</tr>
<tr>
<td>Others</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Some of the investigated cases involved more than one investigated party.

### Figure 9 – Results of concluded cases

<table>
<thead>
<tr>
<th>Results</th>
<th>Number of cases</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalties</td>
<td>7</td>
<td>5.9%</td>
</tr>
<tr>
<td>Recommendations for improvement</td>
<td>51</td>
<td>43.2%</td>
</tr>
<tr>
<td>Claims in discrepancy with facts</td>
<td>14</td>
<td>11.9%</td>
</tr>
<tr>
<td>Lack of evidence</td>
<td>24</td>
<td>20.3%</td>
</tr>
<tr>
<td>Cancelled at the request of the subjects</td>
<td>7</td>
<td>5.9%</td>
</tr>
<tr>
<td>Beyond the competence of GPDP</td>
<td>15</td>
<td>12.7%</td>
</tr>
<tr>
<td>Others</td>
<td>12</td>
<td>10.2%</td>
</tr>
</tbody>
</table>

Note: Some of the results involved both penalties and recommendations for improvement.
Figure 10 – Increment in investigated cases

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>22</td>
</tr>
<tr>
<td>2008</td>
<td>35</td>
</tr>
<tr>
<td>2009</td>
<td>47</td>
</tr>
<tr>
<td>2010</td>
<td>63</td>
</tr>
<tr>
<td>2011</td>
<td>86</td>
</tr>
<tr>
<td>2012</td>
<td>118</td>
</tr>
</tbody>
</table>
III. Summary of selected cases

The following is the summary of some selected cases.
Case 1

Google Street View cars collected data of imaginary information and Wi-Fi Network in Macao

Case Briefing

On March 11th, 2010, the media reported that Google launched the Google Maps Macao with Street View. Considering that this Google service captured real street views in Macao, which involved image data such as pedestrians and license plates, GPDP took the initiative to file a case to follow up.

Analysis and Conclusion

I. Legal analysis

(i) Collecting and processing image data

In accordance with Articles 4(1)(1) and 3(1) of the Personal Data Protection Act (Law 8/2005), the data processing involved in the current case is within the regulatory scope of the said Law.

According to Google’s information, its Street View cars, between December 10th and 19th, 2008, collected street view images in public places and private properties allowed for access. The purpose of launching Street View for Google Map Macao is to provide users the panoramas of Macao, in bid to enhance users’ experience of Google Maps and Google Earth. These panoramic pictures could supply useful information on Macao’s geographical environment and could promote its tourism industry. Google made public commitment that all the originally non-obfuscated images would be permanently obfuscated 12 months after the release of the Street View images on the Google Maps or the Google Earth.

When officers of the Office for Personal Data Protection (GPDP) checked out the Google Street View of Macao, images therein, including those of pedestrians, drivers and license plates, have been obscured. In GPDP’s opinion, the data images that shown any natural person’s appearance or driving plates, before being transferred to US for blurring, were clear, identifiable and relevant to the data subjects, therefore they are regarded as personal data.

In GPDP’s opinion, Google Inc. was responsible for collecting and processing the image data for the Street View Macao. In addition, it decided for the processing purposes and methods of the concerned personal data, therefore Google Inc. should be regarded as the data controller in the case.

Google collected the data with specified, explicit and legitimate purposes and purposes directly related to the activities of a data controller, thus it did not violate Article 5(1)(2) of the Personal Data Protection Act. Furthermore, vehicle graphics of
the Google Maps and Street View on the Google Street View cars were reminders for passers-by. The images collected were blurred before they were shown on the Google Maps and Google Earth. This showed that Google adopted appropriate measures to protect the privacy rights of the data subjects, which, at this stage, Google did not violate the principle of proportionality under Article 5(1)(3).

According to the Dispatch of the Chief Executive 83/2007, under the Personal Data Protection Act GPDP is the public authority responsible for supervising and coordinating the compliance and enforcement of the said Law. In regard whether the images Google captured infringed any portraiture rights under Article 80 of the Civil Code, this is not within GPDP’s competence. However, as a controller, Google should abide by the legal provisions and the respective obligations as given in the Personal Data Protection Act.

In GPDP’s opinions, the MSAR Government has been dedicated to developing tourism and gaming, to this Google Street View serves positive purposes. As long as the interests or rights, freedom and safeguard of the data subjects do not override Google’s legitimate interests, Google is then in accordance with Article 6(5), that is, it has the legitimacy to process the general personal information contained in the street view images.

Macao’s streets are narrow and alleys crisscrossed, with some residents live on ground floors, while collecting images the Street View cars inevitably captured the sensitive data referred in Article 7 of the Personal Data Protection Act, for instance, images showing the personal life of private households, worship in churches or temples, and so forth. No laws explicitly provide for Google’s processing of the said sensitive data, nor it has obtained any explicit authorization from the data subjects. Moreover, GPDP has not received any concerned application from Google and for which no authorization has been issued, as a result the sensitive data collected by Street View cars was contrary to its original intent of collection. Therefore, Google did not have the legitimacy to process such data and violated Article 7 of the said law. Considering that at the present stage no evidence showed that that Google intentionally violated the said provisions, under Articles 33(2) and 35(1) of the said law Google’s act constituted an administrative infraction and all the sensitive data collected for Street View Macao should be deleted immediately.

(2) The Wi-Fi data collected

Under Articles 4(1)(1) and 3(1) of the Personal Data Protection Act, the data processing this case involved is within the regulatory scope of the said Law.

According to Google’s reply, the Wi-Fi network data collected by the Google Street View cars in Macao included the SSID and MAC addresses, other net-work related data, as well as the Payload data from the unencrypted Wi-Fi network which was mistakenly collected. The Wi-Fi network data collected by the Street View cars aimed to develop the geo-location servers (GLS) and to enhance better coverage and accuracy of the coordinates mapped by the MAC addresses of the GLS. While Google was collecting Wi-Fi network data, both the GLS or Google Location Service would not release SSID, MAC addresses or other network data, especially Wi-Fi hotspot data, to any third party. The collected Wi-Fi network data, at the beginning, was stored in
the hard disks of the Street View cars, before being transferred to the Google data centers in the US and uploaded to its secure servers.

According to the explanation on Google’s Blog, SSID (Service Set Identifier) data refers to names of router manufacturers or ISPs (Internet service providers), which are made up of numbers and letters. MAC addresses, on the other hand, refer to Media Access Control Addresses or hardware addresses. Such data is the simple hardware identification numbers distributed by manufactures.

In GPDP’s opinion, generally SSID is the name or identification number of a wireless network, which could be composed by any letters and numbers in a string, with the maximum of 32 characters. When Wi-Fi devices are owned or used by a natural person and when SSID name can reveal a person’s identity, SSID data is regarded as the identifiable information of a the natural person, thus considered as personal data. Moreover, MAC addresses are used to define the positions of network devices, and such are collected when a user surfs on an Internet website. As long as these are combined with identification elements, such as the said SSID names, they turn into the information which can identify a natural person’s identity and become personal data. In addition, when a user disseminates his personal information while the Street View Cars was capturing data, personal data is also found in the payload data.

In GPDP’s opinion, although Google is not a telecom operator or internet service provider, it used the Street View cars and software to collect Wi-Fi network data for specified, explicit and legitimate purposes and purposes directly related to the activities of a data controller. At this stage, no evidence shows that the processing has deviated from its original purposes of collection, thus it did not violate Article 5(1)(2) of the said Law. Furthermore, Google was collecting Wi-Fi data for its legitimate interests.

The analysis report from Stroz Friedberg, an independent organization, pointed out that the Google Street View cars could be static or non-static, on which the Kismet device was configured to rapidly switching between wireless channels. Therefore, Kismet might have collected numerous data packets of any single-user communications (which is the content created by users like emails, file transfer), and each of these packets contained the “payload” data (communication “content” or segments of communication transmitted or received via internet). Although Google refused to allow GPDP to examine the Wi-Fi data that was collected in Macao, GPDP believed that it was impossible during the few days of data collection no one was transferring any data. As a result, it could deduce that the payload data captured by the Google cars contained personal data.

Under Article 18(c), Decree Law 18/83/M (Measures on the use of wireless communications), in the Macao Special Administrative Region it is prohibited for anyone to receive or attempt to receive wireless communications that he should not do so. If such wireless communications are received unintentionally, this person shall not retransmit or disclose to others or use them for any purpose, and shall not disclose to anyone about the existence of such communications. According to Article 6 of the this Decree Law, no one, without prior authorization from the Government, in the Macao SAR, can possess a receiver or transmitter, whether wireless or not; and no one
can establish or operate a wireless station or radio network. To this, the Bureau of Telecommunications Regulations (DSRT) also pointed out that the use of Wi-Fi equipment by Google already exceeded the scope of the exempted equipment under Category 1.7, sub-paragraph 1, Dispatch of the Chief Executive 318/2006. Moreover, DSRT has not received any applications about the current case from Google, nor to which issued any licenses. Moreover, under Article 7(1) of Law 14/2001, telecommunication service users have the legal rights of communication inviolability and secrecy. DSRT is of the opinion that Google infringed the said rights of users while collecting Wi-Fi data, and thus violated the concerned legal provisions.

In GPDP’s opinion, Google, neither as a telecommunications operator nor an Internet service provider, did not act in good faith and illegally collected Wi-Fi data, including personal data and payload data in the unencrypted Wi-Fi networks. Google’s interests did not override the interests or rights, freedom and guarantees of the data subjects, thus it violated Article 6 of the Personal Data Protection Act. Under Article 33(2) of the same Law, such act constituted an administrative infraction.

Google transferred outside Macao the Wi-Fi data, including personal data, collected locally, and GPDP has not received any application from Google for transferring the personal data as required by Articles 19 or 20 of the same Law. Also under its Article 33(2), Google’s act constituted an administrative offense.

In accordance with Article 21(1) of the Personal Data Protection Act, as a data controller Google is obliged to inform GPDP that the Google Street View cars, in Macao, has collected the network data that contained personal data like image data and Wi-Fi network data and the series of automatic processing afterwards.

2. Results

In summary, Google, through the Street View cars, obtained image data of the Macao’s public streets, and collected a large amount of data and personal data transmitted via Wi-Fi networks, in addition to transferring such data out of Macao, its acts violated a number of the provisions of the Personal Data Protection Act and constituted administrative infractions. As a result, fines could be imposed.

Result

The following factors were taken into consideration by GPDP: 1. The images captured by Google’s Street View cars were only used in Google’s products and services for its own interests; 2. It collected large amount of images and Wi-Fi data which contained personal data, including sensitive data, which had been transferred to US; 3. Google refused to allow GPDP to examine the Wi-Fi data collected in Macao; 4. It was the first time that Google breached the Personal Data Protection Act. And Google cooperated during the investigation and admitted its own mistakes.

Therefore, according to GPDP’s decision,
1. As the Google Street View cars collected sensitive data in Macao without obtaining any authorization from GPDP, it did not have any legitimacy for processing and violated Article 7 of the Personal Data Protection Act. However, since no evidence indicated that Google violated the provisions intentionally, under Articles 33(2) and 35(1) of the same Law, a fine of MOP$10,000 is imposed.

2. Google violated Article 5(1)(1) as it did not process the data lawfully and did not act in good faith to collect Wi-Fi data, which contained personal data, and payload data in the unencrypted Wi-Fi networks. Obviously, Google’s interests did not override the interests or rights, freedom and guarantees of the data subjects, thus violating Article 6 of the said Law. Under Article 33(2) of the said Law, a fine of MOP$10,000 is imposed.

3. Google collected the Wi-Fi data in Macao, which personal data is included, and transferred such data to US. This violated Articles 19 or 20 of the Personal Data Protection Act. Under Article 33(2) of the said Law, a fined of MOP$10,000 is imposed.

4. Google should immediately delete all the illegally collected sensitive data by the Street View cars in Macao. As for other general data, Google should keep its commitment, within 12 months after the release of the streetscape images, to obfuscate all the non-obfuscated images as contained the original data.

5. Google shall delete the payload data and SSID data found in the Wi-Fi data in which natural persons are, or could be, identifiable.

6. Google automatically processed the image data and Wi-Fi data the Google Street View cars collected in Macao, for which notification to GPDP is compulsory under Article 21(1) of the Personal Data Protection Act.

The aforementioned fines have been imposed.
Case 2

A company used before and after plastic surgery photos for promotion without the patient’s consent

Case Briefing

While working for Company A as a salesperson, X underwent a plastic surgery there at a discounted price. Before the surgery, Doctor Y verbally promised X that the photos taken would only be used for before and after comparison. In 2010, the said Company printed X’s photos, without blurring at all, on its brochures that were available from its branches.

X believed that Company A might have violated the Personal Data Protection Act by using the before and after photos for its promotion material, to which her consent was not given.

Analysis and Conclusion

According to Articles 4(1)(1) and 3(1) of the Personal Data Protection Act, the processing of personal data in the current case falls within its regulatory scope.

From the information Y provided, if a salesperson received a discount for her surgery, she had to promise her photos to be used for promotional purposes. All the plastic surgery photos were stored in a computer in Y’s room, and could have been stored in a computer at the reception desk, too; login password and authority for information retrieval had not been set up for these computers. Z was commissioned for the brochure production by Company C, in Mainland (Company A and Company C were under the same name and owned by the same chain group). Z, on several occasions, came to Company A, located in Macao, to retrieve information wherein X’s photos were included, but the computers showed no such records.

Y was the person who took X’s photos before and after the surgery, and the photos were preserved by and stored in a computer of Company A. In GPDP’s opinion, Company A, being the controller, has the rights to control and decide for the before and after surgery photos.

During the investigation, it found that the description “Miss Macao” was added to the photos on the brochures of the case, in tandem with the introduction of Y and the flagship store of Company A in Macao. In GPDP’s views, although the brochures were printed by the Mainland company, Company C, Y himself is its shareholder as well as Company A is a member of the same group, Company A should have known of and allowed Company C to print the photos on its brochures, in order to obtain direct commercial interests.
Company A’s processing personal data of its customers was for the purpose of its plastic surgery services. If using the photos beyond such purpose and for publicity, in particular printing on promotion material for posting and distributing, there should exist the expressed consent received from the data subject, or an authorization issued by the GPDP, according to Article 7 of the Personal Data Protection Act.

X received the surgery before the said Law came into force, during which no law governed that Company A should receive the expressed consent, in a statutory way, from X in order to process her photos of plastic surgery. But after this Law came into effect, Company A’s processing of personal data is subject to legal requirements of the Law.

According to Company A, photos of all its patients who received plastic surgery could have been stored in the computer at its reception desk. The computer had neither set up login password nor information retrieval authority, as well as no video surveillance system had been installed. Furthermore, Company A admitted that it did provide the before and after photos of X to Company C in Mainland for printing brochures, which caused a release of X’s sensitive information. In addition, Company A had no knowledge of the specific type of data that Company C took away, and its computers failed to provide records to follow. Moreover, a number of surgical consent forms its patients signed were lost while an interior decoration carried out in 2008. As a consequence GPDP regarded Company A failed to assure the security of the said information, and violated Article 16 of the Personal Data Protection Act.

The brochures of the current case were printed in Mainland, to where X’s photos were transferred accordingly. Company A, located in Macao, had never applied to GPDP any notification, authorization or decision for its transfer of personal data, hence it violated Articles 19 and 20 of the Personal Data Protection Act. According to Article 21(1) of the said Law, Company A used computer to process the photos of all its patients receiving plastic surgeries, this already involved the auto processing of personal data that GPDP should be notified.

In summary, Company A in its processing of sensitive information had not introduced the special security measures, and had not notified or applied to GPDP for its transfer of information, which constituted violation of the said Law.

Result

Considering the present case is the first offence of Company A and the cooperative attitude it showed throughout the investigation, in addition to its improvement initiatives, such as appointing specialized staff to manage sensitive information, setting up computer passwords and formulating policies for handling sensitive information, and requesting the franchise store in China to destroy the brochures with which X’s photos were printed, GPDP made the following decisions:

Company A, located in Macao, did not act in accordance with Article 16 of the Personal Data Protection Act to introduce special security measures, therefore a penalty of MOP$4,000 was resulted from Article 33(1) of the Personal Data Protection Act.
Protection Act. Its conduct violated Articles 19 and 20 of the said Law, leading to a penalty of MOP$8,000 imposed under Article 33(2) of the same Law. These punishments have been implemented.

To prevent continuous harm the infractions caused to the data subject, according to Article 43(1) of the Personal Data Protection Law, Company A has been banned from using any photos for marketing purposes without expressed consent of the data subjects.
Case 3

Receiving the photos taken by video surveillance camera inside the lift of the building

Case Briefing

Citizen A expressed that Department A where he worked received a letter sent by Person B containing the number of his rental parking space in Building B, the license plate number of his car and six black and white photos taken by the video surveillance camera inside the lift of Building B.

As Citizen A believed that the aforementioned six photos were disclosed by the security guard of Company C working in Building B and a consequent invasion of privacy, he asked for a follow-up to the situation from the Office for Personal Data Protection (GPDP).

Analysis and Conclusion

The data processing of the current case is regulated by the Personal Data Protection Act under its Article 4(1)(1) and 3(1).

According to a statement made by Person C, the ex-chairman of the Management Committee of Building B, the surveillance system in Building B was managed by Company C. Person B had formerly been a director of the Management Committee and Building B currently had no Management Committee.

According to the information provided by Company C, the surveillance system was controlled and processed by Company C. Although the security guard of the building would monitor for any suspicious characters or situations via the screen of the said system, he would not provide any CDs or image data to anyone without permission.

GPDP considered that since Company C was entitled to personal data processing captured by the video surveillance camera installed in building B, Company C was the controller.

Person B did not send the letter on behalf of the Management Committee of Building B. Under Article 3(2) of the Personal Data Protection Act, Person B was not the controller; therefore the Personal Data Protection Act was not applicable to the aforementioned processing.

The surveillance system of Building B was collectively owned by all individual proprietors in the building, and Company C was hired by these proprietors to manage the building and maintain the safety and normal operation of the building, therefore
we could conclude that the installation of the respective video surveillance camera by Company C was for security purposes in the building and thereby had legitimacy in accordance with Article 6(5) of the Personal Data Protection Act.

After investigation by GPDP, the authority of the security guard of Building B was only limited to the surveillance of the relevant images and there was only one screen and one surveillance system controller on the scene. Thus, the residents of the building were not able to view relevant images through the surveillance system located inside the building. However, the corresponding screen was located next to the window of the building entrance that the window was always open. Person B might have captured the display image without the safety guard’s awareness (for example, due to said safety guard being temporarily absent). As such, the security measures Company C was adopting presently were insufficient and did not conform to Article 15 of the Personal Data Protection Act.

If Citizen A suffered damages due to the behavior of Company C, he could exercise his right to indemnification as envisioned in the Personal Data Protection Act.

In summary, Company C breached Article 15 of the Personal Data Protection Act.

**Result**

GPDP informed both Citizen A and Company C, in writing, of the aforesaid analysis and decision and requested Company C to improve his security measures in regard to the personal data processing from the video surveillance cameras. Company C also had to create the relevant “Personal Data Collection Statements”, and make the respective declarations to GPDP. The case was closed.

Company C had made corresponding improvement measures according to GPDP’s request.
Case 4

Public Department A recorded phone calls without obtaining callers’ consent

Case Briefing

Citizen X called the contact number of Public Department A and Y, responsible for managing the complaints, answered the call. During the conversation, X was feeling dissatisfied and expressed he wanted to complain the staff of the Department. So the call was forwarded to Z. Both of the two calls were recorded without voice prompts presented before the conversation started. Y and Z admitted that his calls were recorded only after X asked if there was any.

X believed that Public Department A recorded the calls without obtaining his consent, which could have violated the Personal Data Protection Act, thus he requested the GPDP to follow up.

Analysis and Conclusion

In accordance with Articles 4(1)(1) and 3(1) of the Personal Data Protection Act (Law 8/2005), the data processing involved in this case is within the regulatory scope of the said Law.

Under Article 4(1)(1) of the Law previously mentioned, the data subject is an identifiable person as long as he could be identified, directly or indirectly, and distinguished from others by certain identifying features. In GPDP’s opinion, the recordings made by the system were clear and legible. With elements such as X’s last name and phone number, X’s identity could be established or confirmed. Therefore, the “voice” recorded by the recording system of Public Department A is regarded as the information of an identifiable person, i.e., X, and therefore is taken as personal information.

According to Department A’s reply, dates back to the end of 2010, it started using a phone recording system to assist callers’ complaints. Due to technical problems, it failed to provide automatic voice prompts, so each time a staff answering a call would actively remind callers of the recording. X had made a number of complaints for different matters. Except the phone call related to the current complaint to GPDP, X was reminded of the recording in the rest of the other calls.

According to Department A’s declaration made to GPDP, the purpose of telephone surveillance was to “ensure service quality, assess staff performance and protect the legitimate interests of the Department”. In GPDP’s opinion, the voice recordings involved both the Department staff and the callers. To the Department, recording staff while on duty was to monitor their activities. Generally speaking, based on operation, business and overall needs to monitor staff activities is legitimate and lawful, which also meet the legitimacy given in Article 6(5) of the Law previously
mentioned. Although recording callers’ conversation safeguards the legitimate interests of the Department, it should also respect the rights of the former, allowing them to decide whether to make their complaints while being recorded. If disagreed, the said Department should offer other means of communications, such as face-to-face meeting, e-mail, fax, letter etc. Therefore, in this case the legitimacy for Department A to record its callers could only derive from their consent.

For the two recordings to which X’s complaints referred, the recording data provided by the said Department showed that while answering the phone calls from X, his phone calls were recorded without any voice prompts. One recording showed that X was not informed of the recording that was taking place, while the other showed that X was informed only after he asked if any recording was taking place. In GPDP’s opinion, in the last call, after X was informed of being recorded, X did not disagree and continued the call. Therefore, it could assume that X agreed with the recording throughout the call. For the other one, because X was uninformed, GPDP is in the opinion that Department A failed to achieve the legitimacy for the recording.

As mentioned, in this case the legitimacy of the recordings could only be obtained from the subject’s consent. Article 4(1)(9) of the Personal Data Protection Act stipulated “the data subject’s consent” shall be explicit and shall be made under “any freely given specific and informed” condition. Consent as such shall be derived from the expression of intent, either explicit or implicit, and shall be beyond doubts, reflecting the data subject was informed of and agreed to the processing of his personal data. Although X had “agreed with” the recordings on several occasions, his consent was only made for his previous calls and could not apply the same consent for other calls he later proceeded with other Department staff. If this Department had to record, it shall ask for X’s explicit consent every time. Therefore, for the above mentioned call, without clear prompts in advance, the said recording could not be viewed as based on X’s explicit consent. Thus, Department A’s processing of personal data lacked the legitimacy under Article 6 of the Personal Data Protection Act.

According to the investigation, the processing of personal data in the current case that failed the legitimacy under Article 6 of the Personal Data Protection Act is not a single incident, but a problem in the processing mechanism. In GPDP’s opinion, Department A’s recording system started automatically after the switchboard forwarded the calls. The caller and staff member were already being recorded before the responsible staff asked if the caller agreed to the recording. Under normal circumstances, if a staff reminded the caller of the recording, this would not be questioned of. However, because “recordings take place automatically before reminding callers”, in special circumstances (e.g. a bad atmosphere the between the staff and the caller’s conversation or a staff forgot to remind a caller of the recording) where a reminder was difficult, or not timely, to be delivered and the recording started, as well as when a caller disagreed to the recording after the reminder, the Department then failed to have the legitimacy to process the recordings, thus violating Article 6 of the Personal Data Protection Act.

In summary, due to the defect of the phone recording system, the said Department recorded the phone calls between its staff and the callers, which violated Article 6 of the Personal Data Protection Act.
Result

The following factors were taken into consideration by GPDP: 1) Department A recorded the conversations between its staff and the callers in order to ensure service quality. Its purpose was legitimate and lawful. However, the defect of the recording system failed to seek consent from the data subjects, but it was not a deliberate violation of the Personal Data Protection Act. 2) It was the first time that Department A violated the regulations of the Personal Data Protection Act. 3) During the investigation, Department A maintained a cooperative attitude, and an automated voice prompt system was installed in mid-2011, which has improved the settings of the caller recording system.

In summary, GPDP took into account that Department A recorded the phone calls between its staff and the callers but failed to achieve the legitimacy under Article 6 of the Personal Data Protection Act. Under Articles 33(2) and 35(1) of the said Law, GPDP, therefore, decided to impose the said Department a fine of MOP$8,000. The punishment was implemented.
Case 5

Data of labour dispute complainant transferred to his employer in labour dispute

Case Briefing

In May 2011, Citizen X lodged a complaint to GPDP in person, revealing that the Labour Affairs Bureau (DSAL) passed his personal data to his employer when handling his dispute. When he made an inquiry with DSAL, its staff explained that normally if there was no specific request for confidentiality, the complainant’s personal data would be transferred to his employer. X pointed out that he was not informed of such transfer when DSAL was taking his statement of record, in addition that it had not obtained his consent. X believed that being a department to resolve labour disputes, DSAL could have thought of the “possible retaliation”. He pointed out that what DSAL had to do was to inform his employer of the contents of his complaint, with which disclosing personal data was unnecessary.

X believed the said practice of DSAL might have violated the Personal Data Protection Act (Law 8/2005), therefore he filed a complaint with GPDP.

Analysis and Conclusion

Under Articles 4(1)(1) and 3(1) of the Personal Data Protection Act, the data processing involved in this case is within the regulatory scope of the said Law.

According to the reply of the DSAL, to comply with the aforementioned Law, when complainant’s personal data were to be collected for labour disputes, the complaint statement and the statement of record used in the case contained a personal data collection statement, which states that “…… DSAL may transfer the declarant’s personal data to other administrative and judicial authorities, etc…….” X was asked to sign and acknowledge the content therein, during which he did not ask for the confidential processing of his complaint, nor any other special requirements. Then the labour inspector followed up on the complaint in accordance with the law. If X’s name was not provided to his employer, the case could not be followed up.

After analysis, in GPDP’s opinion, because the above mentioned statement of record did not specify that the DSAL would deliver the personal data provided by the declarant to the Complainee(s), to which it should not be deemed as an explicit consent has been given. As a consequence, under Article 6 of the Personal Data Protection Act, DSAL failed to have the legitimacy from the explicit consent given by X for transferring the data to his employer.

However, in addition to obtaining the data subject’s explicit consent, the data controller could be legitimate to process personal data if it fulfilled other conditions as
described in Article 6 of the same Law. In this case, in accordance with the Administrative Regulation 24/2004, Organizational Structure and Functions of Labour Affairs Bureau, and Administrative Regulation 26/2008, Operating Rules for Labour Inspection, DSAL has the legal duties to handle labour disputes and investigation procedures for contraventions (contravenções), which are in line with Article 6(4) of the Personal Data Protection Act.

In accordance with Article 7(1) of the Administrative Regulation 26/2008, labour inspectors shall make a statement of record once discovering any contraventions. Also under Article 7(4) of the same Regulation, the said statement should also be taken once wage arrears are found and should provide detail of the arrear calculations. In the current case, X requested DSAL to follow up on the wage arrears and, in fact, the actual amount of unpaid wages could not be calculated and the case could not be followed up without providing X’s name to his employer. X should have foreseen this situation while making complaints to DSAL for his unpaid wages.

In this case, the DSAL included the personal data collection statement in both the complaint statement and statement of record, but failed to state clearly that X’s information would be transferred to the complainee. Since labour relations were sensitive and would directly affect the relationship between the employer and the complaining employee, who may not understand the relevant procedures of the DSAL, the information available is crucial to the employee’s decision to make a complaint or not. Also in accordance with Article 10 of the Personal Data Protection Act, DSAL should inform the data subjects of the data recipients or categories of data recipients.

In summary, no information showed that the data processing of DSAL violated the Personal Data Protection Act. However, there was room for optimization.

**Result**

As it is not necessary for GPDP to follow up this case further, it decided to inform X that the investigation results and the case is closed. In addition, GPDP also reminded, in writing, DSAL of improving its statement of records (for example, providing supplementary information that the complaint information will be transferred to the complainee, or the persons or institutions to be contacted for the complaint). If feasible and lawful, the data subjects may request DSAL not to transfer his information to his employer in order to avoid unnecessary misunderstandings.
Case 6

Displaying medical certificate publicly

Case Briefing

X, who is a staff member of Bureau B, complained to Public Authority A about his direct superior Y publicly displayed his medical certificate, which contained his personal data. Y is a functional head of Department C, which is a subordinate unit of Bureau B. Because of this, X believed that Y might have violated the secrecy obligation.

Due to the complaint may involve violations of the Personal Data Protection Act, Public Authority A, therefore, transferred the case to GPDP.

Analysis and Conclusion

According to Articles 4(1)(1) and 3(1) of the Personal Data Protection Act, whose regulatory scope the processing of personal data in the present case falls within.

Bureau B explained that, as its subordinate unit Department C requires staff to work on shifts, Y had to reassign staff immediately on that day as X suddenly took a sick absence. Later, Y fastened up X’s medical certificate, along with the roster changes, in the rest area for team members, in order to promptly notify the staff members on shift that day. The said area was restricted to be used by three staff members on shift, and the medical certificate was attached to the glass door of a cabinet until the end of the reassignment. Afterwards, Y was requested by Division Head Z to apologize personally to X. In addition, a letter of apology and review was also put up on the same place where the medical certificate was. This is the first occurrence of such incidence in Bureau B.

The information provided by Bureau B showed that it has not regulated for the processing of medical certificates. According to the established general procedures, staff members will submit the said document to a superior to confirm and sign, before it was handed over to the personnel department for related administrative procedures. Later, this will be published in the weekly internal news bulletin.

The crux of the present case is to confirm who the controller is. According to Article 4(1)(5) of the Personal Data Protection Act, a controller shall mean the party that makes decision for the purposes and methods of data processing. The organizational law of Bureau B regulates its director within his competence to formulate compliance rules and guidelines for the normal functioning of the department. GPDP believed that, in the present case, due to Bureau B has the right to decide the processing purposes and methods of the medical certificates, it possesses the identity of the controller. Despite Bureau B explained that it was a personal
conduct of Y to put up X’s medical certificate, in the current case since the latter did not possess the competence to process medical certificates, therefore, Y engaged in the said conduct for discharging his duties. For this reason, Bureau B, instead of Y, was indeed the controller.

With regard to the nature of data, as the medical certificate contained X’s personal data, partly of which related to X’s health conditions, therefore they are considered sensitive. According to Articles 6(2) and 7(2)(1) of the Personal Data Protection Act, Bureau B has the legitimacy to process X’s medical certificate though, the processing should be in accordance with the principles laid out in Articles 2 and 5 of the said Law, including the principle of proportionality. In other words, the processing purposes should be in line with that the controller intended to and where processing is necessary.

In GPDP’s point of view, no detail specification for the processing procedures of medical certificates has been laid down in the Statute of Workers of Macao Public Administration, as approved by Decree Law 87/89/M, and consequently it remained as the decision of a public department. In the current case Bureau B has not fulfilled its prudent obligation and put up X’s medical certificate, thus giving access to personal data by non-interested parties. To its intended purposes, the said processing was evidently inappropriate and unnecessary, which violated the principle of proportionality given in Article 5(1)(3) of the Personal Data Protection Act.

In terms of the security for processing sensitive data, Article 16(1) of the said Law specified a list of special security measures, amongst which in particular Article 16(1)(2) regulated that “preventing data media from being read, copied, altered or removed by authorised persons”. If the processing of X’s medical certificate were in accordance with the general procedures, the other two team members would only learn of X’s absence from their superior or the internal news bulletin, instead of finding it out from the medical certificate directly. That is to say, these team members are considered as the aforesaid “unauthorized persons”. The processing by Bureau B violated Article 16(1)(2) of the Personal Data Protection Act as a consequence.

In relation to secrecy obligation, from Y’s putting up of medical certificate of X, to Y’s subsequent explanation and apology, these were carried out in the identity of a functional head, and the processing of personal data was accordingly considered as Bureau B’s conduct. In addition, the disclosure or dissemination of personal information contained in the certificate were both unintentional, thereupon it showed no indication the conduct violated the secrecy obligation laid out in Article 41 of the Personal Data Protection Act.

In summary, Bureau B’s processing violated Article 5(1)(3) and 16(1)(2) of the said Law.
Result

Bureau B’s conduct violated Article 5(1)(3) of the Personal Data Protection Act, which constituted an administrative infraction, leading to a fine of MOP $ 4,000 according to Article 33 (1) of the Personal Data Protection Act.

Its conduct was also in violation of Article 16(1)(2) of the Personal Data Protection Act, which constituted an administrative infraction, to which, according to Article 33(1) of the same Law, a fine of MOP $ 4,000 was imposed.

According to Article 34(2) of the aforesaid Law, concurrent administrative infractions are subject to penalties issued in conjunction. As a result, Bureau B was fined with MOP $ 8,000, and the punishment has been executed.
Case 7

Placing the course enrolment data of employees onto one collective application form

Case Briefing

Bureau A forwarded a complaint made by a staff from Bureau B to the Office for Personal Data Protection (GPDP). The complaint indicated that all the staff of Bureau B had to fill in their personal data such as their identity card numbers and academic qualifications onto one application form to enroll in course “X”, which led to the data to be seen by applicants from another course while the form was being passed around. In addition, Bureau B saved the respective application form within a common computer folder which could be accessed by all the staff with computer accounts.

Analysis and Conclusion

The data processing of current case is regulated by the “Personal Data Protection Act” under its Articles 4(1)(1) and 3(1).

The application forms involved in the present case were about the collective application forms of Bureau A’s course, which required applicants to fill in information such as their names, identity card numbers, job positions/ranks, academic qualifications and telephone numbers, etc.

Bureau B explained that the collective application forms for course “X” could be obtained through Bureau A’s internal network and the staff could download it individually. After completing the form, they needed to submit it to their supervisor for endorsement and send it back to the team of instructors via a specific e-mail account, which could only be accessed by duly authorized personnel. If a person enrolled in Bureau A’s courses for the first time, a photocopy of his identity card must also be submitted by the department to the Division of Training and Documentation within a sealed envelope.

Afterwards, GPDP received a letter from Bureau A, stating that it had cancelled collective application forms for its courses and switched to individual application forms with the identity card number column only requiring the first 5 digits or letters (a photocopy of the identity card was still required for those enrolling for the first time) so as to better protect personal data.

In this case, as the data being processed was not considered sensitive data under Articles 7 and 8 of the “Personal Data Protection Act” and data that was suspected of being involved in illegal activities, or in criminal or administrative offences. Bureau B should comply with the relevant security criteria specified in Article 15 of the
“Personal Data Protection Act” to process such common personal data.

After investigation, GPDP felt that Bureau B implemented all the appropriate security measures by only allowing those staff, who was responsible for the relevant work, accessed and consulted the course application details. There was no evidence that Bureau B breached Article 15 of the “Personal Data Protection Act”.

Result

As there was no evidence to prove Bureau B breached Article 15 of the “Personal Data Protection Act” and Bureau A had already switched to using individual application forms, the controversial issues in this case had been resolved. Therefore, GPDP decided to close this case and informed Bureau B, Bureau A and the data subject of its results.
Case 8

Filming a medical procedure

Case Briefing

The Office for Personal Data Protection (GPDP) received a referral from the Health Bureau regarding a complaint made by Citizen A that Doctor B filmed himself carrying out a dental implant procedure on Citizen A without his consent, thereby invading his privacy.

As the complaint involved the possible breach of the provisions of the “Personal Data Protection Act”, the Health Bureau forwarded the case to GPDP for follow up.

Analysis and Conclusion

The data processing of current case is regulated by the “Personal Data Protection Act” under Article 4(1)(1) and 3(1) of the “Personal Data Protection Act”.

After viewing the information from the Health Bureau website, it was confirmed that Doctor B is a registered dentist.

According to the information provided by Doctor B, he had asked Citizen A to open his mouth to take pictures. Citizen A saw and knew what was happening at the time and never expressed his dissatisfaction or raised an objection. Doctor B expressed that the purpose of filming the dental implant procedure was to improve the follow-up services after tooth loss surgeries. The data photographed by Doctor B was kept in Citizen A’s personal file locked inside his personal office. The data was processed by Doctor B and not used outside of the medical treatment and all of the photos would be deleted upon completion of the treatment. Similar types of photos were taken within a period of four months and Citizen A raised no objections during the payment of the repeated follow-up consultations, and signed the confirmation receipts. Of the 3 treatment receipts that Doctor B provided, two contained Citizen A’s signature. Moreover, the receipts all contained the following reminder: “I clearly understand the doctor’s description of the entire medical treatment procedure, and hereby give my consent to this person to provide me with the corresponding medical treatment, which I confirm through my signature and payment.”

In this case, although the photos taken were of the oral cavity area, each person’s teeth have unique characteristics such as shape, arrangement, degree of wear and dental arch shape, due to the differences in each person’s age, sex, nationality, living area and eating habits. As such, the person’s teeth can be used to confirm his or her identity. In addition, all of Citizen A’s photos were stored in a subdirectory of Doctor B’s personal computer. As Doctor B had stated that those photos were taken for Citizen A, his identity could be confirmed, making this information fall under the definition of “personal data” specified in Article 4(1)(1) of the “Personal Data Protection Act”. 
Doctor B expressed that he is a dentist at Medical Center B. In order to provide the customer with better follow-up services, the center asks its doctors to take photos during the dental implant procedures. In addition, all of Citizen A's proofs of payment were issued under the name of Medical Center B. It was therefore clear that Medical Center B was the controller for the personal data processing as specified in Article 4(1)(5) of the “Personal Data Protection Act”.

Citizen A’s dental health and further treatment needs could be determined from the photos provided by Doctor B and this data consequently falls under the definition of sensitive data related to healthcare matters provided in Article 7 of the “Personal Data Protection Act”.

In this case, there was no evidence that Doctor B possessed legitimacy beyond the data subject’s consent, in accordance with Articles 6 and 7 of the “Personal Data Protection Act”, thus the data subject’s consent was the only way to prove Doctor B would have had the legitimacy to take the relevant photos.

According to the information provided by the Health Bureau and Doctor B, Citizen A had full knowledge of and did not object to Doctor B taking photographs of him during the dental implant procedure. This is a free, specific and informed consent given by the data subject, in line with Article 4(1)(9) of the “Personal Data Protection Act”. As to the processing of sensitive data, in accordance with Article 7(2)(3) of the same Act, the data subject must give his or her “explicit consent” (consentimento expresso), which can be given verbally, in writing or through the data subject’s explicit actions. In this case, the information provided by Doctor B indicated that the photos were taken during a 4-month period with each session lasting over an hour and each photo taken more than one minute following the previous one. After the photos were taken, Citizen A continued to receive treatment from Doctor B at least three more times, two of those times having been dental implants. The information provided by the Health Bureau indicated that Citizen A chose to receive treatment from Doctor B consciously and autonomously. Therefore Citizen A's conduct clearly reflected his consent to Doctor B to proceed with the photos, in accordance with Article 209 of the “Civil Code” which states that it can be “otherwise given through any direct manifestation of the subject’s will”. As such, the aforementioned situation complied with the requirement of explicit permission.

In this respect, Doctor B’s taking of relevant photos possessed the legitimacy of “when the data subject has given his explicit consent for such processing” as specified in Article 7(2)(3) of the “Personal Data Protection Act”.

When processing Citizen A's personal data, Medical Center B not only satisfied the legitimacy criteria specified in the “Personal Data Protection Act”, but also followed the principles of data processing which includes the requirement that the data can be “collected for specified, explicit, legitimate purposes and for purposes directly related to the activity of controller” as specified in Article 5(1)(2) of the same Act, and the principle of adequateness as specified in sub-paragraph 3 of the same paragraph.
None of the photos taken involved situations beyond the dental implant procedures and the photos taking was one of the methods for recording the progress of the medical treatment. Since neither the Health Bureau nor Citizen A could provide any evidence to prove Doctor B using the photos other than the treatment purposes, there was no evidence that Medical Center B breached Article 5(1) (2) and sub-paragraph (3) of the “Personal Data Protection Act”.

In summary, no evidence showed that the respective processing procedures breached the provisions of “Personal Data Protection Act”.

**Result**

In view of the fact that Medical Center B’s processing of relevant personal data was in line with the Articles 5, 7, 15 and 16 of the “Personal Data Protection Act”, GPDP decided to close this case and notify Citizen A and Doctor B of the results.

In addition, GPDP sent a letter to Medical Center B, reminding it to execute Articles 10, 11 and 16 of the “Personal Data Protection Act” by establishing a “Personal Data Collection Statement” as soon as possible, and informing GPDP of declaration of the relevant data of automated processing of personal data, as specified in Article 21 of the same Act. It also suggested Medical Center B to avoid taking photos of the medical procedures if the record was unnecessary prior to asking for the data subjects’ explicit consent.
Case 9

Displaying user’s personal data on electronic screen while borrowing / returning books

Case Briefing

Citizen A complained to the Office for Personal Data Protection (GPDP), stating that upon borrowing some books from Activity Center A – which operated under Bureau X - a few months ago, the two electronic screens (one facing the borrower and the other facing the staff) displayed his name and identity card number or telephone number. This data would remain displayed for a long time whereas no operations were carried out. Although he reported the problem to that Bureau a few months ago, the situation was the same when he went back to the center to return some CDs on the other day. After complaining to Bureau X, the staff explained that the relevant software program supplier indicated that major changes would be required, but the Bureau’s IT department would attempt to modify the program itself.

Citizen A considered what Activity Center A did caused his personal data to be leaked and the staff should not be allowed to have knowledge of above data. Therefore, he suspected that Activity Center A breached the provisions of the “Personal Data Protection Act” and filed a complaint to GPDP.

Analysis and Conclusion

The data processing of current case is regulated by the “Personal Data Protection Act” under its Article 4(1)(1) and 3(1).

Bureau X’s reply indicated that, in order to facilitate the verification of the data pertaining to the lending and returning of books by the public and to avoid arguments, Activity Center A would allow the public to view the relevant data. As to the problem of possibly being seen by others during the verification, immediately after receiving the report from Citizen A at the beginning of the year, the Center requested the front-desk staff strictly to comply with the work guidelines by not displaying the book lending/returning interface of the computer system and turning off the interface after the lending/returning procedures had been completed. The library of the Center improved the display method of the readers’ data in the borrowing/returning system by displaying only the identity card and the first and last digit of the mobile number with the middle numbers replaced by “XX”. A privacy filter was also placed in front of the display screen. Bureau X then called Citizen A to give his opinion on the measures and Citizen A indicated that he was satisfied with the result of the measures implemented. Finally, all the staff operating the system must first register a system account and be given access rights by the system administrator (which included viewing, book borrowing and returning procedure and data maintenance rights). Bureau X also formulated a “Personal Data Collection Statement –Data on the Users
of the Center” for use by the various centers under it when collecting the public’s data.

After an on-site investigation, GPDP staff found that the computer screens facing the public and located above the counters were inactive either during the book lending/returning process or when searching for un-returned books.

According to the organic law and relevant regulations of Bureau X, as well as Article 4(1)(5) of the “Personal Data Protection Act”, Activity Center A was subordinated to Bureau X and did not possess the right of decision on the purpose and method of the personal data processing, thus Bureau X was the controller in this case.

In this case, Citizen A provided his personal data to register an account at Activity Center A for the purpose of using its library facilities. As such, Bureau X fulfilled the legitimacy criteria specified in Article 6 of the “Personal Data Protection Act”, as the data subject gave his explicit consent. Even so, pursuant to Article 5 of the same Act, Bureau X should, when processing personal data, still follow the various principles, including the principle of proportionality. Considering that Bureau X’s explanations along with GPDP staff’s discovery that the display screens in the Center were only turned on when the data subjects themselves needed to verify certain information, it could be deduced that Activity Center A’s original intention was to display the personal data only to the data subject in order to allow him checking and verifying its personal data and not to the public. Moreover, the Activity Center A was responsible for ensuring that public resources were not damaged or wasted, hence it was necessary for the Center to verify the identity of the book lender so as to protect the interests of the persons borrowing or returning books. Therefore, the Center’s relevant practice did not obviously breach the principle of proportionality specified in Article 5(1)(3) of the “Personal Data Protection Act”.

According to Article 15 of the “Personal Data Protection Act”, Bureau X should implement the necessary security measures to protect personal data. As the measures applied by Bureau X allowed for other people present to view the data displayed on the electronic screens, Bureau X should have foreseen the associated risks and adopted the corresponding adequate security measures. Bureau X had already adopted improvement measures to prevent other people present from viewing the relevant data. As there was no evidence that Bureau X allowed data to be leaked by not adopting sufficient security measures, there was no existence of violation.

In the current situation, and according to Bureau X’s reply, all the staff operating the system were now required to apply for a system account and be assigned the necessary access rights by the system administrator. Under Article 18(1), 41(1) and 41(2)(1), when processing personal data, the staff of Bureau X should be bound by professional secrecy and restricted by all the applicable rules of criminal law. As no evidence was found that the staff had disclosed data inappropriately, there was no existence of violation.

In summary, no evidence indicated that Bureau X’s processing breached the “Personal Data Protection Act”, whereas there was room for improvement in this area.
Result

GPDP decided to close the case and notify Citizen A and Bureau X of the results.
Case 10

A recording of the interviewee conducing the street questionnaire was taken without his consent

Case Briefing

Citizen A called the Macau Radio Station (TDM Cantonese), expressing that a survey conductor from Department A had secretly used a recording pen to record the interview without his consent during a street questionnaire held in Z.A.P.E. He considered that this was a potential breach of the “Personal Data Protection Act”. The Office for Personal Data Protection (GPDP) took the initiative to follow up the case.

Analysis and Conclusion

The data processing of current case is regulated by the “Personal Data Protection Act” under its Article 4(1)(1) and 3(1).

According to Department A’s reply, the questionnaire involved was an activity jointly organized by Academic Society B and Association C.

Academic Society B’s written reply expressed that the questionnaire organized jointly by Academic Society B and Association C had been delegated to Company D. The recording had been carried out during the random sampling stage and had been ceased when the official survey launched. Company D’s reply claimed that it had trained the survey conductors and requested them to start taking the recording after obtaining the interviewees’ consent.

As the questionnaire involved in this case was jointly organized by Academic Society B and Association C, which delegated to Company D for execution, GPDP believed that Academic Society B and Association C were the controllers for the processing of the recorded personal data. Company D was the processor delegated by these two entities, and that Department A had not participated in the processing of relevant personal data.

According to Article 6 of “Personal Data Protection Act”, personal data may be processed only if the data subject has unambiguously given his consent or under other circumstances determined by law. The execution of street questionnaires by the academic organizations aimed at research purposes that did not satisfy the other requisites provided in Article 6 of the “Personal Data Protection Act” and therefore the controller should ensure that the data subject had given his or her explicit consent before recording. Otherwise, no recording was allowed.

In summary, there was no evidence at this stage to show that the organizations which conducted the questionnaire proceeded the recording without the interviewee’s
consent, and also no evidence indicated that the “Personal Data Protection Act” was breached. However, GPDP had already requested the respective controllers to immediately and permanently erase all the recordings where the interviewees did not give their consent or where the voices of non-interviewees could be heard.

**Result**

GPDP informed Department A, Academic Society B and Association C, in writing, of aforementioned analysis and decision. The case was closed.
Case 11

Hotel customers’ personal data was forwarded to a third party and transferred outside Macao

Case Briefing

A legal proceeding document of Company A against its shareholder X and an investigation report have been spread over the internet. These documents alleged that Company B, being a locally registered company and a subsidiary of Company A that is registered in Country D, passed the personal data of its hotel customers to its parent company. To this, GPDP decided to actively intervene.

Analysis and Conclusion

After investigation, Company A was found, during the end of 2011, commissioning Company C to conduct an independent investigation, which aimed at finding out if X violated his management duties with Company A, and if violated the anti-corruption law of where Company A is registered. The investigation was launched to examine what X had put in for establishing his business in Country E. To this, Company C sent investigators to Macao, and, with Company B’s collaboration, collected its hotel customer data. In the investigation report later submitted to Company A, Company C recorded the personal data of a number of individuals, including those officials from Country E who had contacts with X and stayed in the hotel of Company B, as well as those who travelled together and their relationships with these officials. In addition, the report also contained the detailed information about these people’s period of stay in the hotel, expenses and payment of their purchases and entertainment, in tandem with their travel arrangement in Macao.

According to Articles 3(1), 4(1)(1) and 7(1), the Personal Data Protection Act (PDPA, Law 8/2005), Company B’s processing of hotel customer personal data, including their sensitive data (for instance, information about their expenses while travelling in Macao and so forth, which are related to their personal lives), falls under the regulatory scope of the said Law.

Taking into account in this case, the data controller (Company B) and the data recipient (Company A) are both commercial organisations, Company B could process personal data, but excluding data of sensitive nature, only based on the consent of the data subjects or the legitimacy under Articles 6(1) and 6(5).

Company B admitted that, without the data subjects’ consent, it disclosed their personal data to a third party. Moreover, this Company failed to justify its disclosure was aimed at executing the contract it concluded with its customers, accordingly, failing to establish the legitimacy given in Article 6(1). As for the legitimacy governed by Article 6(5), Company B explained that since X owned a number of
companies that indirectly enhanced his major ownership of Company B’s capital, and X’s acts could endanger the company business in Macao. However, as the aim of Company A to collect data from Company B was to investigate whether X violated the anti-corruption law of where Company A is located, by which the ultimate goal was to protect the commercial interests of the group. Article 5 of the PDPA specified that “data processing shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed”. The data Company B collected from its hotel business should be used for the same business. If such data was forwarded for its parent company’s investigation, it had already deviated from the data collection purposes. The hotel customers of Company B would not have expected their personal information to be disclosed for investigation purpose. In other words, this is already beyond the reasonable expectation of the hotel customers, consequently it should not deem that their interests do not prevail, therefore Company B did not have the legitimacy as referred in Article 6(5) of the PDPA. Company B by all means did not fit for the conditions of legitimacy as defined by Article 6 of the said law.

In view of processing sensitive personal data, the law laid down more stringent requirements than processing ordinary personal data. When a controller does not have the prerequisite for processing ordinary personal data, definitely it does not have the legitimacy to process sensitive data. Considering the fact that Company A has initiated a legal proceeding against X, but in which Company B is not an interested party, the derogation specified in Article 7(3)(4) of PDPA, which governs the exemption of processing sensitive data by controllers, does not apply to its forwarding of data. As both Articles 6 and 7 of the PDPA intend to govern a data controller’s processing of personal data on the prerequisite for processing legitimacy, particularly Article 7 is a special provision aimed at safeguarding processing sensitive data. As a consequence, Company B in the current case does not fit for the conditions to process sensitive information specified by Articles 6 and 7 of the same Law, as a result it should be sanctioned with more serious violations, i.e., Article 7 of the PDPA.

On the other hand, in GPDP’s views, Company B revealed the customer information to the investigators sent by Company A, this is equivalent to transferring customer data outside the Macao SAR. However, Company B has never applied to GPDP for any notification, authorization or decision for its transfer of personal data according to Article 19 and 20 of the PDPA. As a matter of fact, Company B’s transfer of information to Country D violated Articles 19 and 20 of the same Law.

**Result**

In view of how Company B disclosed the data and the influence it may have brought to the data subjects, in addition to its degree of guilt, cooperation during investigation and as a first-time offence, GPDP decided to impose sanctions. Since Company B revealed its customers’ data, including sensitive data, to a third party without fulfilling Article 7 of the PDPA, and transferred the data out of Macao SAR without meeting the conditions governed by Articles 19 and 20, such acts already constituted two administrative infractions. Therefore, a fine of MOP$20,000, as MOP$10,000 for each infraction, was imposed to Company B, according to Articles
33(2) and 34(2) of the same law. These sanctions have been implemented.
Case 12

Payroll slip distributed without data masking

Case Briefing

In March 2013, GPDP received a complaint, referred by Institution A, from X, an employee of Bureau B. X pointed out that the payroll slip he had received was without any data masking and its contents (including the employee’s name, contact, department, salary, overtime compensation and various allowances, etc.) could have been seen by others. Every month after the division secretary received the payroll slips of staff members, he/she would deliver them to the department head for perusal before distribution. X questioned whether this division head has the right to look at these slips.

Due to what has been described in the current complaint could lead to violations of the Personal Data Protection Act, Institution A referred this case to GPDP to follow up.

Analysis and Conclusion

While being asked to provide information, X filed a complaint with GPDP about the handling of payroll slips by Bureau B. Since the practice of the concerned division head, according to B, not simply involved X’s personal interest, therefore, it did not hinder GPDP from analyzing and following up when necessary.

In accordance with Articles 4(1)(1) and 3(1) of the Personal Data Protection Act (Law 8/2005), the data processing involved in this case is within the regulatory scope the same Law.

According to the investigation, Bureau B is a legal person of public law (pessoa colectiva de direito público). With the open design having been used for many years, the payroll slips were designed and printed by Bureau B. After the slips were printed, they would be divided into batches according to the employees’ department, then they were put into one sealed envelope before being delivered to the concerned department head to follow up. The department head or his or her secretary would then distribute them to each staff member. However, some departments would place such slips in a specified location for the staff members to collect personally. In some other cases, if requested, a number of these slips were delivered to the personnel department for the staff to collect.

In GPDP’s opinion, as a public authority of relatively larger scale (with over 1,000 employees), the said distribution by Bureau B could prevent others from accessing the data on the slips while they are delivered from the personnel department to other departments, during which the risk of data leaking or mishandling could be reduced. Moreover, Bureau B also allows its staff to personally collect their payroll
slips at the personnel department if they have requested so. Under such circumstance, it incurs relatively lower risks as no delivery was taking place.

According to Bureau B, it has not set up any uniform policy for the distribution of payroll slips, and the arrangement was decided by the head of each department. Even though the staff members who are responsible for the distribution could have access to the slip data, but are bound by professional secrecy (under Articles 18(1) and Article 41 of the said Law), thus causing lower risk of information leakage. However, as some departments simply placed the slips in a lever arch file for staff to pick up and, due to the open design, the slip data could be accessed by any third parties while collecting their slips. Since this kind of access has no relation to the carrying out of duties and it is possible for the slips to be taken away intentionally or unintentionally, therefore, Bureau B was unlikely to monitor the payroll distribution and collection effectively.

Although Bureau B to a certain extent took measures to enhance data security of the distribution process, in a number of cases internal supervision was insufficient. Afterwards, Bureau B promised to make improvements, including better design for the said slips, thus similar skepticism about the distribution process could be avoided in the future.

On the other hand, after analyzing the distribution process, it was found that the previously mentioned envelopes were addressed to the department heads (i.e., the division heads). Thus, unless a division head has instructed his or her secretary earlier to open the envelope and distribute the enclosed payroll slips, it was not improper for a secretary to pass the envelope to the division head, which is also within the scope of Bureau B’s competence. Moreover, division heads who accessed the payroll data from carrying out their duties are bound by professional secrecy, they shall not disclose or disseminate the concerned data without justified reasons or appropriate consent. Thus, there was no indication that GPDP should follow up the case.

In summary, the processing of data by Bureau B did not breach the Personal Data Protection Act, but there was room for optimization.

**Result**

Several departments of Bureau B placed their staff’s payroll slips in lever arch files and asked the staff to collect personally. Even if the Bureau masked the data on the slips or sealed these slips in the future, it would still be difficult to monitor the process. Therefore, the said Bureau should improve the administrative measures for the mentioned distribution process in order to strengthen its internal supervision. However, GPDP could not assume that Bureau B violated the Personal Data Protection Act while processing its staff’s personal data, in addition that this Bureau has already offered improvements on the issues. Therefore, it was unnecessary for GPDP to follow up in this regard. GPDP already informed Bureau B, in writing, of the issue and requested follow ups, as well as notifying Institution A and X of the investigation result.
Case 13

Personal data on treatment certificate

Case Briefing

Mr. X reported to GPDP that a treatment certificate he received from Hospital A contained his name, age, and patient number.

In X’s opinion, it was unnecessary to print the patient’s age on the certificate and asked GPDP to follow up.

Analysis and Conclusion

Under Articles 4(1)(1) and 3(1) of the Personal Data Protection Act (Law 8/2005), the data processing involved in this case is within the regulatory scope of the said Law.

In general, if a patient took the initiative to receive treatment in and applied for a treatment certificate from Hospital A, his data was processed based on his explicit consent. As a consequence, the Hospital also has the legitimacy as stipulated in Article 6 of the said Law.

In GPDP’s opinion, upon the patient’s application for a certificate, on which Hospital A printed the patient’s information is to assure the identity of the certificate applicant. This practice did not deviate from the processing purpose, which is also in line with Article 5(1)(2) of the same Law.

At present, neither the Macao Civil Servants Regulations (Estatuto dos Trabalhadores da Administração Pública), which regulates the civil servants; nor the Law of Labor Relations (Lei das relações de trabalho), which regulates general labour relations, governs the data contained on a treatment certificate. As a consequence, upon the patient’s application, Hospital A, being a professional medical institution, has the rights to decide the content to be revealed therein. As age data is significant in establishing patients’ identities, it helps to avoid patient identification errors caused by identical names. Moreover, patient number is also useful in assuring patient identity. Therefore, Hospital A’s practice of listing out personal data including number, name and age did not go beyond the purpose a certificate serves, which is in line with Article(1)(3) of the Law previously mentioned.

In summary, Hospital A’s practice did not violate the Personal Data Protection Act.
Result

The case was closed.
Law Implementation

I. Following ups of applications

In 2012, applications for personal data processing received by GPDP included 40 applications for opinion, 27 applications for authorization, and 291 notifications on personal data processing (73 of which concerned transfer of personal data outside Macao SAR and 218 notifications of other types of personal data processing).

Figure 11 – Types of applications for personal data processing

<table>
<thead>
<tr>
<th>Application Category</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications</td>
<td>291</td>
</tr>
<tr>
<td>Notifications on transfer of personal data outside Macao SAR</td>
<td>73</td>
</tr>
<tr>
<td>Notifications on other types of personal data processing</td>
<td>218</td>
</tr>
<tr>
<td>Applications for authorisation</td>
<td>27</td>
</tr>
<tr>
<td>Applications for opinion</td>
<td>40</td>
</tr>
</tbody>
</table>
1. Opinions issued

The GPDP received a total of 40 applications for opinion in 2012, a 25% rise over the 32 cases in 2011. Together with the 6 applications left over from 2011, the GPDP processed 46 such applications in the year, 43 of which were concluded.

Of the 40 applications for opinion in 2012, 27 were from public institutions, 11 were from private institutions and 2 were from individuals.

Figure 12 – Increment in applications for opinion

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>27</td>
</tr>
<tr>
<td>2008</td>
<td>35</td>
</tr>
<tr>
<td>2009</td>
<td>35</td>
</tr>
<tr>
<td>2010</td>
<td>24</td>
</tr>
<tr>
<td>2011</td>
<td>32</td>
</tr>
<tr>
<td>2012</td>
<td>40</td>
</tr>
</tbody>
</table>
2. Authorisations issued

Of the 27 applications for authorisation received by the GPDP in 2012, 26 applications concerned personal data combination. Among them, 17 were from public institutions, 10 from private institutions. The number of applications for authorisation in 2012 remained almost the same level as the previous years (25 applications for 2009; 28 for 2010 and 24 for 2011).

Taking into account the 52 applications carried over from 2011, the GPDP had 79 applications to process in 2012, of which 72 were concluded and for which 20 authorisations were issued. Some of the applications which concluded as closed cases proved not involving personal data combination or authorizations of other sorts.

Figure 13 – Increment in authorization applications

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>15</td>
</tr>
<tr>
<td>2008</td>
<td>152</td>
</tr>
<tr>
<td>2009</td>
<td>25</td>
</tr>
<tr>
<td>2010</td>
<td>28</td>
</tr>
<tr>
<td>2011</td>
<td>24</td>
</tr>
<tr>
<td>2012</td>
<td>27</td>
</tr>
</tbody>
</table>
3. Notification of personal data processing received

In 2012, the GPDP received a total of 291 notifications on personal data processing (73 of which concerned transfer of personal data outside Macao SAR and 218 notifications on other types of personal data processing). The number of notifications of personal data processing increased significantly over the 125 notifications of 2011, mainly due to the enhanced efforts made by the GPDP to promote the registration of personal data processing, as well as the improved awareness of personal data protection amongst organizations.

With the 335 cases carried over from 2011, the GPDP had 626 cases of personal data processing notifications to handle, of which 559 were concluded. Of the 73 notifications for transfer of personal data outside Macao SAR received during 2012, 8 were from public institutions, and 65 from private ones. As to notifications regarding other types of personal data processing, 156 were from public institutions and 62 from private ones.

Figure 14 – Increment of notifications of personal data processing

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>68</td>
</tr>
<tr>
<td>2008</td>
<td>216</td>
</tr>
<tr>
<td>2009</td>
<td>359</td>
</tr>
<tr>
<td>2010</td>
<td>361</td>
</tr>
<tr>
<td>2011</td>
<td>125</td>
</tr>
<tr>
<td>2012</td>
<td>291</td>
</tr>
</tbody>
</table>
II. Coordination and promotion of law implementation

1. Development of guidelines

Being the regulatory authority, the GPDP continued to deepen the understanding of the PDPA through law enforcement and to promote compliance of law, in addition to establishing legal guidelines. In November 2012, the GPDP published the reference document *General Notes on Handling Personal Data by Non-Tertiary Education Institution*, mainly targeting the education sector in Macao, hoping to effectively protect the lawful interests of the respective data subjects and educational institutions and to promote the protection of personal data in Macao.

In addition, in view of the situations that most merchants required customers to provide their IDs when they paid in credit/debit cards, due to anti-money laundering obligations and the guidelines for anti-terrorist financing or card transaction security etc., many merchants and customers were in doubt and found it controversial whether asking for IDs is in compliance with the PDPA. The GPDP, therefore, drafted the document *Guidelines on Merchants’ Processing of Identification Documents of Payment Cardholders*. After consulting the banking industry and the relevant public departments, the GPDP made appropriate changes to the relevant text.

2. Online inquiry system for personal data processing

In order to facilitate residents to consult the database and also to improve the transparency of public and private institutions in personal data processing, the GPDP has developed an online inquiry system for personal data processing. The residents could log onto GPDP’s website to access the system. And as of December 31st 2012, the GPDP has received 1,296 notifications regarding personal data processing (917 from public departments and 379 from the private sectors and individuals), of which 1,229 cases have been processed. At present, a total of 933 valid registrations (including 664 from public institutions and 269 from private institutions and individuals) were recorded. The above-mentioned registrations have been stored in the online inquiry system for personal data processing of the GPDP.

3. The translation of international reference documents

As the Personal Data Protection Act of Macao has the same legal origin of European laws, personal data protection experience of the EU is worth referencing. The GPDP, therefore, has been translating EU documents into Chinese, as a source of reference for the Macao community. During 2012, three EU legal documents were translated by the GPDP, including:

1) Opinion 15/2011 on the Definition of Consent;

2) Opinion 3/2012 on Developments in Biometric Technologies; and
3) Opinion 05/2012 on Cloud Computing.
Connection, Cooperation and Publicity

I. International and regional connection

In the era of advanced information technology, information flow has crossed geographical boundaries. In addition to keeping pace with the international community in the protection of personal data and for better developing personal data protection work in Macao, while strengthening communication and cooperation with other regions, the GPDP has been actively participating international conferences and exchange programs on personal data protection, for example, attending the Asia Pacific Privacy Authorities Forum as an observer, to establish close communication channels with personal data protection agencies in other countries or regions and to maintain close contact and regular exchanges of law enforcement experience with other authorities and learn from their development.

After years of efforts, the GPDP finally became a member of both the Global Privacy Enforcement Network (GPEN) and the Asia Pacific Privacy Authorities (APPA) in July 2012, which is not only the recognition and encouragement of the international community for GPDP, but also a spur encouraging us to continue to optimize our work and to make Macao a successful region of personal data protection.

1. Data Protection Awareness Seminar

At the invitation of the Government of Malaysia, Mr. Yang Chongwei, Deputy Coordinator of the GPDP attended the Data Protection Awareness seminar held on February 9th in Kuala Lumpur and the opening ceremony of the Malaysian Department of Personal Data Protection. Since Malaysia’s Personal Data Protection Act would come into effect soon, Mr. Yang Chongwei, Deputy Coordinator of the GPDP introduced to the participants about the implementation of the Personal Data Protection Act in Macao and shared with them the experience in personal data protection. The speakers of the Seminar also included Ms. Katrine Evans, Assistant Commissioner of the Privacy Commissioner of New Zealand, and the officials, academics and sector representatives from Malaysia.

2. The Asia Pacific Privacy Authorities forum

The GPDP participated as an observer in the 37th Asia Pacific Privacy Authorities Forum, held on June 13th–15th in Hong Kong, and participated as a member for the first time the 38th Asia Pacific Privacy Authorities Forum, held on December 3rd–4th in San Francisco. The representatives reported their recent work during the Forum and discussed the law enforcement and the development of privacy protection, as well as how to effectively carry out cross-border cooperation, etc.
II. Community relations

The representatives of Caritas Macao – Suicide Prevention Services paid a visit to the GPDP on June 20th and met with Deputy Coordinator Yang Chongwei. The two sides introduced their scope of work and responsibilities, and exchanged views on their daily work that may involve personal data.

On July 23rd and July 25th, Coordinator Chan Hoi Fan, respectively, met Ms. Ho Sio Kam, Director of the Chinese Educators Association of Macao, and the person in charge of the Macao Catholic Schools Association. In the two meetings, both sides introduced their recent work, and Coordinator Chan Hoi Fan also introduced the preliminary draft of General Notes on Handling Personal Data by Non-Tertiary Education Institution, hoping to receive the coordination and support from the local education sector. She encouraged the sector to actively express their views on the draft in order to reach a consensus, to further improve the contents and to improve its operability and effectively protect the legitimate interests of the educational organizations and the data subjects.

III. Publicity and promotion

As a persistent channel of education, publicity always requires one to keep pace with the times. In 2012, the GPDP continued to carry out and optimize in-depth publicity work for the Personal Data Protection Act by making use of hard-copy and electronic publications, video and audio productions, and to organize a variety of events, such as the four-panel cartoon competition. To open up new communication channels, in this year, for the first time advertisement outside buses was used, in order to communicate to the public data protection. The GPDP also cooperated with the Companhia de Electricidade de Macau (CEM) to send leaflets to local merchants and citizens, in order to deepen public awareness of personal privacy protection.

In 2012, one of our focus is to educate high school and college students. Therefore, in April, at the invitation of the Debate team of Kiang Wu Nursing College of Macao, the staff of the GPDP attended the event it organized and explained to the students and teachers about the PDPA. Additionally, in September and October, the staff of the GPDP attended respectively the events organized by the volunteer team of the Macao New Chinese Youth Association and the volunteer team of the Legal Affairs Bureau, explaining to the participants about the issues related to personal data protection via sharing and practical examples.

At the same time, by cooperating with public and private organizations, we conducted many training courses, presentation sessions, case sharing sessions, and seminars relating to the PDPA, to have direct contact with the participants, and to exchange views and to listen to their opinions and suggestions, in order to better plan and promote the protection of personal data in Macao.
1. Seminars on the PDPA

Holding seminars on the PDPA is one of the GPDP’s publicity priorities. Via those seminars, the GPDP could explain to the participants about the PDPA and issues relating to personal data processing, in addition to exchanging views regarding data processing in their daily work. In 2012, the GPDP held 30 seminars in cooperation with 14 private and public institutions, with a total of 1,960 participants.

![Figure: Seminars on the Personal Data Protection Act](image)

<table>
<thead>
<tr>
<th>Year</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of participants</td>
<td>1,339</td>
<td>1,169</td>
<td>1,041</td>
<td>1,561</td>
<td>1,960</td>
</tr>
<tr>
<td>Number of seminars</td>
<td>22</td>
<td>23</td>
<td>23</td>
<td>25</td>
<td>30</td>
</tr>
</tbody>
</table>

2. Conferences and seminars

1) Debate - Personal Data Privacy and Confidentiality (legal and ethical aspects)

At the invitation of the Kiang Wu Nursing College of Macao, on April 13th, the GPDP participated in the discussion held by the debate society of the Student Union. During the event, Yang Chongwei, Deputy Coordinator of the GPDP gave a brief introduction to the students and teachers of the Kiang Wu Nursing College of Macao on the main provisions of the PDPA. Then the students were divided into groups to analyze the personal data protection issues involved in a simulated medical case and report their views. Their performance was reviewed in the end by the teachers and the Deputy Coordinator.

2) Seminar on Policies and Practices of Personal Data Protection

On June 15th the GPDP and the Legal Affairs Bureau held the Seminar on Policies and Practices of Personal Data Protection, at the Training Centre for Employees in the Public Services. Representatives of the members of the Asia Pacific Privacy Authorities, members of the Portuguese Data Protection Authority, experts and scholars from Mainland China, introduced the personal data protection system of Mainland China, Portugal and the Asia-Pacific region, and shared their experiences to more than 200 representatives from the public and private institutions, persons from the legal sector, and scholars in Macao.

3) International Experience on Personal Data Protection Seminar

In order to promote the work of personal data protection in Macao, broaden
international perspective, and more effectively protect the legitimate rights and interests of data subjects and controller, the GPDP and the Legal Affairs Bureau held the International Experiences on Personal Data Protection Seminar, on June 16th at the Grand Hyatt Macao Hotel. The seminar was attended by officials, experts and scholars from privacy protection organizations of Hong Kong, Australia, New Zealand, Japan, Portugal, Canada, Mexico, etc. More than a hundred people attended the sessions named International Experience of Regulating Cross-Border Flow of Personal Data, Public Interests and the Rights of Personal Data Privacy, etc.

4) The Lecture on Video Surveillance in Public Spaces and the Protection of Personal Data

The Lecture on Video Surveillance in Public Spaces and the Protection of Personal Data was held on June 18th, which was co-organized by GPDP and the Office of the Secretary for Security. Guest speakers included Dr. Isabel Cristina Cerqueira Da Cruz, Secretary General of the Portuguese Data Protection Authority and Dr. Sonia Cristina De Sousa Pereira, and representative from the Portuguese Data Protection Authority. They shared their experiences of using video surveillance in public spaces and how to protect personal data during the process with more than 100 participants attended the event, coming from the Unitary Police Service, Macao Customs Service, Public Security Police Force, and the Judiciary Police.

5) The Direct Marketing and Personal Data Protection Seminar

To generate the awareness of direct marketing and personal data protection in Mainland China, Hong Kong and Macao, the GPDP, on November 9th, organized the Seminar Direct Marketing and Personal Data Protection Seminar, which invited experts and scholars, managers or representatives of the supervisory and law enforcement agencies of the said places to discuss and comprehensively exchange their experience in direct marketing and personal data protection.

The Seminar included four main topics: privacy regulation of direct marketing, consumer protection in direct marketing, value of direct marketing in the market, and regulation of direct marketing in the telecommunication sector. The event invited officials and representatives from more than one hundred institutions of different sectors that relate to direct marketing, including banking, insurance, beauty, telecommunications and gaming industries as well as government agencies and educational institutions.

6) Lectures and seminars relating to the Personal Data Protection Act

At the invitation of the University of Saint Joseph, on November 26th, Deputy Coordinator Yang Chongwei attended the seminar the Implementation of the Personal Data Protection Act, and explained the PDPA and its implementation in Macao to teachers and students of the University.
7) Consultation sessions

In order to promote the work of personal data protection in Macao and more effectively protect the legitimate rights and interests of data subjects and educational institutions, the GPDP organized four consultation sessions in September and October, in order to seek opinions from the local educational institutions on the draft of the document *General Notes on Handling Personal Data by Non-Tertiary Education Institution*, in a bid to reduce the troubles and burdens of educational institutions that might face during disputes of personal data processing and to promote effective implementation of the PDPA in Macao.

Considering the doubts and queries regarding asking payment card customers to produce their ID during transactions, the GPDP, on October 15th, organized a consultation session on the document *Guidelines on Merchants’ Processing of Identification Documents of Payment Cardholders*, in order to consult the banking industry and payment card organizations for their opinions, with a view to improve the guidelines and safeguard the lawful rights of stakeholders.

3. Contact with the media

In order to enhance the transparency of its work, the GPDP released information on personal data protection to the public through various channels, including publishing press releases and giving media interviews.

Moreover, the GPDP held regular press conferences to publish cases in which penalties were given, in order to remind the public to process their own and others’ personal data cautiously. For example, on March 5th, the GPDP organized a press conference and published the investigation outcome of four cases.

On July 19th, head of Exmoo News visited the GPDP and had a meeting with Deputy Coordinator Yang Chongwei, during which both sides introduced their work and responsibilities and exchanged views.

4. Training Courses

1) Personal Data Protection Act and personnel data management

The GPDP continued to organize courses regarding PDPA and personnel data management, in collaboration with the Macao Productivity and Technology Transfer Center. The courses were organized in May, June, October, and November, with a total of 88 students enrolled. The course was mainly for professionals of human resource management, giving introduction to the PDPA and discussing issues commonly found during processing personal data relating to human resources management. Exams were included in these courses; certificates were awarded to students who reached the attendance standard and passed the exams.

In addition, the GPDP, together with the Macao Productivity and Technology
Transfer Center, offered the Conceptual Course — Personal Data Protection for the staff members of the University of Macao in February. With over 20 participants enrolled, the course was aimed at improving their understanding and awareness of personal data protection.

2) 2012 Police Officer Course

On the invitation of Public Security Police Force (PSP), the GPDP gave lectures on the PDPA to students of the PSP 2011 Police Officer Course between May and August. The course aimed to explain the PDPA and more than 990 police officers attended.

5. Publicity through media

1) Privacy & You

In 2012, the GPDP continued publishing the newspaper column Privacy & You in Chinese and Portuguese newspapers in Macao. The contents were mainly based on real cases or actual situations, in order to generate the public awareness of privacy protection. The GPDP also translated those column articles into English and publish them in local English newspapers.

2) Promotional video and audio clips

For publicity under the theme of “personal data is important, awareness of protection is indispensable”, the GPDP continued the publicity in electronic media, especially during festivals such as Christmas and the New Year, when collection and processing of personal data by the commercial sector were most frequent. Thus, the GPDP increased the publicity during these periods, broadcasted six promotional video clips on four local TV channels and six promotional audio clips on local radio stations at different period of time, to raise the awareness for personal data protection through interesting means.

3. Bus advertising

To continue promoting the PDPA and diversify publicity channels, for the first time, advertisements regarding personal data protection were put outside buses of the three local bus companies, with which the importance of personal data protection could be communicated to the public.
6. Various forms of publicity

1) The four-panel cartoon competition on the Personal Data Protection Act

In order to deepen the residents’ understanding of the PDPA, the GPDP organized a four-panel cartoon competition on the Personal Data Protection Act during September and October 2012. There were two groups of participants, the student group and the public group, submitting a total of 35 work. Macao cartoonists Mr. Chan Wai Fai, Mr. Chou Cheong Hong, Mr. Michael Wong and the Deputy Coordinator of the GPDP Mr. Yang Chongwei were invited as judges. 16 winning work were selected, based on the criteria of topic expression, creativity, composition and overall quality. The coordinator of the GPDP, Chan Hoi Fan, and the judges awarded the prizes to the winners of the competition and invited their friends and family members to participate in the awarding ceremony.

After the announcement of the competition results, the six awarded work, of the first, second and third prizes of the two groups, were published in the local Chinese newspapers, in order to promote the message of personal data protection.

2) IT Week 2012

During the previous IT Week, the booth was effective in the promotion of the Personal Data Protection Act. Taking into account of such experience, in order to raise people’s awareness of self-protection, on November 23rd to 25th, the GPDP continued to participate in the activities of the IT Week 2012, at the Tap Seac Multisport Pavilion. The booth of the GPDP informed the residents personal data protection through funny games, which were welcomed by the residents.

3) Pop-up banners

To continue the publicity and promotion of the PDPA, the GPDP produced 9 easy pop-up banners and placed them in locations designated by the Union of Neighbourhood Associations of Macao, General Association of Chinese Students of Macao, and the Macao New Chinese Youth Association. The banners were placed for the purposes of exhibition and promotion, in order to generate the importance of personal data protection and awareness of law compliance in the public community.

7. Journals and leaflets

1) The GPDP Newsletter (seasonal journal)

The GPDP continued to publish its seasonal journal – the GPDP Newsletter – in printed and electronic versions, as part of its promotional efforts. The newsletter not only can help the public to deepen their understanding of the latest information and
activities of the GPDP but also raise their awareness of the PDPA, further bringing benefit to the publicity and promotion of the GPDP.

2) Annual Report 2011

Publishing the Annual Report of the GPDP is also a part of the promotional efforts of the GPDP. Annual Report 2011 summarized GPDP’s legal work of the year, including legal enquiries, case investigations, and law implementation. It also outlined GPDP’s international engagements in the previous year, community relationship building and publicity and promotion. As per Article 25(5) of the PDPA, the report also published some of the opinions and authorizations issued during 2011.

3) Leaflets – Data Processing Policies Protects Lawful Interests

In line with GPDP’s publicity work under the theme of “personal data is important, awareness of protection is indispensable”, GPDP has produced the leaflet Data Processing Policies Protects Lawful Interests (Chinese and Portuguese), which were sent to the merchants and citizens in Macao with the help of Companhia de Electricidade de Macau (CEM), as an attempt to raise public awareness of personal privacy protection.

4) Publicity items

Taking into account the aim of promoting public awareness of personal data protection, the GPDP produces a variety of publicity items on a regular basis to remind citizens the importance of personal data protection.

Table: Publicity items prepared by the GPDP

<table>
<thead>
<tr>
<th>Items</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013 Desk calendars</td>
<td>2,000</td>
</tr>
<tr>
<td>New Year Greeting cards</td>
<td>2,000</td>
</tr>
<tr>
<td>Christmas Cards</td>
<td>500</td>
</tr>
<tr>
<td>IPhone pens and ballpoint pens</td>
<td>1,000</td>
</tr>
<tr>
<td>Ballpoint pens and highlighter pens</td>
<td>5,000</td>
</tr>
<tr>
<td>Environmental protection tableware</td>
<td>2,000</td>
</tr>
<tr>
<td>Universal Travel Bag</td>
<td>1,000</td>
</tr>
<tr>
<td>Portable digital reader</td>
<td>500</td>
</tr>
<tr>
<td>Handbag</td>
<td>200</td>
</tr>
</tbody>
</table>
IV. Website

As one of the effective channels of communication with the public, the GPDP keeps updating its website contents and design, in order to serve the needs and inform the public of its latest information. During 2012, a record of 90000 visits to the GPDP’s website was recorded.