Office for Personal Data Protection

Annual Report 2010

Unofficial English Translation

Disclaimer

This is an unofficial English translation of some major chapters in the Annual Report 2010 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
August, 2011

Preface

For more than three years since its inception in 2007, the Office for Personal Data Protection (GPDP) has been promoting the Personal Data Protection Act (PDPA, or Law 8/2005) in all sectors of the society through various channels. Through these years, the GPDP has been keeping with the spirit of "awareness and education first, penalty second". The year of 2010 saw the gradual maturity and a new stage of development, with human resources growing and working conditions improving. All the staff members have been working with a proactive attitude to join efforts for the implementation of the PDPA.

The year of 2010 saw some major events in international and inter-regional protection of personal data, which have posed certain challenges to GPDP. The "Google incident" reverberated around the world, and Macao, as an international city, cannot stay out of it. Together with authorities for personal data protection from other countries and regions, the GPDP launched investigations into the incident. Other incidents like selling personal data for profit in the neighboring regions also alerted Macao due to the close geographical proximity. Thus, the GPDP took initiatives to investigate and follow-up the incident, in order to prevent similar selling of data in Macao. All these reflected that Macao is closely linked to other countries and regions, and personal data protection in Macao must keep pace with global development.

As we gradually expand the reach of our promotions and deepen our work, we are impressed that in Macao no matter data controllers or Macao residents who are data subjects are increasingly aware of the importance of personal data protection. Institutions have enquired how to handle personal data in accordance with laws; residents have inquired how to protect their data from illegal use and reported improper handling of data. The number of such cases has been increasing over the years. Some industries have started developing their own code of conduct for personal data processing in order to enhance industry regulation and to avoid the legal consequences from inadvertent legal violations caused by unclearly defined areas.

It is worth mentioning that we have successfully implemented a system of notification of personal data processing amongst public institutions. Macao is the first one to implement such a system among the Asia Pacific countries and regions, which showcased that although Macao started late in personal data protection, it can also make achievements by giving full play to its characteristics as a small town. The implementation of the system has been dependent upon the full support of the Chief Executive and the full cooperation of the related public institutions. Hereby we would like to offer our heartfelt thanks to them.

Social development, transfer and protection of personal data are increasingly globalized, and international and inter-regional privacy institutions and organizations continue to grow. Certain legal and institutional standards have been developed in various regions, for example, the system of EU and the system of former Commonwealth countries. Some members of the international/inter-regional

organizations have signed cooperation agreements on personal data protection, forming international or inter-regional networks of regulatory authorities of personal data protection, in order to join efforts to combat unlawful activities. Originated in Europe, Macao's legal norms are very strict. Due to the fact that GPDP is a temporary public department, this created difficulties for it to become a member of international and inter-regional organizations. In order to become a member of networks of personal data protection authorities, the priority at present is the formal establishment of an institution for personal data protection. We believe that establishment of an institution for personal data protection with clear mandate and legal competence will help promote Macao's reputation for the rule of law and its international status and widen and deepen its efforts in personal data protection.

Being the regulatory authority monitoring the implementation of the Personal Data Protection Act, the GPDP has a deep sense of responsibility. We hope that with the team work of all the staff of the GPDP and the full support of the public and private institutions, personal data protection in Macao will achieve more encouraging results.

Coordinator

Chan Hoi Fan

Major events

2/2010

- Extensive exchanges with Roderick Woo, Privacy Commissioner for Personal Data of Hong Kong, who was visiting Macao.
- Two follow-up seminars on Registration of Personal Data Processing for the public departments.

3/2010

- The inauguration of Coordinator Chan Hoi Fan, chaired by the Chief Executive the Honorable Dr. Chui Sai On.

5/2010

- Launching the Online Self-assessment System for Personal Data Privacy Awareness, one of the Privacy Awareness Week (PAW) 2010 activities.

6/2010

- Attending the 33rd Asia Pacific Privacy Authorities Forum as an observer.

8/2010

- Publication of the document *Right to Information in the Indirect Collection of Personal Data.*
- The Conference on Protecting Your Customers' Data, in collaboration with the Judiciary Police and the Payment Card Industry – Organization of Macao.
- A visit by the representatives from the Korean Information Security Agency (KISA).

11/2010

- Participation in the IT Week 2010.

12/2010

- Attending the 34th Asia Pacific Privacy Authorities Forum as an observer.

Processing of enquiries and complaints

I. Enquiries about law

In 2010, the Office received a total of 704 enquiries about personal data (excluding those of routine procedures), of which 699 were concluded. Among them, 33.8% of the enquiries were regarding the legitimacy of personal data processing and 88.2% were phone enquiries. In terms of the types of enquirers, the percentage of public and private institutions was rather close, whereby the former accounted for 21.6%, the latter 28.3% and individual enquirers of 50.1%.

In addition, 5 enquiries from 2009 were also concluded.

Figure 1 – Categories of enquiries by nature

	Number of enquiries
Scope of application and definitions of the Personal Data Protection Act	114
Nature and principles of data processing	152
Legitimacy of data processing	264
Rights of data subjects	126
Security and confidentiality of data processing	32
Data combination	24
Data transfer	32
Notifications and authorizations	171
Consequences of violations	16
Guidance issued by the GPDP	27
Rights to privacy as provided for in other laws	20
Others	57

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

Figure 2 – Means of enquiry

	Number of enquiries	%
Phone	621	88.2
Online	52	7.4
Personal visits	28	4.0
Mail/fax	3	0.4

Figure 3 – Categories of enquirers

	Number of enquiries	%
Public institutions	152	21.6
Private institutions	199	28.3
Individuals	353	50.1

While the GPDP carried out its works further, with the growing sense of personal data protection among citizens, the recent years saw a corresponding rise in the number of enquiries. In 2010, the number of enquiries increased at a rate of 16.9%.

Figure 4 – Increment of enquiries

Year	2008	2009	2010
Number of enquiries	207	602	704

II. Case investigation

The GPDP identified a total of 63 cases for investigations in 2010, a rise of 34.0% over the 47 cases in 2009. With the 29 cases from 2008, the GPDP investigated 92 cases, of which 43 were concluded. Of the 63 new cases investigated in 2010, 38.1% was regarding cases in which processing legitimacy were not established, 46.0% regarding incompliance of data processing principles, and 50.8% in regard complaints from data subjects. Of the parties investigated, private institutions accounted for the majority, in the total of 66.0%. Of the 43 concluded cases, 20.9% of them were found genuinely reported.

Figure 5 – Nature of the cases investigated

	Number of enquiries
Breach of confidentiality obligations	2
Lack of security precautions	11
Failure to secure data subjects' rights	7
Violating data processing principles	29
Lacking Legitimacy in data processing	24
Improper access	2

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

Figure 6 – Investigated cases by ways of instigation

	Number of cases	%
Complaints	32	50.8
Reports	19	30.2
Referral	5	7.9
Voluntary intervention	7	11.1

Figure 7 – Categories of investigated parties

Number of cases	Number of cases	%
Public institutions	22	22.7
Private institutions	64	66.0
Individuals	11	11.3

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

Figure 8 – Categories of investigated private institutions

	Category	Number of cases
Commercial enterprises	Public enterprises (excluding telecommunication and the media organizations)	1
	Gaming	1
	Hotel	5
	Travelling agencies	1
	Financial sector	28
	Insurance	1
	Telecommunication	4
	Property management, cleaning and security	6
	Health and hygiene	3
	Education	1
	Media	1
	Publishing and printing	1
	Information services	1
	Marketing, consultancy services (exhibition, advertising, market research and promotion, consultancy services)	1
	Wholesale and retail	4
	Real estate (property)	1
	Other commercial enterprises	1
Associations, non-profit organizations and the like		3

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

Figure 9 – Results of cases concluded

	Number of cases	%
Verified as truthfully presented	9	20.9
Claims in discrepancy with facts	24	55.8
Unable to follow up on for lack of specific information	5	11.6
Referred to the police authorities who have the authority to follow up	1	2.3
Cancelled at the request of the subjects	1	2.3
Beyond the competence of GPDP	3	7.0

Figure 10 – Increment of investigated cases

Year	2008	2009	2010
Number of cases	35	47	63

III. Summary of selected cases

The following is the summary of some selected cases.

Case 1

Full BIR numbers of public exam candidates published in the examination venues

Case Briefing

Resident I participated in public examination X for Department A and discovered that the Chinese and Portuguese names, along with the full BIR numbers of the candidates had been published in the list of accepted candidates posted at the examination venue.

Resident I was concerned about the practice of publishing the full numbers of the candidates' BIRs, believing it to be a breach of the Personal Data Protection Act and consequently filed a complaint with this Office (GPDP).

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

Department A explained that it had published the candidates' full BIR numbers in order to avoid confusion, as there were a lot of candidates taking the exam and many of them had identical names.

In GPDP's opinion, the information that should be published in the candidate lists posted at the examination venues have not been defined in any detailed and explicit manner in the "Regulations on Workers of the Public Administration" (hereinafter referred to as the "ETAPM"), approved by Decree-Law no. 87/89/M. Article 57 of the ETAPM states only that the temporary candidate list must contain the names in alphabetical order and contain the following information: approved candidates, conditionally approved candidates and rejected candidates. We can use the provisions of the ETAPM in principle and then also the "Personal Data Protection Act" to find a solution for the present case.

The investigated information indicated that the publication of the accepted candidates' BIR numbers at the examination venue, along with their Chinese and Portuguese names by Department A, were measures taken to identify the candidates.

Although there are no legal provisions regulating the use of BIR numbers and copies, a BIR number is personal information unique to a particular individual and therefore should be processed carefully by data controllers. As such, if it is not necessary, BIR numbers should not be published, and in particular the full names and BIR numbers of the holders should not be published jointly.

As BIR numbers are unique, they can still be used to identify a candidate sufficiently even a part of them are hidden (for example if 'XX' is used instead of the last two numbers of a BIR card). Department A's publishing the full BIR numbers of the candidates in the list of accepted candidates posted in the examination venue might be against the principle of proportionality determined in Article 5.1.(3) of the "Personal Data Protection Act".

However, in GPDP's consideration, Department A published the information contained in the list to facilitate the confirmation of the personal data and location of respective examination room by the candidates. This is a perfectly legal act, carried out in good-faith and with no intention to reveal the data subject' information in an excessive manner. Moreover, the examination was held in a reserved location accessible only by the department staff and the candidates. The extent of the damage caused was relatively light and there have been no cases of personal data leakage as a result of the present case. As such, Department A is not at serious fault and its conduct did not cause any severe adverse effects.

In light of the above, GPDP concluded that Department A did not observe the terms of Article 5.1.(3) of the "Personal Data Protection Act", but its conduct did not constitute an administrative offence.

Result

GPDP sent an official letter to Department A, suggesting that it create a unified policy personal data processing during public exam procedures, namely one which would allow the exam adjudicators to possess a set of unified rules and therefore avoid the mishandling of personal data.

Department A accepted GPDP's suggestion and implemented the respective measures.

Case 2

A medical institution registered visitors' personal data

Case Briefing

Citizen X complains that a healthcare institution A requires visitors to fill in Visitor Registration Forms with such data as name, gender, ID number, contact number, the gender and bed number of the visited person, etc. Citizen X thinks that it is not necessary for Institution A to collect visitors' ID numbers.

In addition, X claimed that Institution A usually denies access should a visitor refuse to provide his personal data, which X thinks is as good as forcing the visitors to surrender their personal data. X also alleged that the security staff of Institution A had double standards in managing visitor access, e.g., some visitors were allowed access without providing their ID numbers.

X believed that A's conduct violated the Personal Data Protection Act, and filed a complaint with this Office (GPDP).

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

Article 5.1.(3) of the Personal Data Protection Act provides that "personal data must be relevant, appropriate and not excessive for the purposes for which they are to be collected and processed." Whether Institution A was over-collecting visitors' personal data in this case should be judged in reference to its purposes of data collection and whether the data collected were necessary for its purposes. In general, institutions may, for security reasons, collect visitor data such as name, type and numbers of ID documents, etc., so that the visitors may be identified. Other information to register may include the time and place of the visit and data of the visited persons.

To ensure the security of its patients and caretakers, it is apparently necessary for Institution A to collect visitors' personal data. As a person's ID number is a unique identifier of a person, it makes sense to collect it for effective and efficient identification of the visitor. Therefore, collecting personal data such as ID numbers by Institution A in security management did not constitute what X claimed to be the over-collection of personal data by the institution.

As for X's allegation that denying visitor access who fail or refuse to provide personal data is as good as forcing them to surrender their personal data, it should be

pointed out that Institution A has the right to frame its visitor registration rules to ensure the security of itself as well as the citizens in its vicinity. Besides, hospital wards are not meant for free access. As Institution A bears the responsibilities to ensure the security of the wards, the patients and other users of the institution, it has the right to register the personal data of identifiable visitors so it can trace suspects should any security incident occur. Any one visiting the institution, be it the complainant or other citizens, should abide by its rules. If they refuse to have their data registered, Institution A has the right to deny them access.

As to X's allegation that the security staff of Institution A use double standards in managing visitor access (e.g. allowing visitors access without registering their ID numbers), GPDP believed this was only the internal management issue of Institution A.

In summary, Institution A's data processing was in compliance with the Personal Data Protection Act.

Result

GPDP sent letters to X and Institution A to inform them the analysis, and referred to Institution A the issue that the security staff use double standards in managing visitor access.

Case 3

The job seekers asked for return of documents

Case Briefing

Using the information from a job advertisement in a newspaper, citizen X visited the recruiting Company A in person to apply for the job. He was asked to fill out a form with his name, ID number, etc., which he did. He also gave Company A his photos and the original of his recent electric bill receipt and a copy of his Macao resident ID card.

Afterwards, in the follow-up interview, X learned that Company A would offer him a salary less than that achievable salary advertised, if he took the job. Unhappy about that offer, X refused to take the job, and demanded that Company A return all the personal data he had supplied. Eventually however, he got only his original electricity bill receipt back.

Citizen A claimed that Company A obtained his personal data by cheating, for other illegal purposes, violated the Personal Data Protection Act, and then filed a complaint to this Office (GPDP).

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

In GPDP's opinion, while X was asked to supply his personal data to meet the Company A's requirement, as a data subject he could have chosen to either oblige or refuse to supply. However, his factual supply of his personal data may well be viewed as his consent to Company A processing of his personal data for the job application he was making, in exchange for the opportunity of landing the job. In other words, it was with X's consent that Company A processed his personal data for the recruiting, and therefore Company A has the legitimacy in the processing of his data under Article 6 of the Personal Data Protection Act.

In general, it is common practice that an employing institution collects job seekers' personal data before interviewing and assessing them for the jobs, a process that so far has shown no procedural inappropriateness.

On another score, the achievable salary promise to a job seeker as advertised in the company's ad, by a common understanding, is interpreted as the level to which the salary may attain should one get the job. Therefore, even if the salary offered to X by Company A was less than that advertised, it did not constitute inconsistency with what was advertised, nor could one conclude that the company was cheating in this

regard.

Therefore, in the absence of any evidence in support of X's allegation, GPDP cannot conclude that Company A has obtained X's personal data by cheating or used the data for any illegal purpose.

In summary, there was nothing to prove that Company A had violated the legal provisions in Personal Data Protection Act, the case should be closed.

Result

GPDP sent letters to X and Company A and informed them about the analysis and decision.

Case 4

Staff in a museum recorded the Macau Resident Identity Cards (BIR) numbers of visitors

Case Briefing

Resident I stated that in Museum A there was a price differentiation policy in its admission prices, and visitors were asked to provide their Macau Resident Identity Cards (BIR), student cards and other personal identification documents to the museum staff to register and confirm that they were eligible to receive the discount or fee waiver.

Resident I considered that BIR numbers were irrelevant for the purposes of verifying the ages of the visitors and that the museum staff did not need to register the document number. In addition to this, resident I stated that there was no "Personal Information Collection Statement" or any similar notifications posted at the museum premises. Resident I considered that the registration of the BIR numbers was a potential breach of the terms of the "Personal Data Protection Act" and consequently filed a report to this Office (GPDP).

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

Museum A explained that it registered the names and BIR numbers of the visitors for statistical purposes. However, the Museum reviewed and amended its rules after the complaints. The visitors then could only display their identification documents. Museum A no longer collected and registered any of their personal data.

GPDP believed that Museum A registered the BIR numbers of the visitors not only to verify whether they were eligible to purchase tickets at a discount price or for free, but also for financial supervision purposes; which was legitimate purpose for data processing. The data processing observed the principle of proportionality. If visitors chose to obtain a discount or fee waiver, and this act should be considered as the visitors giving their tacit consent or the execution of a contract in which the museum and visitors were parties. GPDP consequently considered that the verification of the visitors' identities to confirm that such persons were eligible to receive the discount or fee waiver was a legitimate and necessary act.

Regarding the lack of a "Personal Information Collection Statement" or a similar notice in Museum A, another issue raised by Resident I, according to the terms of article 10 of the "Personal Data Protection Act", Museum A was obliged to provide

the information required by law to satisfy the data subjects' right to information. However, the law does not force museum A to post a "Personal Information Collection Statement" or any similar notice. Museum A had declared that they no longer processed the data in such a way and had implemented a series of measures, including a "Personal Data Collection Statement", in order to improve their observance of the legal rules on the subject of "right to information" of the visitors.

In summary, GPDP believed that Museum A's conduct didn't entirely conform to the provisions stated in article 10 of the "Personal Data Protection Act" in relation to the right to information, but it did not constitute an administrative offence.

Result

GPDP sent an official letter containing the foregoing analysis to Museum A and recommended that it should set a retention period for the preservation of names and BIR numbers collected and registered to "allow people to receive discounts or waivers for the admission fee" so that they could subsequently be blocked, deleted or destroyed in a timely manner.

Museum A replied, stating that they had accepted the recommendations of GPDP and implemented the appropriate measures.

Case 5

Security Guard registers identity card and phone numbers of visitors

Case Briefing

Resident Y was a frequent visitor of Office Building X and he knew that he would be asked to register his identification card number with the security guard while going in and out of that building. One day, when Resident Y went inside Office Building X as usual, the security guard on duty asked him for his contact phone number in addition to his identification card number for registration. Although Resident Y asked for the reason right away, the security guard's only reply was that he was following instructions from his superiors, and if Resident A did not provide above information right away, he would not be allowed entry into Office Building X. In the end, he provided his contact phone number for registration.

Resident Y noticed that the "Visitor, please register here" sign on the registration counter did not ask for the contact phone number of visitors and that no relevant information on personal data collection was available. Resident Y filed a complaint with this Office (GPDP), claiming that the "Personal Data Protection Act" had been breached because of the security guard's unreasonable practice.

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

After a letter was sent by GPDP requesting clarification, Entity A and Security Company B, both of which were responsible for managing the building explained that the main purpose of the security guard requesting that visitors provide their identity card number for registration was to protect the personal and property safety of the users of that building. At the same time, the sign on the registration counter also only asked for the identification number of visitors and the collection of the contact phone number was non- mandatory.

GPDP felt that, as Entity A and Security Company B, were both responsible for managing the building as the data controller and data processer, respectively, and responsible for the processing of personal data with the purpose of protecting the offices within the building, their clients' property, and safety of the staff and other visitors, as well as providing an effective tracking and control during the outbreak of epidemics, yet still gave visitors the choice to provide personal data, the personal data was only collected with the consent of the data subjects. As such, both Entity A and Security Company B therefore legitimately processed visitors' personal data in

accordance with Article 6 of the “Personal Data Protection Act”.

Regarding the security guard collecting Resident Y’s identification card number and phone number simultaneously, as neither Entity A nor Security Company B forced visitors to provide their phone numbers and other information. The problem was thus the lack of a standardized operation practice of visitor registration by the security guards, leading to Resident Y’s yield dissatisfaction in regards to the relevant measures.

At the same time, in handling visitors’ data, Entity A and Security Insurance B also needed to follow the relevant provisions of the “Personal Data Protection Act”, including the data subject’s right to information as well as the security and confidentiality of the handling procedures.

In light of the above, GPDP believed that this was only an isolated incident with the related matter being internal management and disciplinary issues of the building management company. However, Entity A has room for improvement in ensuring the “right to information” of the data subjects.

Result

GPDP sent a letter to remind Entity A that although this was only internal management and discipline problem n this case, Entity A still needed to effectively deal with the formulation and implementation of relevant policies and measures for processing visitor data. In addition, this office also suggested that Entity A provide the registration counter with a relevant “Personal Data Collection Statement” so that when visitors exercise their “right to information”, the security guard will be in a better position to answer the questions asked in a timely manner.

Entity A replied, stating that the corresponding improvements had been made.

Case 6

Duration of posting of Candidate List and Examination Results

Case Briefing

Resident X indicated that the Professional Work Permit (taxi) Candidates List and the respective Examination Results had been posted for a long period of time on Bureau A's website and in a service area which anybody could access. Resident X filed a complaint with this Office (GPDP), claiming that Bureau A processed the personal data improperly and thus breached the "Personal Data Protection Act".

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

GPDP found that the respective candidates list and examination results list posted on the website of Bureau A included the Chinese and Portuguese names of the candidates, the first 4 digits of their identity card number, and the first 2 digits of their local driver's license. The Candidate List within the website contains 5 types of data: their candidate number, their Chinese and Portuguese names, the first 4 digits of the number of their identity card, the first 2 digits of their local driver's license, whereas the Examination Result only contained 3 types of data: the candidate number, their Chinese and Portuguese names. From this information, it is safe to assume that Bureau A could determine the identity of the data subject using only the candidate number, the Chinese name and the Portuguese name. No information could be found as reasons of publishing different types of data at different stages of the examination.

After checking the information regarding the Professional Taxi Driver's License Exam within the website of Bureau A, GPDP discovered that the lists available included the Candidate Lists from April 2007 to the date on which GPDP visited the website, and the Examination Results from January 2007 to the date on which GPDP visited the website. Both lists contained personal data of the candidates. GPDP found no indication as to whether Bureau A had set an exact deadline for the posting of these lists.

GPDP sent a letter to Bureau A requesting its explanation and follow-up.

Bureau A explained that the three items of personal data (candidate number, Chinese name and Portuguese name) were not published in a standardized manner between the candidates list and examination results list, because there might be situations where the candidates had identical names, or had lost their examination receipt, and thus did not know about their exact candidate number. Therefore, it was deemed necessary to publish the first 4 digits of the identity card number of the

candidates in order to facilitate their knowledge of the relevant information.

Furthermore, after receiving GPDP's official letter, Bureau A implemented a preservation deadline for the relevant data: the candidates list posted inside the service area would be posted one month prior to the examination until the day of the examination, and the examination results would be posted up one month after the announcement of the results. In addition, the candidates list and examination results announced through the website would be updated once a month.

In GPDP's opinion, in accordance with the terms of Article 6 of the "Personal Data Protection Act", personal data can only be processed with the data subject's clear and explicit consent or as determined by law. Pursuant to Article 3.(16) of Administrative Regulation No. 3/2008, Bureau A's responsibilities include the issue and renewal of the professional taxi drivers work permits, as well as the inspection of taxis and taxi meters. This showed that Bureau A, by law, has the right to issue and renew professional taxi drivers' licenses. Furthermore, when a candidate applies in Bureau A to participate in the written examination to obtain the abovementioned license, he or she is clearly and explicitly allowing Bureau A to use his or her personal data for examination purposes. Therefore, Bureau A legitimately processed the candidate's personal data in accordance with the terms of Article 6 of the "Personal Data Protection Act".

As it was necessary to list the personal information of candidates in the candidates list and examinations results list within Bureau A's website for the purpose of distinguishing the identity of candidates, as identification card numbers and driver's license numbers are unique, and as Bureau A had already partially hidden these numbers, therefore the publication of these types of data did not breach the principle of proportionality as specified in Article 5.1(3) of the "Personal Data Protection Act".

According to Articles 5.1.(3) and 5.1.(5) of the "Personal Data Protection Act", Bureau A should set a specific deadline for the posting of the lists according to the objective of the publishing. When such a purpose no longer exists or is fulfilled, the relevant data should be deleted right away. Bureau A followed GPDP's recommendation and adjusted its policy by setting the posting duration to no more than one month. After visiting the service area in Bureau A and revisiting its website, GPDP verified that Bureau A has taken significant steps to improve its policies and now only posts the Candidates List and Examination Results of the Professional Taxi Driver's License Examination for the same month on its website.

In summary, GPDP found no breach of the "Personal Data Protection Act".

Result

GPDP sent a letter to Bureau A and informed it about the above-mentioned analysis and recommendations. Bureau A accepted GPDP's advice and set a posting period for the respective information.

Case 7

Customer refused to receive bank transaction records by post

Case Briefing

When Resident X opened a securities trading account in Bank A, he verbally asked not to receive transaction documents by mail but instead, by email or SMS. Bank A refused his request and indicated that Resident X could only refuse to receive promotional materials by mail.

Resident X stated that he had previously opened a securities trading account with Bank B and that they used SMS instead of mail to transmit the relevant transaction information. Therefore, Resident X filed a complaint with this Office (GPDP), claiming that Bank A's conduct had breached the "Personal Data Protection Act".

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

According to Resident X's statements, although he had requested Bank A not to send account transaction records by mail, he did not provide any reasons for this request.

Resident X's declaration and notification also indicated that he had never used above account in Bank A to carry out any transaction and moreover at the present time, that account had already been cancelled.

In GPDP's opinion, in this case, Resident X had provided his personal data to Bank A in order to apply for a securities trading account. From this, it can be seen that Bank A had obtained the consent for the implementation of the contract prior to processing Resident X's personal data. Therefore, Bank A legitimately processed Resident X's personal data, in accordance with Article 6 of the "Personal Data Protection Act".

Under the terms of the "Personal Data Protection Act", data subjects enjoy different kinds of rights including the "Right to Information", the "Right of Access" and the "Right to Object". Regarding the "Right to Object", Article 12.1 of the "Personal Data Protection Act" states that if the data subject has compelling legitimate justifications related to his situation, he would be entitled to exercise his "Right to Object" in regards to his personal data and before Bank A. Although Resident X had exercised his "Right to Object", he had not provided any justifications regarding his particular situation. As such, GPDP felt that there was not enough evidence to assess whether Resident X's objection to Bank A processing his personal data was

compelling and legitimate.

Actually, different banks in Macao operate and provide services in different ways under the relevant provisions of the local financial system. For example, in situations such as the "account transaction notification measures for applicants", where the law does not provide specific provisions, each individual bank defines its own notification measures. Sending such notifications by post tends to be the most common notification method. Of course, some banks may offer other means of notification to clients such as by e-mail or SMS. This shows that each bank can set distinct notification measures according to their own policies and conditions. There is no obligation which requires all banks to serve customers the same way. In the present case, Bank A's transmission of Resident X's account transaction records by mail did not deviate from or exceed the objectives of the data processing. There was no invasion of privacy as alleged by Resident X, and no other incidents which could be construed as a breach of the "Personal Data Protection Act" were found. Therefore, when applying for the respective services, Resident X should have considered beforehand whether the bank would be able to provide the appropriate support services.

As Resident X had never carried out any transactions with the above mentioned account in Bank A, and as the account had already been cancelled, there was no need to follow up on the relevant complaint any further.

In summary, since Bank A had obtained Resident X's consent for the implementation of the contract, in accordance with Article 6 of the "Personal Data Protection Act", Bank A legitimately processed Resident X's personal data. Furthermore, Bank A's transmission of Resident X's account transaction records by mail had not deviated from or exceeded the objectives of data processing and as such Bank A in no way breached the "Personal Data Protection Act".

Result

GPDP sent a letter to Resident X informing him of the relevant analysis and decision.

Case 8

A supervisor took pictures of a security guard who was sleeping while on duty

Case Briefing

Resident X worked as a night-shift security guard at Company A. While on duty, Resident X's supervisor repeatedly took pictures of Resident X without his consent. Resident X had asked Supervisor B why these pictures were taken and asked Supervisor B not to hand these pictures back to Company A. Supervisor B did not explicitly reply and ignored Resident X's request. Resident X indicated that Company A had never told him that the pictures would be taken while on duty, and was not aware of whether such measures were applied to other employees.

Company A subsequently dismissed Resident X, claiming that X repeatedly sleeping while on duty although he was warned by the company for various times, which is a serious reach of the Code of Conduct of security guards. Company A provided pictures as evidence. Resident X consequently filed a complaint to the Labour Affairs Bureau for dismissal without just cause. While handling the complaint, the Labour Affairs Bureau showed Resident X the photos of him sleeping on duty that had been provided by Company A.

Resident X then filed a complaint with this Office (GPDP), claiming that the "Personal Data Protection Act" had been breached because Company A took pictures of Resident X without his consent.

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

Company A provided GPDP a copy of Resident X's employment contract, which stated that Resident X was bound to comply with the company's Code of Practice. Company A claimed that the company distributed and explained the regulations to any new security guards when they were employed, including that when they breached these regulations, the company could gather evidence on the spot and provide such evidence to the relevant government departments, whenever necessary.

In GPDP's opinion, to manage employees effectively, especially regarding the implementation of the rules of compliance and discipline in the workplace as determined in Law No. 7/2008, (the "Labour Relations Law") employer are, in a general manner, entitled to manage and monitor the activities of their employees in the workplace.

Company A is an organization which provides security services and is responsible for protecting the personal and property safety of their clients. As Resident X was a security guard, Company A needed to monitor whether the quality of the service he provided was up to standard.

According to the information provided by Company A, Resident X was aware of and had explicitly given his consent to the collection of on-site evidence by Company A upon any breach of its code of practice while working.

Therefore, under the terms of Article 6 of the "Personal Data Protection Act", Company A legitimately processed Resident X's personal data in monitoring whether the quality of the service provided was up to par and in executing the contract entered into with Resident X.

Company A had informed its security guards of its monitoring measures beforehand and did not handle their personal data in a secretive manner. As Company A's purpose in collecting the data was specific, clear, legitimate and directly related to its activities, it was therefore carried out in accordance with the principle of legitimacy specified in the "Personal Data Protection Act".

In fact, Company A only monitored employee activities in the workplace during their working hours and these monitoring activities were directly related to the work being carried out. At the same time, Company A only used the photos as evidence during labour disputes and employee dismissals. This shows that Company handled the photos in a suitable and appropriate manner, never going beyond the purpose of data collection and processing.

In addition, Resident X also requested that Company A return the photos in which he appeared. According to Articles 10 to 14 of the "Personal Data Protection Act", data subjects have different kinds of rights such as the "Right to information", the "Right of access", and the "Right to object", but not the "Right to the return of personal data". However, the law does not prevent Company A from answering Resident X's request to delete or return the photos to him. Therefore, Company A is free to choose whether to accept Resident X's demand, in accordance with its specific handling policies.

In summary, GPDP believed that there was no indication that Company A had breached the "Personal Data Protection Act" and the case could therefore be closed.

Result

GPDP sent a letter to Resident X and Company A, respectively notifying them of the abovementioned analysis and decision.

Case 9

Resident dissatisfied with having his name appear in a notice published within a newspaper

Case Briefing

Resident A and his wife are both owners of Unit X. As illegal additional work was carried out on Resident A's Unit X, the Land, Public Works and Transport Bureau of the Macao Special Administrative Region (hereinafter referred to as DSSOPT) issued a ban on the project to Resident A and his wife. Resident A then visited DSSOPT personally to find out the details of the ban. As he had not yet decided if he would have the illegal part removed, he asked a DSSOPT staff whether his and his wife's name would be published in the newspaper. The staff responded, verbally stating that their names would not be published.

Resident A later discovered that DSSOPT had published the "Final Notice" regarding Unit X in the newspaper, which contained both their names. Resident A subsequently filed a complaint with this Office (GPDP), claiming that the "Personal Data Protection Act" had been breached by DSSOPT. Resident A felt that since its staff had verbally agreed not to publish their names in the newspaper, he was dissatisfied that DSSOPT had allowed their names to be published in a newspaper without their consent.

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

DSSOPT explained that Resident A's illegal project had breached the terms of Article 8.12 of the Decree-Law No. 24/95/M, (the "Fire Safety Regulation"). As a result, in accordance with the regulations of Article 88.1 of the same Law, the project was banned and an order for its removal was issue.

As the final decision for the removal of the relevant illegal project and the evictions involved resident A, his wife, other third parties in the project and the trustees and owners of the works, DSSOPT consequently published a notice in a newspaper, in accordance with the provisions of Article 72.2 of the "Administrative Procedure Code". In addition, in order to allow Resident A and his wife to be informed of the content of the final decision, DSSOPT issued an official letter and handed it over to the wife of Resident A.

In GPDP's opinion, as the project breaching the "Fire Safety Regulation" had to be removed and was banned by DSSOPT, DSSOPT could process Resident A's

personal data within the purview of its powers granted to it by the "Fire Safety Regulation" as a public authority. As such, the personal data processing was carried out in accordance with the regulations of Article 6.(4) of the "Personal Data Protection Act". DSSOPT thus had legitimacy to process Resident A's personal data without his consent.

DSSOPT published the notice containing the names of Resident A and his wife within the newspapers in order to notify other unknown third parties or trustees in involved in the project. As DSSOPT was unable to obtain the specific contact details of the abovementioned people, it published the respective notice, in accordance with the terms of Article 72.2 of the "Administrative Procedure Code".

Suppose that there are unknown third parties involved in the project or trustees are simultaneously involved in other projects similar to Resident A's, if the names of the project owners had not been published, there would be no way to determine which illegal project needed to be removed. Therefore, and in accordance with the terms of Article 113.1.(c) and Article 70.(b) of the "Administrative Procedure Code", DSSOPT could publish the names of Resident A and his wife. This action was also carried out in observance of the principle of proportionality determined in Article 5 of the "Personal Data Protection Act".

With regards to Resident A's claim that DSSOPT's staff had verbally promised not to publish his and his wife's names in the newspaper, GPDP felt that it was an internal affair of DSSOPT and will take no further action in this matter.

In summary, GPDP believed that the publication of the respective notice by DSSOPT did not breach Articles 5 or 6 of the "Personal Data Protection Act".

Result

GPDP sent an official letter informing DSSOPT of the abovementioned assessment.

DSSOPT later replied and claimed that the matter had been handled internally.

Case 10

Banks might transfer and sell consumer data

Case Briefing

It was widely reported by Hong Kong and Macao media in August 2010 that six banks in Hong Kong had acknowledged transferring the personal data of their clients to third parties for marketing purposes in the last five years, and that five of them had even profited from this. This caught the attention of local residents, who wanted to know whether a similar situation was occurring in Macau and if so, whether this breached the "Personal Data Protection Act".

In view of this, this Office (GPDP) took the initiative and filed the case for investigation to find out whether local banks had transferred personal data of clients for marketing purposes.

Analysis and Conclusion

In accordance with the provisions in articles 4.1.(1) and 3.1 of the Personal Data Protection Act, the data processing involved in this case is within the scope of regulation by the said Act.

To better understand the respective issues, GPDP sent official letters through the Association of Banks to its member institutions, and sent letters directly to non-member banks.

GPDP also obtained information on the relevant situations through the Monetary Authority and other channels.

The banks replied to the GPDP, respectively, from August to November 2010. All of them denied that they had transferred personal data of their clients to third parties for marketing purposes and profit.

According to the information obtained from the Monetary authority, there was nothing indicating that local banks or Macao citizens were involved in this incident.

In summary, GPDP believed that there was nothing indicating that banks in Macao had transferred personal information of clients to third parties for marketing purposes.

Result

The case was closed.

Law Implementation

I. Following ups of applications

In 2010, applications for personal data processing received by the GPDP included: 361 notifications on personal data processing (49 of which concerned transfer of personal data outside Macao SAR and 312 notifications on other types of personal data processing), 28 applications for authorizations and 24 for opinions.

Figure 11 – Types of applications for personal data processing

	Number of cases	%
Notification	361	87.4
Application for authorization	28	6.8
Application for opinion	24	5.8

	Number of cases	%
Notification of transfer of personal data outside Macao SAR	49	13.6
Notification of other types of personal data processing	312	86.4

1. Opinions

In 2010, GPDP received a total of 24 applications for opinions from public and private institutions. Together with the 8 applications carried over from 2009, in 2010 GPDP processed 32 applications, 30 of which were concluded.

During 2010, 24 applications of opinions were received, 19 of them came from public institutions, 5 from private institutions or organizations. 20 applications (83.3%) involved the legitimacy or lawfulness of personal data processing.

Figure 12 – Increment of applications for opinions

Year	2007	2008	2009	2010
Number of applications	27	35	35	24

2. Authorisations

Of the 28 applications for authorization received by GPDP in 2010, 27 applications concerned personal data combination. Due to the fact that government agencies were asked to apply for their personal data combination, which were basically completed during 2008, therefore the number of applications for authorization became rather stable in 2009 and recorded a slight increase of 12% in 2010.

Taking into account the 104 applications carried over from 2009, in 2010 GPDP processed 132 applications of authorizations, of which 40 were concluded and 3 authorizations were issued. Some of the applications were concluded as closed cases as proved not involving personal data combination or authorizations of other sorts.

Figure 13 – Increment of authorization applications

Year	2007	2008	2009	2010
Number of applications	15	152	25	28

3. Notification of personal data processing received

In 2010, GPDP received a total of 361 notifications of personal data processing from public and private institutions (including 49 for transfer of personal data outside Macao SAR and 312 for other types of personal data processing); the total was roughly the same as that of 2009 (359 notifications). Taken with the 286 notifications (including 33 for transfer of personal data outside Macao SAR and 253 for other types of personal data processing) carried over from 2009, in 2010 GPDP handled 647 personal data processing notifications, of which 68 were concluded. In 2009 and 2010, GPDP implemented the registration for personal data processing in public services stage by stage and in multiple batches, requiring public services to complete registration for personal data processing within the designated time. Thus, the number of notifications received by GPDP increased sharply. GPDP was stepping up its scrutiny and coordination of the notifications.

Of the 49 notifications for transfer of personal data outside Macao SAR received in 2010, 24 were from public institutions, and 25 from private institutions. As to notifications regarding other types of personal data processing, 260 were from public institutions and 52 from private institutions.

Figure 14 –Increment of notifications of personal data processing

Year	2007	2008	2009	2010
Number of applications	68	216	359	361

II. Coordinating law implementation

1. Registration of personal data processing in public departments

In 2010, GPDP continued its effort in the personal data processing registrations, stage by stage and in multiple batches, for the public departments. To facilitate the advancement of the registration process, GPDP organized 2 follow-up seminars in late February, with a total of 285 department chiefs and officials in charge of the related work, from 76 departments or agencies, attended. In addition, GPDP separately organized working sessions for 10 public departments.

With the support and cooperation of various public services, the first stage of the registration last mentioned completed in the middle of the year as planned. Until July 31, GPDP received a total of 438 notifications from 68 public services (excluding the applications for authorizations and the notifications submitted by public departments before the start of the registration). The GPDP will expedite the scrutiny, coordination and registration for these applications.

2. Translation of international reference documents

As the PDPA has its legal origin of European laws and the EU has a lot for Macao to reference to, GPDP continued its work in 2010 to translate a number of international legal documents into Chinese or Portuguese. Translations as such have been uploaded to its official website. The general public can download those documents free of charge; completed works include:

1). *Opinion 1/2010 on the concepts of "controller" and "processor"* issued by the Article 29 Working Party of EU (Chinese translation).

2). *The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy*, adopted by the 31st International Conference of Data Protection and Privacy Commissioners (Chinese and Portuguese translation).

3. Development of guidelines

In response to the practical issues relating to the provision of information to data subjects during indirect collection of personal data reflected by various sectors of the society, GPDP released in August the guidelines *The Right to Information in the Indirect Collection of Personal Data*, as a guidance notes, for effective protection of personal data, to various sectors of the society for their understanding and implementation of the PDPA. At the same time, taking into account that personal data were increasingly published on the Internet, GPDP invested resources in the related researches, and in December 2010 completed *the Guidelines on Publication of Personal Data on the Internet*. That document was published in January 2011.

Connection, Cooperation and Publicity

I. International and regional connection

To establish better connection and cooperation for data protection with other countries and regions, GPDP attended several international forums and events during 2010. Connection and interaction with relevant data protection authorities have been achieved, along with sharing work experience and deepening regional cooperation.

1. Privacy Awareness Week 2010

The Privacy Awareness Week 2010, during 2nd to 8th May, 2009, was hosted by the Asia Pacific Privacy Authorities (APPA). The activities in 2010 focused on the promotion of privacy protection awareness among the elderly. The Office of the Privacy Commissioner for Personal Data, Hong Kong joined the members of the Asia Pacific Privacy Authorities (including Australia, Canada, Hong Kong and New Zealand) to develop an "online self-assessment system for personal data privacy awareness". Through this elderly people can evaluate whether their awareness of personal data protection was adequate. The efforts highlighted the importance of personal data protection, and provided some practical recommendations to elderly people.

As part of such efforts, GPDP, with the copyright permission of the Office of the Privacy Commissioner for Personal Data, Hong Kong, produced the Portuguese version of the mentioned self-assessment system for the Privacy Awareness Week of year 2010. After logging on GPDP's website, users could use the self-assessment system either stored on the Hong Kong Office of the Privacy Commissioner for Personal Data or the Portuguese and Chinese system found on GPDP's website.

2. The 33rd Asia Pacific Privacy Authorities Forum

GPDP, as an observer, participated in the 33rd Asia Pacific Privacy Authorities Forum, during June 3rd and 4th in Darwin, Australia. During the conference, the delegates briefed their work of the past six months, and exchanged views and shared experiences on a number of issues relating to personal data protection. The representatives of GPDP briefed the participants on Macao's new endeavors in the introduction of personal data processing registrations amongst the public departments, and shared its relevant experience. The conference also discussed the policies and conditions for the admission of new members.

3. The 34th Asia Pacific Privacy Authorities Forum

GPDP participated as an observer in the 34th Asia Pacific Privacy Authorities Forum, which was held between December 6th and 8th in Auckland, New Zealand. The meeting confirmed the admissions of the Federal Trade Commission, United States; the Federal Institute for Access to Information and Data Protection, Mexico; and the Office of the Information Commissioner, Queensland, Australia as new members. In addition to discussions about the recent situations of personal data protection in various jurisdictions and the plans for the Privacy Awareness Week of 2011, the meeting also touched upon issues such as the interactions between the national, regional regulatory authorities and multinational corporations, challenges posed by the development of science and technology, the latest international trends, the progress of cross-border cooperation and networking among data protection authorities, etc.

4. Roderick Woo, Privacy Commissioner for Personal Data of Hong Kong, visited the GPDP

Roderick Woo, Privacy Commissioner for Personal Data of Hong Kong, visited GPDP on February 5th, and made exchanges with the staff of GPDP. During the exchange, Mr. Woo analyzed some cases handled by the Hong Kong Commissioner Office, shared its valuable experience in personal data protection, and conducted extensive exchanges with the staff of GPDP. Mr. Woo's visit helped strengthen the co-operation between Hong Kong and Macao on personal data protection, and expanded the horizons of the staff of GPDP.

5. A visit to the Office of the Privacy Commissioner for Personal Data, Hong Kong

A team led by Coordinator Chan Hoi Fan visited the Office of the Privacy Commissioner for Personal Data, Hong Kong on July 29, receiving a warm reception by Commissioner Roderick Woo. Both sides presented their recent works and future plans, and exchanged views on issues related to Hong Kong and Macao.

6. A visit by representatives from the Korean Information Security Agency

The Korea Information Security Agency sent representatives to visit GPDP twice, in August and November respectively, receiving warm welcome by Yang Chongwei, Deputy Coordinator of GPDP. The Bureau of Telecommunications Regulation of Macao also sent representatives to participate the first meeting held by GPDP and the Korea Information Security Agency. During the talks, the two sides shared their experience in personal data protection, especially the cracking down on the unlawful disclosure of the ID numbers on the Internet. Specific cases as well as the feasibility of bilateral cooperation were discussed, and a preliminary consensus on the direction

of cooperation was reached.

7. Attending the quarterly meeting of the banking sector in Hong Kong and Macao on Visa risk management

GPDP was invited to attend the titled meeting, held on April 27th in Hong Kong, and explained to participants from the banking sector about the Personal Data Protection Act of Macao (PDPA) and data transfer between the two regions. Many participants came into contact with the PDPA for the first time. They got a first time understanding of the Macao legal provisions, which help their personal data processing in compliance with the laws.

II. Community relations

Representatives from four companies, including Transmac, visited GPDP on March 12th and held meetings with Coordinator Chan Hoi Fan. GPDP's representatives introduced the visitors the PDPA and answered their questions.

Representatives from the Macao Association of Banks and Monetary Authority (AMCM) visited GPDP on June 21, and held a meeting with GPDP's staff. During the meeting, staff of GPDP introduced the provisions of the PDPA, and encouraged the sector to establish its own code of practice that, through self-regulation, help ensure legitimate processing of personal data, in addition to introducing the current practices of other countries and regions. The two sides discussed the feasibility of implementing relevant mechanisms in the banking sector in Macao. Representatives from the Macao Association of Banks expressed that the Association basically agreed to promote personal data protection in the banking sector, and would begin the relevant researches and advocate progressive development of code of conduct in the sector.

On June 24th, a team led by Coordinator Chan Hoi Fan visited the Property Management Business Association Macao and Macao Property Management Professionals Association, receiving warm receptions from the leaders of the two associations. Lao Ngai Leong, chairman of the Property Management Business Association Macao, said that the sector emphasized the protection of personal data in their business, and elaborated on the difficulties and questions faced by the industry. The representatives of GPDP introduced the work of GPDP as well as the key elements of the PDPA, replied to the questions encountered by the sector in their practical works, and encouraged it to consider establishing its own code of conduct. The two sides agreed to jointly organize seminars to further promote protection of personal data in the sector.

On September 20th, a team led by Coordinator Chan Hoi Fan visited the Chinese Educators' Association of Macao, receiving a warm reception by the leader of the association Ho Sio Kam, Chairman of Administrative Board of the Association. The latter pointed out that protection of personal data was very important, and there were

many problems in the practical implementation of data protection in the education sector due to its nature. She expressed that further discussion could be initiated for implementing personal data protection in the education sector and the PDPA should be promoted. Coordinator Chan Hoi Fan gave a brief introduction of the GPDP, and looked forward to further cooperation between the Association and the GPDP, with a view to promote the PDPA in education sector and encourage it to establish its own code of conduct.

In addition, some institutions from the banking industry and the insurance industry visited GPDP on different occasions, expressing the importance they attached to personal data protection, and came up with certain recommendations and suggestions. In addition to presentation about its works, GPDP thanked the sectors for its attention on personal data protection, and provided recommendations on certain issues.

III. Publicity and promotion

In 2010, GPDP continued its work on publicity and promotion, which included several seminars, conferences and talks. On the lines of publicity the GPDP also organized promotional activities, media promotions, and produced publications, newsletters and annual reports, promotional materials, which were all aimed at promoting the PDPA through different channels to generate public awareness of personal data protection.

1. Seminars on the PDPA

Organizing seminars to promote the PDPA is one of GPDP's publicity priorities. GPDP continues to organize seminars on the PDPA with the public departments and private institutions in order to increase their understanding of this Law and make sure both institutions and citizens could effectively obey and enforce the act, which help to make sure data is protected during their daily works. In 2010, the GPDP organized 23 seminars with 17 institutions respectively, accounted for a total of 1041 participants.

Figure 15: Seminars on the *Personal Data Protection Act*

Year	2008	2009	2010
Number of participants	1339	1169	1041
Number of seminars	22	23	23

2. Conferences and seminars

1) Conference: *Protecting Your Customers' Data*

The conference on Protecting Your Customers' Data, hosted by GPDP and in collaboration with the Judiciary Police and the Payment Card Industry Organization in 2009, was highly praised. In order for businesses and banks in Macao to learn more about personal data protection and the respective safety standards, in 2010 the three institutions continued their cooperation in this area and hosted the conference Protecting Your Customers' Data, at the Macao World Trade Center on August 24th. More than two hundred participants from the organizing institutions, banks and enterprises attended the conference, discussing and communicating on issues such as requirements of PDPA, solutions to the issues, criminal cases of credit cards and data security and protection, etc.

2) Seminar: *The Perils and Promise of Data Privacy*

On the invitation of the British Chambers of Commerce (BCC), representatives of GPDP attended the seminar on The Perils and Promise of Data Privacy: Protecting Client Data, Ensuring HR Compliance, Leveraging IT Assets hosted by the BCC on May 26th. The representatives briefly introduced the functions of GPDP and the focus of the PDPA. Representatives of other institutions invited by BCC elaborated on the protection and management of customers' data, certification of data management system, etc. During the Q&A session, representatives of GPDP and other speakers answered questions from the audiences about the practical operations of personal data protection.

3) Training courses

1) Training course: Personal Data Protection Act and personnel data management

GPDP hosted a course on Personal Data Protection Act and personnel data management from April to May and September to October, respectively, in collaboration with the Macao Productivity and Technology Transfer Center. The course, mainly for employers and professionals of human resources management, was highly appreciated by the participants. In phase I and phase II of the course, four classes in total, a total of 100 students were recorded.

Apart from giving a systematic introduction of the PDPA, the course also discussed the common problems encountered in personal data processing of human resource management, such as employee recruitment, attendance management, monitoring of employee performance, employee data collection and retention, transfer of data outside Macao SAR, employee data processing in transnational company, etc. Examination was included in the course; altogether 87 students passed the examinations and reached the attendance standard, and were awarded certificates. 84% of the students considered that the course was good or very good, 84% agreed or strongly agreed that the objectives of the course were achieved, and 85% of the students agreed or strongly agreed that the contents of the course met their needs.

2) Training course: Personal Data Protection in Social Service Agencies

GPDP hosted the course of Personal Data Protection in Social Service Organizations from April to May, in collaboration with the Macao Productivity and Technology Transfer Center. The course was intended for staff of social service organizations. GPDP invited 20 staff members from four Macao social service organizations, including the Caritas Macao, Macao Federation of Trade Unions, the Women's General Association of Macao, and Union of Neighborhood Associations of Macao, to attend the course.

The course consisted of 3 parts: part I introducing the main contents of PDPA and the important issues of data protection faced by social service organizations; part

II focusing on information security, including setting passwords for computers, email security, internet security and etc. In part III, students visited the St. James' Settlement in Hong Kong and exchanged views. Based on the experiences from this course, GPDP will further optimize the course design, and continue to cooperate with the Macao Productivity and Technology Transfer Center in 2011, to launch a new course for professionals from social service organizations.

3) Training course: Knowing the ISO27001- 2005 Information Security Management System

In May, GPDP hosted a course on Knowing ISO27001- 2005 Information Security Management System, in collaboration with the Macao Productivity and Technology Transfer Center. The course was for the staff of GPDP and staff in the public services. It lasted for 2 days, introducing information security and risk management, management system architecture, the requirements of ISO27001-2005 certification, qualifications for certification, etc.

4) 2010 Refresher Course for Police Officers

On the invitation of Public Security Police Force (PSP), GPDP's staff introduced Personal Data Protection Act for its 2010 Police Officers Course, held between June and August. 38 classes of 1330 police officers attended the three months' course.

4. Publicity and promotion

1) *IT Week 2010*

GPDP took part in the IT Week 2010 held at the Tap Seac Multisport Pavilion, during 26th and 28th November. The event was well received, during which GPDP promoted to the citizens the personal data protection through funny games.

2) Publicity through theme banner

For the publicity under the theme of "personal data is important, awareness of protection is indispensable", banners were put up on the main streets of Macao, in order to enhance the awareness of personal data protection amongst citizens. Publicity slogans included: learn more about privacy policy before signing a contract; think more and see more to protect personal data; do not upload personal data to Internet without considering online risks; leaking personal data induces serious consequence; use IT technology with caution and take safety measures; laws governed the right to object, say no to direct marketing.

5. Publicity through media

1) *Privacy & You*

In 2010, GPDP continued publishing the newspaper column *Privacy & You* in Chinese and Portuguese newspapers in Macao. Case analyses were given to raise the awareness of privacy protection. Afterwards these column articles will be translated into English and published in local English newspapers.

2) Promotional video and audio clips

For the publicity under the theme of "personal data is important, awareness of protection is indispensable", GPDP produced 6 video clips and audio tapes to raise public awareness of personal data protection. The video clips and audio tapes will be broadcasted in the local TV and radio stations in 2011, and they are also available on GPDP's website. Moreover, they will be showcased in activities hosted by GPDP, in order to promote data protection in a more understandable way.

6. Journals and leaflets

1) *The GPDP Newsletter* (seasonal journal)

GPDP continued to publish its seasonal journal – the GPDP Newsletter – in printed and electronic versions, delivering timely information on personal data protection to citizens in various forms.

2) *Annual Report 2009*

Annual Report 2009 summarized GPDP's law implementation, including handling legal enquiries, case investigations, supervision and coordination in the implementation of the law, as well as system building. 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 Personal Data Protection Act, the report also published some of the opinions and authorizations issued during 2009.

3) Tips on Personal Data Protection Leaflets

To complement the publicity under the theme of "personal data is important, awareness of protection is indispensable", GPDP produced the leaflets entitled Tips on Personal Data Protection, which disseminating information about self-protection of personal data.

4) Publicity materials

To generate publicity in communities, GPDP continued to create different publicity materials during 2010.

Table: Publicity items prepared by the GPDP

Items	Quantity
2011 desk calendars	2,000
Re-usable bags	5,000
Umbrellas	1,000
Portable electric fans	4,000
Sun hats	3,000
Notepads	5,000
Environmental protection tableware	2,000
USB memory sticks	1,000
A4 plastic envelopes	5,000
CD covers	500

IV. Website

As website is an effective communication channel with the public, the GPDP will continue update its official website in order to publish the most updated news for the needs of the public. During 2010, more than 60,000 visits to its website were recorded.