

Office for Personal Data Protection

Annual Report 2008

Unofficial English Translation

Disclaimer

This is an unofficial English translation of some major chapters in the Annual Report 2008 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.gmdp.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, 2009

Preface

It is two years since the founding of the Office for Personal Data Protection. In 2008, we steadily pushed forward several schemes of personal data protection in terms of public-awareness enhancement, supervision and coordination, policy-making, and complaint processing, which may be summarised as follows:

1. Building law implementation regime

Carrying on from what we achieved in 2007, we continued to issue four more Exemption Authorisations, a step forward in phasing-in the personal data processing registration regime.

Another work of far-reaching significance was the launch of compulsory personal data processing registration regime, with the support from the MSAR government. In this regard, Macao may well have been in the forefront in Asia. We initiated the registration regime in all levels of government agencies, with a view to setting a good example of respecting and implementing personal data protection on the part of the government agencies. When conditions for this work become right, we will institutionalise this regime to all entities that process personal data.

With regard to the increasingly popular use of biometric attendance systems, we published *Issues Relating to Using Fingerprint / Hand Geometry Devices to Check on Work Attendance*, aiming at guiding employers in legal and appropriate use of the technologies with due respect to their staff's personal data, and on the other hand, familiarising the employees with their rights and protection they are entitled to.

2. Advancement in daily operation

Viewed from a perspective of personal data protection, our work is just beginning to take off, with many aspects needing enhancement and substantiation. However, we notice to our delight that, on their own initiatives, many local institutions and associations have turned to this Office and asked us to help run briefing sessions and hold consultation on their operational procedures, as well as their formulating their personal data protection rules. There has been significant increase in the number of individuals seeking consultation or reporting suspicious cases. The number of cases processed by the Office also multiplied. It is safe to say that in varying degrees there is a growing sense of personal data protection among local institutions, associations and citizens.

For personal data processing institutions, it is import to have personal data protection policies in compliance with the law. Policy-making has two objectives: to bring the institutions' practice of personal data collection and processing in line with the provisions of law; and to offer a clear guide for staff to distinguish between responsibilities of their own and that of the employer.

Meanwhile, people are increasingly alert to personal data abuses. When they find their personal data processed in a suspicious manner, they will consult or lodge complaints with us. There were even cases where outsiders went to great lengths to help those whose personal data was improperly processed. A good example is the complaint we received against the employment agencies' mishandling of personal data of job seekers. Based on field findings and citizens' reports, we undertook to rectify the mal-practice of the employment agency, and issued *Guidelines on Employment Agencies Handling Customer Personal Data*, to complement our publicity sessions and patrols, which effectively protected the job seekers' personal data from abuse.

3. International exchange and cooperation

With the acceleration of the globalisation process, Macao's connections with international communities have reached a point where they became indispensable. Tackling an international issue such as personal data protection requires that we know about the international trend of privacy protection, and be involved in the endeavours of related international organisations, which turn out to be a route of course to our international accommodation and self-perfection.

In 2008, we attended as observers the 29th Asia Pacific Privacy Authorities (APPA) Forum as well as the 30th International Data Protection and Privacy Commissioners Conference; thereby we established our connections with some of our counterparts in other parts of the world. While introducing Macao to them and sharing our views with them, we also learned a lot from their experience and lessons.

We are convinced that cooperation and sharing will enable us to speed up and better implement personal data protection in Macao, and enable Macao to build up a positive image in this regard, and thereby give impetus to Macao's progress on other fronts.

The year 2008 was significant to us in that we not only initiated effective and efficient work on several fronts, but also successfully knocked open the door to international exchange and cooperation. More importantly, we phased in the regime of compulsory personal data processing registration in all seriousness, taking a substantial step towards institutionalisation of personal data protection in Macao. It is our expectation that by the combined effort of staff of this Office, and with the support, care and attention from the community, Macao will be able to scale higher in personal data protection.

Chan Hoi Fan

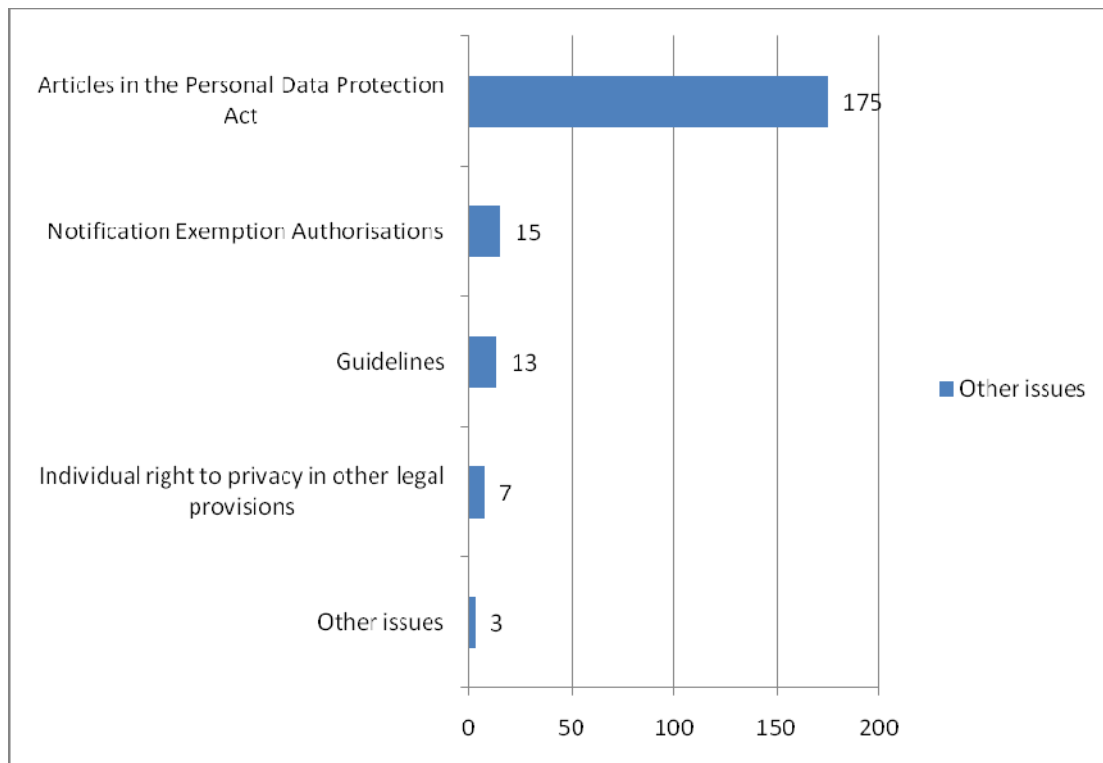
Coordinator

Processing of Enquiries and Complaints

I. Enquiries about law

In 2008, the Office received 207 enquiries about personal data protection (excluding those about work procedures), of which 206 cases were settled. As our services roll out gradually, the number of enquiries coming our way were much higher than the 43 in 2007; of those 82.16% were about articles in the *Personal Data Protection Act*, 93.24% made via phone call. The types of enquirers are rather evenly distributed, with government agencies, private institutions and individuals each accounting for about one thirds.

Fig. 1 – Enquiries sorted by nature and content



Note: Some enquiries were about more than one issue.

Fig 2 – Media of enquiry

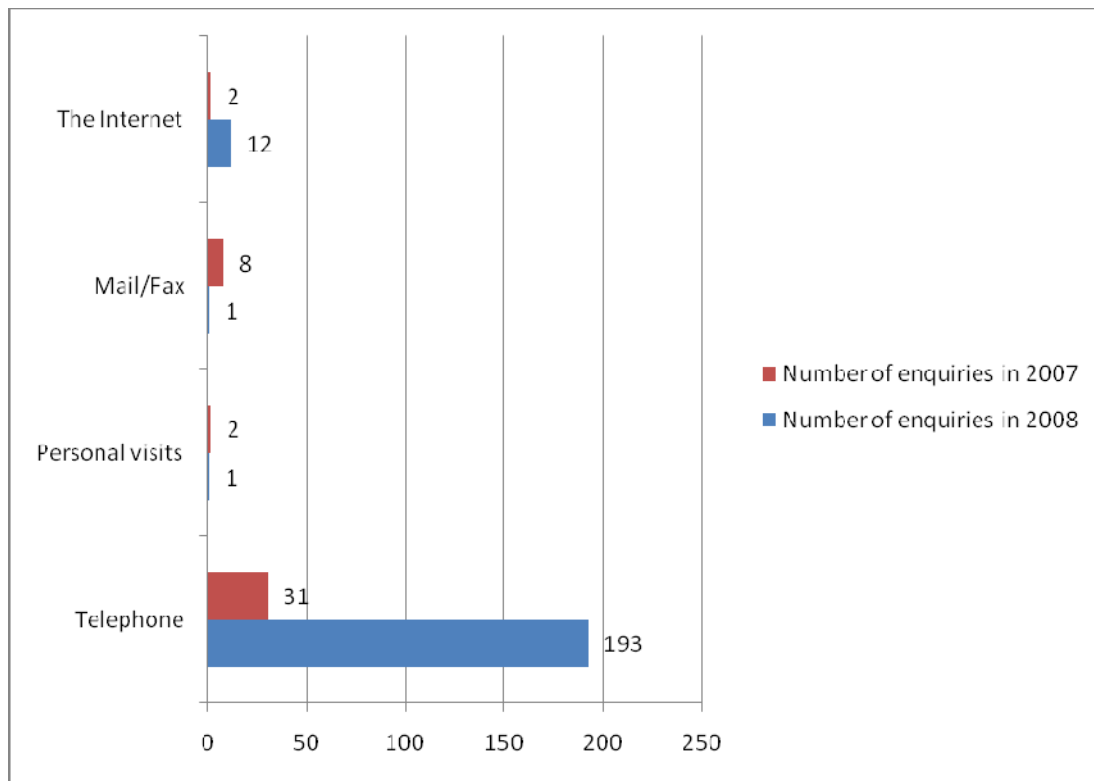
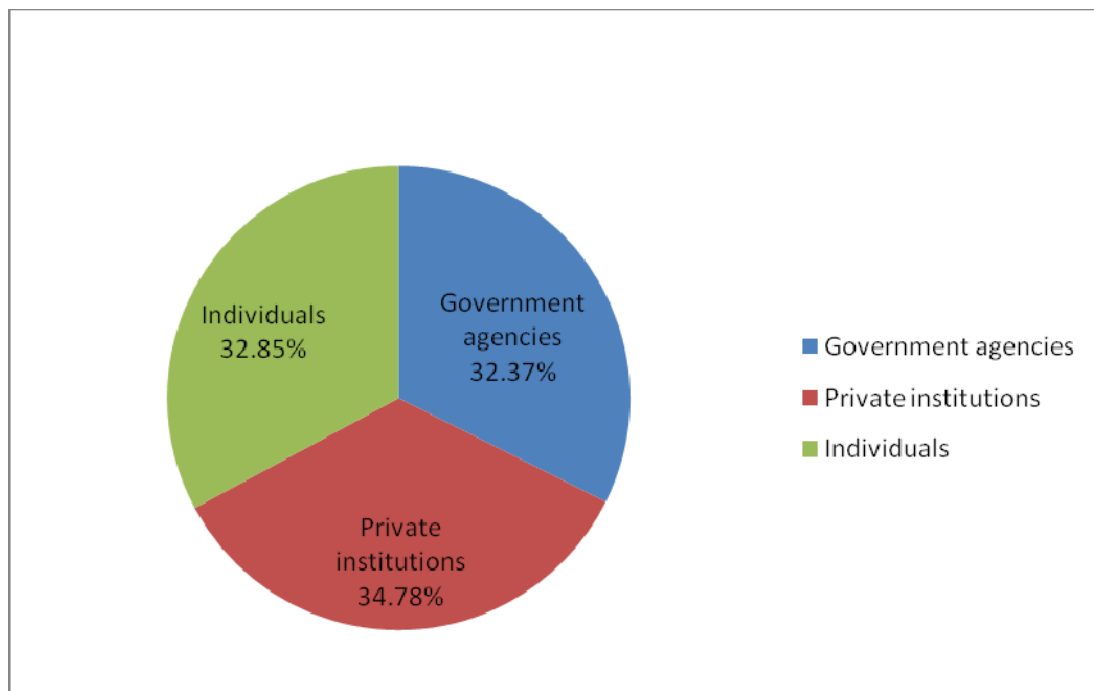


Fig. 3 – Categories of enquirers



II. Case investigation

In 2008, the Office initiated 35 cases for investigation, 59.09% more than that of 2007 (22 cases). With one case carried over from 2007, the Office processed 36 investigation cases, and concluded 25 of them. Of the cases initiated for investigation in 2008, 37.14% involved lack of legitimacy in data processing; 28.57% found in breach of the principles of personal data processing. 57.14% of investigations were initiated after the receipt of the related complaints. The parties investigated were mostly private institutions, accounting for 65% of the total. 31.43% of the cases investigated were found truthfully reported.

Fig. 4 – Investigated cases sorted by nature

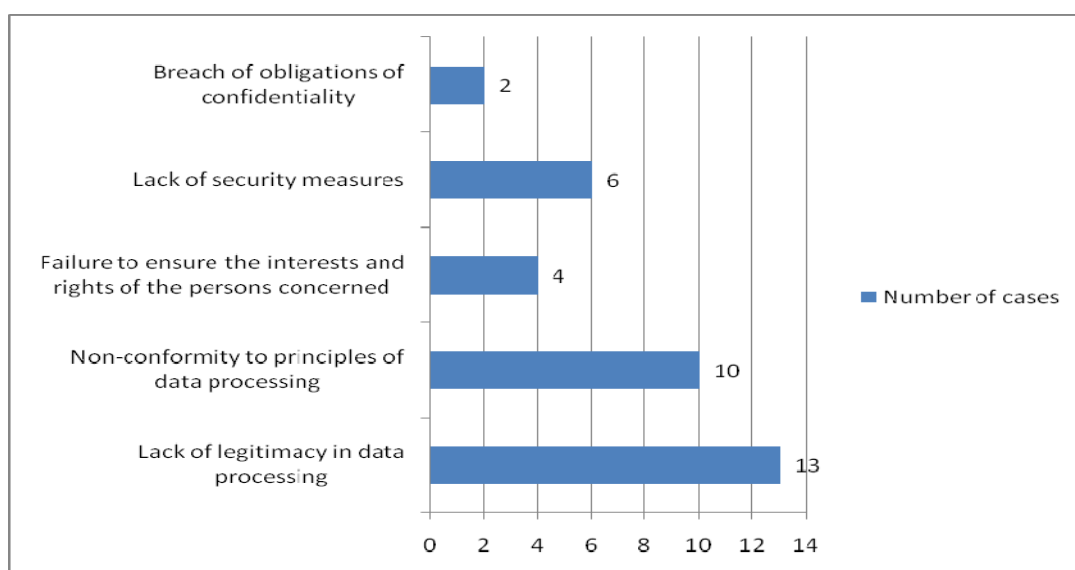


Fig. 5 – Investigated cases sorted by ways of initiation

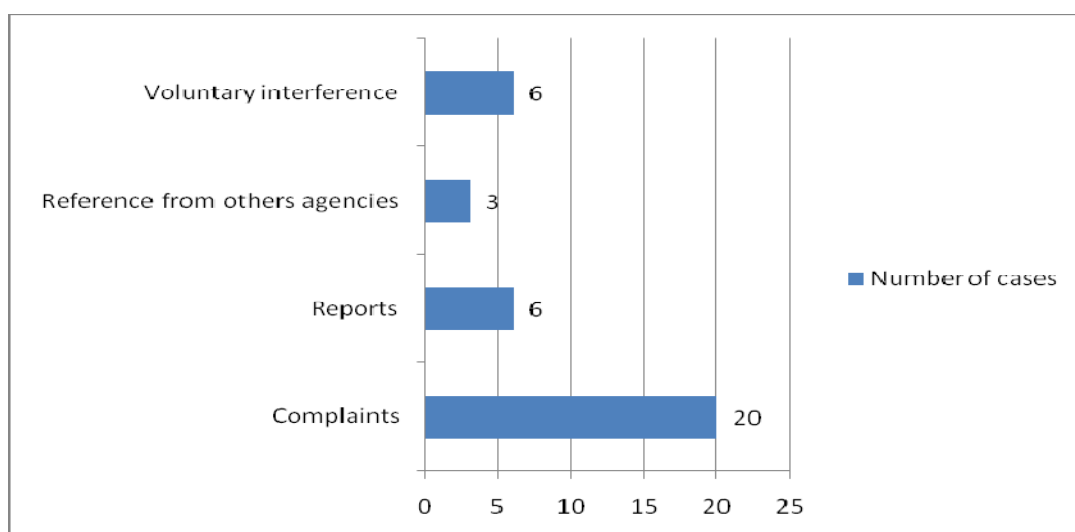
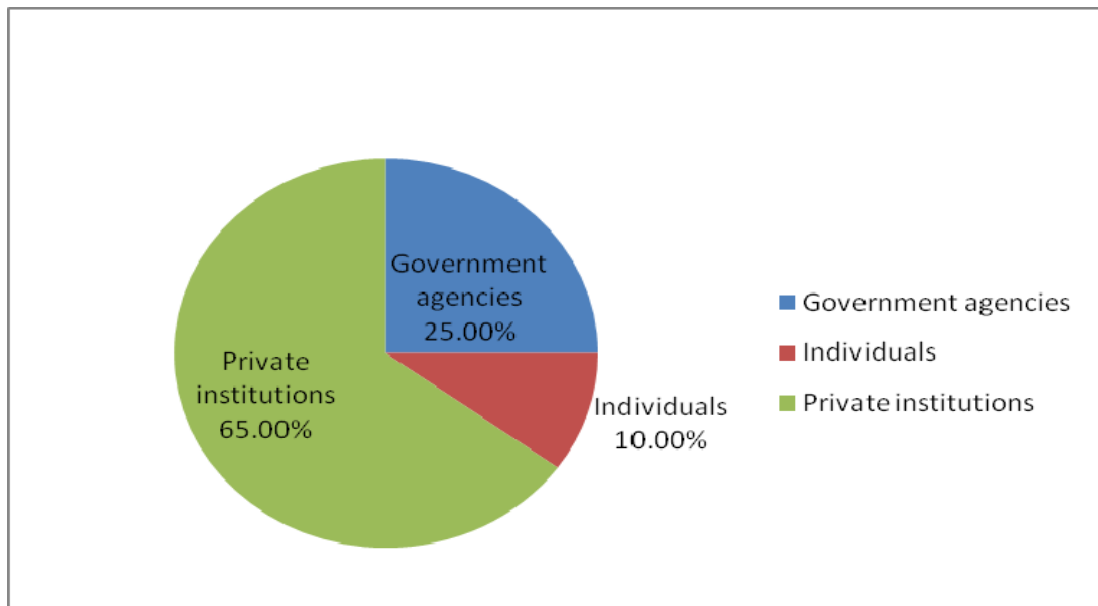
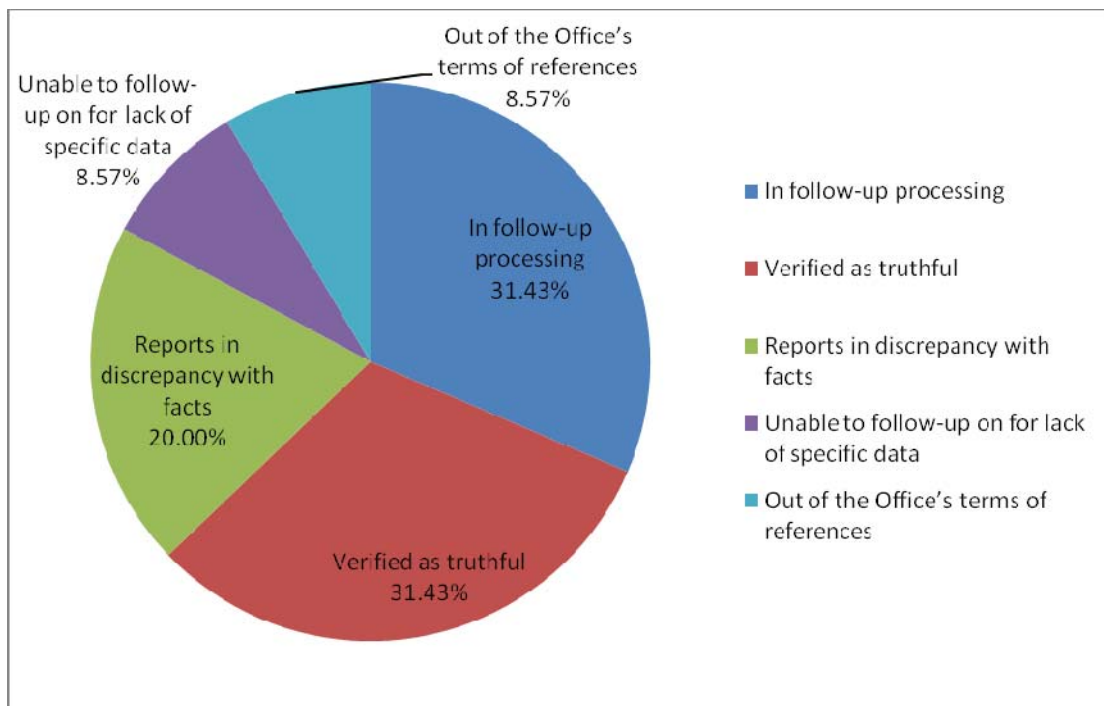


Fig. 6 – Categories of investigated parties



Note: Some of the cases involved more than one parties investigated

Fig. 7 – Results of investigation



III. Summary of selected cases

The following is the summary of some selected cases.

Case 1

Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. (No. 1 of Article 5 of the *Personal Data Protection Act*)

Complaint and investigation

An institution started using an ID checking mechanism on visitors, requiring not only that they show their ID document, register their names, ID card numbers and phone numbers, but also that they exchange their ID documents (such as Staff Card, Driver's License or Credit Card, etc., with photos attached) for internal Passes. The institution returned the ID documents to their owners upon their returning the passes.

According to the institution, this practice was adopted for security reasons. Taking the visitor's ID documents as collateral was so that visitors return the internal passes to the institution.

Conclusion

According to Article 6 of the *Personal Data Protection Act*, the institution may, for security reasons, legally demand the checking of visitors' ID documents, taking notes of their names, ID card numbers and contact phone numbers, provided that the visitors explicitly agree to this measure. If the visitors refuse to oblige, the institution has the right, for security reasons, to deny access to the visitors.

This Office holds that the institution's practice of taking visitor's original ID documents (that have the holder's photo on them) as collaterals of the internal passes, however, constituted a breach of the principle of reasonability provided for in Article 5 of the same Act. The measure went beyond what security calls for, and constituted over-collecting personal data. For one thing, by checking the original ID document that bears a visitor's personal data, it should suffice for the institution to verify a visitor's identity. Should any visitor damage or lose the pass accidentally or for whatever reasons, the institution could invalidate the pass at any time, without jeopardising its security. There was no need to keep a visitor's ID document as collateral. For another, the institution could recover any loss of passes via other legal channels. Keeping a visitor's ID document as collateral was by itself a deviation from the purpose of processing personal data, which is institutional security.

At the advisory of this Office, the institution has terminated its practice of keeping any document of visitors as collateral for internal passes, and has amended its ID checking procedures and related public notices. It has also made sure that its rules comply with the provisions of Article 10 of the *Personal Data Protection Act*.

Case 2

The data subject has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of commercial research. (No. 2 of Article 12 of the *Personal Data Protection Act*).

Complaint and investigation

An institution started making phone calls to a customer, in an attempt to sell its services or goods, and continued to do so after the customer demanded that it stop this practice. The institution continued making calls to the customer and sending promotional messages to the customer's mobile phone.

Conclusion

No. 2 of Article 12 of the *Personal Data Protection Act* provides that “*The data subject also has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of commercial research, or to be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object free of charge to such disclosure or uses.*”

The customer concerned demanded that the institution stop making sales calls to his or her phone, which is in effect exercise of his or her legal right to object. The institution, on the other hand, kept using the customer's phone as a selling tool, which constituted non-compliance with No. 2 of Article 12 of the Act, even though it did not amount to an administrative offence. This Office therefore ordered the institution to immediately stop making sales calls to customers who have exercised their right to objection.

Case 3

The data controller has the obligation to safeguard the right to information of the data subject whose data it collects directly or indirectly (Article 10 of the *Personal Data Protection Act*).

Complaint and investigation

Agency A ran a training course in conjunction with institution B; A took care of student recruiting, and then passed the students' data such as names and contact phone numbers, etc., to B. B disclosed the data on its notice board.

According to B, the above-mentioned practice was adopted to enable the teachers to contact the students at the beginning of the course, as well as for the students to know and confirm their class assignment and related matters.

Conclusion

Agency A collected students' personal data and passed the data to institution B for processing, therefore they are both regarded, according to No. 1 (5) of Article 4 of the *Personal Data Protection Act*, as data controller.

While institution B may have posted the students' personal data on its notice board to facilitate the teachers contacting their students, this Office thinks that the same purpose could well be achieved by other means. One way would be to provide the students' contact numbers to the teachers, and inform the students of their teachers' contact numbers when giving enrolment notices via phone, so the students could contact their teachers if necessary. There was no need to disclose the students' contact information to the public. Given that institution B had already given verbal notice to the students about their enrolment, it would suffice to indicate their names and classes to which they belong on the class schedules; there was no need to disclose more personal data than necessary.

The manner in which institution B disclosed students' personal data did not comply with the principles of adequacy and proportionality provided for by law. Therefore, this Office demanded that the institution stop its practice of posting students' names and contact numbers on its notice board. If it was necessary to notify the students of class allotment and schedules, the disclosed data could include students' names (or student number), without disclosing their contact numbers or other personal data at the same time.

To protect the right to information of the data subject, this Office also suggested that A and B prepare their own personal data collection statement, and attach it to the application forms or rules of enrolment, so as to ensure that the data subject become aware of such information.

Case 4

Personal data may be processed only if the data subject has unambiguously given his consent, except where the laws provide otherwise (Article 6 of the *Personal Data Protection Act*).

Complaint and investigation

In response to reports, the Office made investigative visits to all business premises of employment agencies in Macao. We found some of agencies had indeed posted job seekers' personal data on the windows or outdoors. The data disclosed generally included job seekers' photo, name, nationality, age, marital status, religion, education, work experience, document number, among other things.

Conclusion

The data concerned here were that of identifiable persons. According to Article 3 and No. 1 (1) of Article 4 of the *Personal Data Protection Act*, such data are protected by law. Article 7 of the Act provides that religion is sensitive personal data by nature, and may only be processed in the circumstances specified by law, with special security measures taken.

This Office holds that, given explicit consent of the persons whose data are concerned, an employment agency may disclose job seekers' data to a reasonable extent. However, the agency must make sure that the data are what job seeking and labour sourcing require. Under normal circumstances, disclosure of data directly relevant to employment purposes should suffice, and there is no need to disclose more personal data than necessary. Otherwise, the agencies may risk violating Article 5 of the same law about the principles of adequacy and proportionality.

According to the *Guidelines on Employment Agencies Handling Customer Personal Data* issued by this Office, in order to adhere to the principles of adequacy and non-discrimination, and ensure the safety of the data, one may not disclose the following data to the public: ID number or travel document number, nationality, origin, birth place, birth date, contact details, certificate of criminal record, and other sensitive data (i.e. political beliefs, political society or trade union membership, religion, privacy, racial and ethnic origin and data concerning health or sex life).

As the result of this Office's advice, the employment agencies involved have all terminated their practice of disclosing job seekers' personal data that should not be disclosed. They are urged to strictly abide by the law and take care in dealing with the related matters.

Case 5

Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. (No. 1 of Article 5 of the *Personal Data Protection Act*)

Complaint and investigation

Macao Daily News Readers' Charity Fund (hereinafter referred to as the Fund) disclosed in the paper the personal data of the Fund's beneficiaries, including name, gender, age, place of residence, the disease and difficulties they had.

The Office found that the Fund had obtained the consent of the persons whose data were concerned before processing their personal data. The purpose of disclosing the beneficiaries' data in the newspaper was to inform the public of how the fund had been used, so the public might have oversight on the use of the Fund.

Conclusion

By disclosing in the newspaper some non-specific data (except for the names) of the Fund's beneficiaries, as well as why the beneficiaries had been subsidised (brief description of the situation in which they found themselves), it was intended to allow the public to know about the use of the fund. The Office thinks that this data use did not deviate from the fund's legal purposes related to handling subsidy applications. The purposes were legitimate and appropriate. The data disclosed did not involve ID document numbers and specific addresses of the persons concerned, nor did it involve over-disclosure. This practice allowed the public to supervise the fund use, with a view to protecting the privacy of the persons whose data were concerned. Therefore, this Office holds that the abovementioned disclosure of data by the Fund was appropriate and proportionate in scope, and as such complies with the principles of personal data processing provided for in Articles 2 and 5 of the *Personal Data Protection Act*.

When applying to the Fund for financial aid, the applicants voluntarily provided their personal data required by the Charity Fund Aid Application Form, which included such sensitive data as the applicant's or their family members' health status. Those applicants were well aware that subsidy beneficiaries' cases would be disclosed via mass media, and if they objected the disclosure, they would not qualify for the subsidy. In other words, the Fund's collection of data of the applicants and their families was in line with Articles 6 and 7 of the *Personal Data Protection Act*, and it had legitimacy in doing so. However, the Fund could not prove that it had duly obtained the consent of the persons whose data were concerned regarding the media disclosure, and had to rely on the fact that the persons concerned had raised no objection, to infer that they were in tacit agreement with the disclosure procedures. This Office holds that this inference was flawed. The Fund should comply with conditions on which legitimacy of data processing depends as provided in Article 6 of

the same law.

The Office also found while following-up on the case that the Fund failed to ensure its applicants' right to information when collecting their personal data using the Charity Fund Aid Application Form.

With the advisory from this Office, the Fund has rectified its practice by measures such as having the applicants sign the relevant document of consent when obtaining their personal data, to ensure their explicit agreement. The Fund has also attached its personal data collection statement to its Charity Aid Fund Application Form, to discharge its duty of providing relevant information to the persons concerned.

Case 6

Personal data must be collected for specified, explicit, legitimate purposes and for purposes directly related to the activity of the controller; and not further processed in a way incompatible with those purposes. (No. 1 of Article 5 of the *Personal Data Protection Act*)

Complaint and investigation

Construction site management company A's proxy company B took some pictures on the sites, which included image data of the workers on site. A dispute over the picture-taking arose because B's cameramen did not explain why they were taking the pictures.

It was later explained that the picture-taking on the construction site was about taking pictorial notes of the operation and progress of the engineering project, and the pictures taken would only be used as internal record.

Conclusion

Judging by (5) of Article 6 of the *Personal Data Protection Act*, it is appropriate for company A to take pictures on its construction site for oversight purposes and to ensure the legal rights and interests of the institution concerned, without obtaining the consent of the data subject (the workers or other people on site). Given that company B was working on behalf of company A, so by the same reasoning, it was also appropriate for company B to take pictures on the site, without the need of obtaining consent of those present.

While company B might take the pictures of the on-site according to company A's managerial requirement, it also processed the photos that contained the image data of the data subject, and only passed those photos to company A when needed. Therefore the Office regards company B as the data controller too. According to Articles 10 and 11 of the *Personal Data Protection Act*, before taking the pictures, companies A and B should have told the data subject about how their personal data might be collected and handled. Company B had the duty to respect the data subject's right to information and right of access, and when taking pictures that would involve personal image data, especially when questioned, to explain the purposes and uses to which the pictures would be put. It was exactly company B's failure to tell the workers on site about the purposes and uses of the photos that gave rise to the ensuing dispute.

The Office therefore demanded that the said companies amend their practice in the following ways – company A may well post notices on eye-catching places in the site, clearly indicating the purposes and uses of pictures taken on site. For example, its notice should state “taking on-site pictures by the management company or the project undertaker company is what the on-site project oversight and operation require; and

the pictures taken will be used for general internal record purposes”, to ensure the right to information of the data subject. Company A was required to advise company B and other related companies that, when taking on-site pictures and if the data subject question, B’s staff should identify themselves and the photo-taking company, and explain the purpose and uses of the photos taken.

Case 7

Personal data must be collected for specified, explicit, legitimate purposes and for purposes directly related to the activity of the controller; and not further processed in a way incompatible with those purposes. (No. 1 of Article 5 of the *Personal Data Protection Act*)

Complaint and investigation

For security reasons, a shop installed and ran a surveillance system on its business premises, and took some pictures of some customers committing shoplifting on the premises. However, the shop did not report the findings and evidences to the police; rather, it made use of such image data in its posters displayed to the public. In those posters, the images of the suspects were clear enough to identify the suspects.

Conclusion

According to No. 1 (1) of Article 4 and Article 3 of the *Personal Data Protection Act*, personal images are personal data protected and regulated by the Act. The shop that ran a surveillance system on its business premises in an attempt to protect its legal rights and interests had a legal purpose according to Article 6 of the Act, and it is therefore appropriate for the shop to process the image data thus obtained.

However, the shop took the liberty of disclosing the image data of those suspected of shoplifting, which constituted processing the suspects' data of criminal deeds, which in turn deviated from the security purposes of collecting the data, and failed to comply with Article 5 of the *Personal Data Protection Act*. It was also evidence of failure to comply with Article 8 of the same Act, according to which it is illegal for the shop to process data of anyone committing criminal deeds in such a manner. Such data must be handed over to a competent law-enforcing department for investigation.

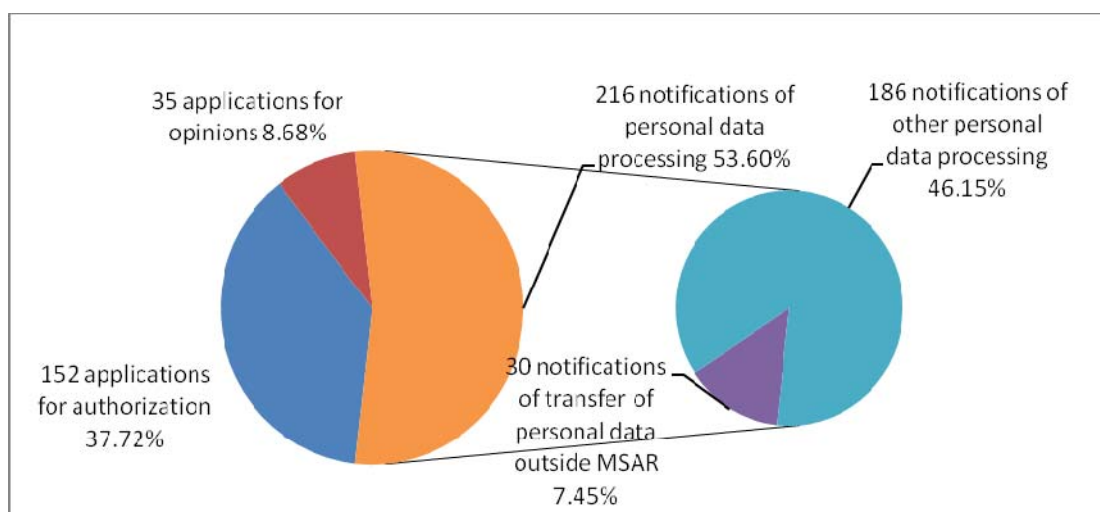
This Office thinks that the shop's practice of displaying suspects' data constituted a deviation from the purposes for which the data had been collected in the first place, and the shop may have violated the *Personal Data Protection Act*. The Office therefore demanded that the shop stop posting and destroy the posters and related notices containing image data of the suspected shoplifters. The Office has also informed the shop that, if it had kept a database of the suspect shoplifters' data, it should stop the practice, hand it over to the police for investigation or destroy it.

Law implementation

I. Supervising law implementation

The applications about personal data processing submitted to this Office in 2008 included 216 notifications of personal data processing (of which 30 were notification of transfer of personal data outside the MSAR, and 186 notifications of other personal data processing), 152 applications for authorization and 35 for opinions. The applicants included government agencies, financial and commercial institutions, among others.

Fig. 9 – Types of applications for personal data processing



1. Opinions

In 2008, the Office received 35 applications for opinion from government agencies and private institutions, a rise of 29.63% over that of 2007 (27 applications). Taking the three applications carried over from 2007 into account, the Office handled 38 applications for opinions, of which 33 were concluded.

The 35 applications for opinions received in 2008 were from 25 institutions, including 15 government agencies and 10 private institutions or associations. Of those applications, about 44% concerned the issue of appropriateness or legitimacy of personal data processing. Ranking the second were applications for opinions concerning “personal data combination (inter-connection)” and those by institutional applicants on “Forms supporting the collection of personal data” and “Personal Data Collection Statement”, accounting for about 26% and 21% respectively. Apart from that, there have also been applications for opinions from institutions on methods of personal data processing, transfer of personal data outside the MSAR and data retention period, among other things.

2. Authorization

The Office received 152 applications for authorization in 2008, of which 151 were for personal data combination (inter-connection) and one for other operation, more than 9 times of the 15 received in 2007. Taken together with the 14 applications carried over from 2007 the Office actually processed 166 applications for authorization, of which 49 were concluded, with 18 authorizations issued. Some of the concluded applications were identified as unrelated to “personal data combination (inter-connection)”, and as such did not need authorization.

The Office issued a circular on 24th Nov 2007 to all government agencies requiring them to seek authorization in compliance with law for “personal data combination (inter-connection)” operations. As a result, 90.79% of the applications received, 138 in total, were from government agencies; those from private institutions accounted for 14, most of which were from banks.

3. Notifications of personal data processing

In 2008, the Office received 216 personal data processing notifications from government agencies and private institutions, of which 30 concerned transfer of personal data outside the MSAR, 186 about other modes of personal data processing. In comparison with the 68 notifications received in 2007, it was a rise of more than two times. Taking into account the 49 notifications carried over from 2007 (including three that concerned transfer of personal data outside the MSAR and 46 in respect of other personal data processing operation), this Office processed 265 notifications of personal data processing, and concluded 203 of them.

Of the 30 notifications received concerning transfer of personal data outside the

MSAR in 2008, 3 were applied by government agencies, the remainder 27 were by private institutions. As to notifications concerning other personal data operation, there were 143 by government agencies and 43 by private institutions.

II. Coordinating law implementation

1. Registration of personal data processing

Pursuant to Article 21 of the Personal Data Protection Act, and approved by the Chief Executive, the Office started from the second half of 2008 to phase in the statutory regime of personal data processing registration in government agencies. The registration began with the agencies and departments directly under the Chief Executive and the Secretary for Administration and Justice. As a prelude to it, the Office held a briefing session on 9th Dec 2008, attended by 38 Chiefs, Directors and staffs of the agencies concerned.

The phasing-in of the personal data processing registration regime among government agencies has received support from the agencies all along, and will reach further in 2009.

2. Alerting government agencies to potential hazards to personal data

In view of the recent raft of incidents in neighbouring areas where personal data was mishandled and disclosed, the Office issued an internal circular to government agencies in May 2008, urging them to take effective measures to ensure the security and confidentiality of personal data being processed. Recommended measures included formulating proper security schemes and guidelines, adopting proper approach to managing data media, as well as refreshing the staff's sense of legal obligations, among others.

3. Translating the EU reference documents

Personal data and privacy protection is a concept deeply rooted in the legal frameworks in Europe. The EU has a lot to offer in this regard, and can well serve as a benchmark for Macao. Therefore, the Office has selected some of EU's documents and translated them into Chinese for the reference of all sectors of the community.

How to protect children's personal data has become an unavoidable issue in a modern society. There is a growing desire in Macao's government agencies, schools and social service institutions to be better informed about personal data protection. Therefore, the Office chose to translate *Working Document 1/2008 on the Protection of Children's Personal Data* drafted by Article 29 Data Protection Working Party, and delivered the translation to government agencies for reference and uploaded it to the Office's website for citizens to download.

III. Regime building

1. Guidelines

In 2007, the Office issued the *Principles of Personal Data/Privacy Protection in Workplaces: Guidelines on Employee Monitoring*, to orient employers towards legal approaches to personal data handling. We achieved good results in preventing employees' personal data from being abused. In 2008, the Office continued to focus on issues widely concerned about by the public and formulated two guidelines - *Guidelines on Employment Agencies Handling Customer Personal Data* and *Issues Relating to Using Fingerprint / Hand Geometry Devices to Check on Work Attendance* – so that sectors of the community may formulate their own policies of personal data processing in ways that effectively protect personal data.

- *Guidelines on Employment Agencies Handling Customer Personal Data*

In 2008, the Office received many complaints concerning employment agencies mishandling of personal data, into which the Office launched immediate investigation. Our officers also made investigative visits to those agencies in all the districts. We found that there was indeed breach of the *Personal Data Protection Act*, mainly in employment agencies' mishandling of sensitive data of job seekers, and subjecting such data to over-exposure, to the detriment of the persons concerned. In order to correct those illicit trade practices, the Office issued on 3rd July 2008 *Guidelines on Employment Agencies Handling Customer Personal Data*, requiring explicitly that all employment agencies strictly abide by the law, and rectify that mal-practice within a designated period of time.

When the Guidelines were ready, the Office sent copies to all the employment agencies across Macao, and hosted in conjunction with the Labour Affairs Bureau two presentation sessions attended by 56 representatives of 44 employment agencies. We made in-depth introduction to the audience about the Guidelines and related provisions of the *Personal Data Protection Act*, in order that people get familiarised with the law, abide by it and, better still, take the initiative in formulating their own policies on personal data processing in line with the law and correct any law-breaching practice on their own.

The Office also sent officers in field visits to ensure that at the expiration of the period of rectification stipulated in the Guidelines, the complained malpractice had been corrected.

- *Issues Relating to Using Fingerprint / Hand Geometry Devices to Check on Work Attendance*

In the second half of 2008, the Office received several enquiries, asking whether it is legal for employers to use fingerprint or hand geometry attendance systems to log employee attendance.

In response to those queries, the Office first made a general study of the various existing systems and devices that employ biometric technologies for attendance logging and access control. We sorted out the type of personal data those systems collected and the effect of it on the persons whose data was concerned, and whether the related processing is in line with the provisions of the *Personal Data Protection Act*. As a result, we formulated and issued in December 2008 the *Issues Relating to Using Fingerprint / Hand Geometry Devices to Check on Work Attendance*. In the opinion of the Office, for attendance logging purposes, the biometric data collected should be limited to fingerprints or hand geometry (such as the shape of the palm, its infrared light features, etc.), if there is no other special purposes to serve, and should not include facial, voice, iris and other bio-features. The employer should pay attention to some specific details in using such equipment, and formulate their policies on personal data handling and notify this Office of such information.

2. Exemption authorisations

In addition to the three exemption authorisations issued in 2007, the Office managed to issue four more in 2008, prepared in compliance with the principles of the law in order to reduce the administrative cost borne by the private and public institutions incurred in personal data processing.

The exemption authorisations issued in 2008 concern the following aspects: “*Data Processing Concerning Billing and Contact Information of Customers, Suppliers and Service Providers*”, “*Data Processing by Educational Institutions Concerning Pupils or Students*”, “*Data Processing Concerning Library-and-Archive Users*” and “*Data Registration and Processing Concerning Arriving and Departing Visitors*”. While seeking proper protection of personal data, the Office will continue to study the possibilities of formulating and issuing more exemption authorisations to meet the needs of the community.

Communications, Cooperation and Publicity

I. International and Regional Communications

To get a sense of the latest international trend in personal data protection as well as share our experience and enhance co-operation with our counterparts in other parts of the world, the Office for Personal Data Protection (the Office) partook in 2008 in a few international forums and activities, where we had talks and shared ideas with our foreign peers. Meanwhile, in response to specialist and academic interest in some countries and regions in Macao's personal data protection status, the Office offered a few briefings in this respect.

1. Visit to the Office of the Privacy Commissioner for Personal Data, Hong Kong

In order to enhance communication and cooperation between Macao and Hong Kong on personal data protection undertakings, Coordinator Chan Hoi Fan and her colleagues visited the Office of the Privacy Commissioner for Personal Data in Hong Kong on 28 March 2008. Privacy Commissioner Mr. Roderick Woo and his staff warmly received the delegation. They mutually briefed on each other's work, exchanged views on certain issues of personal data protection, and finalised the arrangement of the "Privacy Awareness Week 2008" held in August 2008.

2. Attending the 29th Asia-Pacific Privacy Authorities Forum

The Office sent a delegation of observers to the 29th Asia-Pacific Privacy Authorities Forum, held in Seoul, Korea on 19 and 20 June 2008.

The Forum offered opportunities for sharing views on topics such as data breach notification, issues confronting the Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD), advancement in personal data protection in Korea, and personal data protection in the fast developing IT environment, etc. Member agencies and observers also explored the possibilities of further advancement in personal data protection, law reform and cooperation between privacy authorities in the Asia Pacific region.

3. Privacy Awareness Week 2008

The Office joined hands with Hong Kong's Office of the Privacy Commissioner for Personal Data in organising the regional Video Competition (Hong Kong / Macao) entitled "Privacy is Your Business" as a part of the "Privacy Awareness Week 2008" programmed by the Asia Pacific Privacy Authorities (APPA). In that connection, the Office also ran the same competition for the Macao people. Some of the best

contestants also took part in the Asia Pacific international competition. Yuet Wah College and St. Paul's School in Macao emerged as winners of the Best Cinematography Award and the Best Creativity Award respectively in the Hong Kong / Macao competition.

In August 2008, Coordinator Chan Hoi Fan attended the inaugural ceremony of the Privacy Awareness Week as well as the "Privacy is Your Business" International Video Competition Prize Presentation Ceremony in Hong Kong.

4. Attending the 30th International Conference of Data Protection and Privacy Commissioners

The Office participated as observer in the 30th International Conference of Data Protection and Privacy Commissioners held in Strasbourg, France between 15th and 17th October 2008.

The theme of the conference was "Protecting privacy in a borderless world". In its first two days' open sessions, topics were explored about the effect of personal data privacy on economic growth, privacy protection in social networking websites, privacy education and protection concerning adolescents, advantages and disadvantages of using digital technology and the future of personal data protection, among other issues. On the last day's closed session, participants and observers tackled issues including devising international standards, institutionalising the "International Privacy Day" or the "Privacy Week", privacy protection on social networking websites, children's online privacy protection, and the like.

The Office managed to set up preliminary work relations with other personal data protection authorities from all over the world in the course of the Conference. Starting with these relations the Office will further enhance the communication and cooperation with these countries and regions in the future.

II. Building community awareness

Apart from the work of communicating with our international counterparts, the Office also managed to keep it close contact with all sectors in Macao, with a view to develop a community-wide awareness of *Personal Data Protection Act*, and build community support for personal data protection efforts.

1. Working with community seminars

At the invitation of Civic and Municipal Affairs Bureau, the Office's representatives joined a community seminar held at the Carmo Hall, Taipa, on 8th May 2008, at which they made a presentation to people from Taipa and Coloane about the rights of data subject as provided for in the *Personal Data Protection Act*. The Office also took the opportunity to distribute its public awareness leaflets.

2. Reaching out for interaction

There has been attention and support for personal data protection in some government agencies and corporations, as it is obvious in their visits to the Office for information and communication. For example, a staff group of Association of Employment Agency with Chinese Capital (Macao) visited the Office on 2nd September, to show their support for the Office's efforts and exchange views on the work of personal data protection.

On the other hand, the Office also reached out to build relations with all sectors of the community. For example, on 18th April, an office delegation headed by Coordinator Chan Hoi Fan made a well-received visit to the Macao Chamber of Commerce, and was invited to make a presentation to its Board of Directors & Board of Supervisors of the Chamber about the major points of the *Personal Data Protection Act* and the Office's terms of reference. The two parties also agreed to cooperate in the future to enhance awareness of personal data protection among the business sectors.

III. Public awareness campaign

The Office launched a series of publicity activities in 2008 in an attempt to build public awareness of the *Personal Data Protection Act* and personal data protection in general, including hosting multiple law briefing sessions, publishing newsletter and annual report, producing promotional items, organising video sketch show competitions, preparing, and posting awareness advertisements on television, radio and newspapers.

1. Seminars

Since many government agencies and private institutions pay high attention to affairs pertaining to personal data protection, they invited the Office to host briefing seminars on the *Personal Data Protection Act* with a view to enhancing their staff's understanding thereof and better implementing measures for personal data protection. In response to their requests in 2008, the Office organised and co-organised 22 briefing sessions, involving 16 institutions and 1,339 people. Of those, some were organised and co-organised for professional industries and sectors, including banking, employment and social service sectors. These seminars received the support and good comments from the stated sectors.

2. Publications

Since its first issue in December 2007, the *Newsletter of the Office for Personal Data Protection* has become a platform of communication between the Office and the public, a major source of the latest and most detailed information about personal data protection. To ensure that people in all occupations can obtain such information on a regular basis, the Office decided to have the newsletter published as a quarterly and provide an on-line edition for the general readership. In addition, with the assistance of the ISBN Centre of Macao Central Library, the Office acquired an ISSN for the newsletter from Vol. 3, June 2008 from the ISSN (International Standard Serial Number) International Centre, based in Paris, France, making the newsletter a standard publication.

3. Publicity items

To enhance awareness of the *Personal Information Protection Act* and a sense of personal data protection, the Office prepared an assortment of publicity items in 2008, including 2009 calendar cards and desk calendars, Christmas cards, New Year cards, paper bags, eco-bags, notepads, ballpoint pens, folders, towels, mugs, travel power socket adapters and personalised stamps, among other things.

Table 1: Publicity items prepared by the Office

Publicity Items	Quantity
2009 calendar cards	11,000
2009 desk calendars	3,000
Christmas cards	500
New Year cards	500
Paper bags (large size)	200
Paper bags (small size)	300
Eco-bags	5,000
Small-sized note pads	5,000
Mid-sized note pads (with 150g note pad paper)	5,000
Mid-sized note pads (with 80g note pad paper)	5,000
Ball-point pens	5,000
Folders	3,000
Compressed towels	5,000
Color changing mugs	2,000
Travel power socket adapters	1,000
Stamps	500

4. Publicity activities

The Asia Pacific Privacy Authorities (APPA) hosted the “Privacy Awareness Week 2008” from 24th to 30th August. To complement this event the Office organised the Macao-wide “Privacy is Your Business” International Video Competition with a view to arousing concern about privacy, building respect for privacy and awareness of privacy protection among Macao residents, particularly adolescents. The Office also ran a series of complimentary activities in parallel with the competition.

“Privacy is Your Business” International Video Competition		
Dates	Activities	Contents
11 th June 2008	Press conference	Announcing the rules for the Macao-wide competition and introducing the Hong Kong / Macao and Asia Pacific-wide international competition.
5 th and 6 th July 2008	Video-sketch workshop	Adam Wong Sau Ping, a famous Hong Kong director introducing cinematography to and sharing experience with the participants with a view to upgrading the quality of their entries.
31 st July 2008	Panel meeting	Attending the meeting were Dr. Lam Iok Fong, Assistant Professor and Coordinator of Journalism & Public Communication Programme, Department of Communication, Faculty of Social Sciences and Humanities, University of Macao. Lai Fei Loi, Lecturer, Department of Communication, Faculty of Social Sciences and Humanities, University of Macao. Lei Sio Chong, Lecturer, School of Arts, Macao Polytechnic Institute. Chu Lun Bo, Vice President of Macao Video Space and Mr. Ho Ka Cheng from Cut Visual Arts Company. They served as the judges who picked the winning ones from the 13 entries. Eight winning entries were selected for the Hong Kong / Macao and Asia Pacific International Competition.
30 th August 2008	Macao-wide prize ceremony	Privacy Commissioner Mr. Roderick Woo and the jurors attended the prize ceremony. Yuet Wah College, St. Paul’s School and Hou Kong Middle School won the first, second and third prizes respectively. Among them, Yuet Wah College also won the Best Theme Expression, the Best Creativity and the Best Cinematography awards. All the winning entries have been uploaded to the Office website.
December 2008	Airing of first-prize sketch	In praise of the effort made by the contributors to the video competition, the Office aired the first-prize sketch during the advertising slots in December 2008 on Macao TV (Cantonese channel).

5. Publicity via newspapers, radio and television

1) “Privacy and You” column

To enhance the public’s understanding of the *Personal Data Protection Act* and raise their awareness on personal data protection, the Office started to pen a column called “Privacy and You” in the *Macao Daily News* and the *Jornal Va Kio* in 2008. In December, the column featured articles such as “Monthly Financial Statements come without envelops!”, “A row over property management” and “Disclosure of Trainees’ Contact Numbers”, where knowledge of the law is conveyed via simple case studies.

2) “Information Desk”

To make use of electronic media for promotion, and with the assistance of Teledifusão De Macao (TDM), the Office sent staff to prepare the programme “Information Desk” of Macao TV in February and March 2008. The programme introduces the functions of the Office, the rights of data subject, the leaflets and publications of the Office and the procedure of lodging enquiries or complaints with the Office.

3) Publicity video and radio sketches

In 2008, the Office produced five promotional animation video sketches, featuring themes of the “*Personal Data Protection Act*”, “right to information”, “right of access and right to rectify”, “right to object” and “consequences of unlawful practice”. These video and radio sketches will be aired in 2009 on Macao TV and Radio in advertising slots, and will be available on the Office website and other activities, in an entertaining way.

4) Office website

Since its official launch in 2007, the Office website has been continuously updating its contents and design, so that it bears the latest news of personal data protection, and functions as a successful communication platform between the Office and the public. The website registered over 70,000 visits in 2008.