2001 Opinion Survey

Personal Data Privacy Ordinance

Attitudes and Implementation – Key Findings

I Survey of Individuals – Data Subjects

1 Introduction

In 2001 the Office of the Privacy Commissioner for Personal Data ("the PCO") commissioned The Social Sciences Research Centre of the University of Hong Kong to conduct an opinion survey similar in design to that conducted in the previous year.

The first part of this survey investigated the perceptions, attitudes and experiences of data subjects towards personal data privacy in Hong Kong. The objectives of the survey were twofold.

- To investigate public attitudes towards, and experiences of, personal data privacy and its invasion. In terms of invasiveness emphasis was placed upon the types of misuse of personal data, workplace surveillance practices, Internet and E-Business privacy. In so doing the intention was to measure the level of awareness of the Personal Data (Privacy) Ordinance ("the PD(P)O") and the means by which members of the community learnt about the PCO, its role and functioning.

- Secondly, where appropriate, comparisons were made with the findings of the 2000 survey to track changes that had occurred over the intervening 12 months.

The survey was conducted between late March and mid April 2001 when 1,706 respondents were successfully interviewed using a questionnaire administered over the telephone. In this part of the survey questions explored the following range of issues.

~ Sensitivity towards the workplace surveillance

~ The importance of privacy as a social policy

~ Personal data on public registers

~ The misuse of personal data

~ Channels for learning about the PCO and the effectiveness of the PCO

~ Usage of the Internet for personal purposes

~ Privacy and security concerns about purchasing on the Internet

~ Sensitivity towards actions involving personal data on the Internet.

The key findings of the data subjects survey are summarized below.

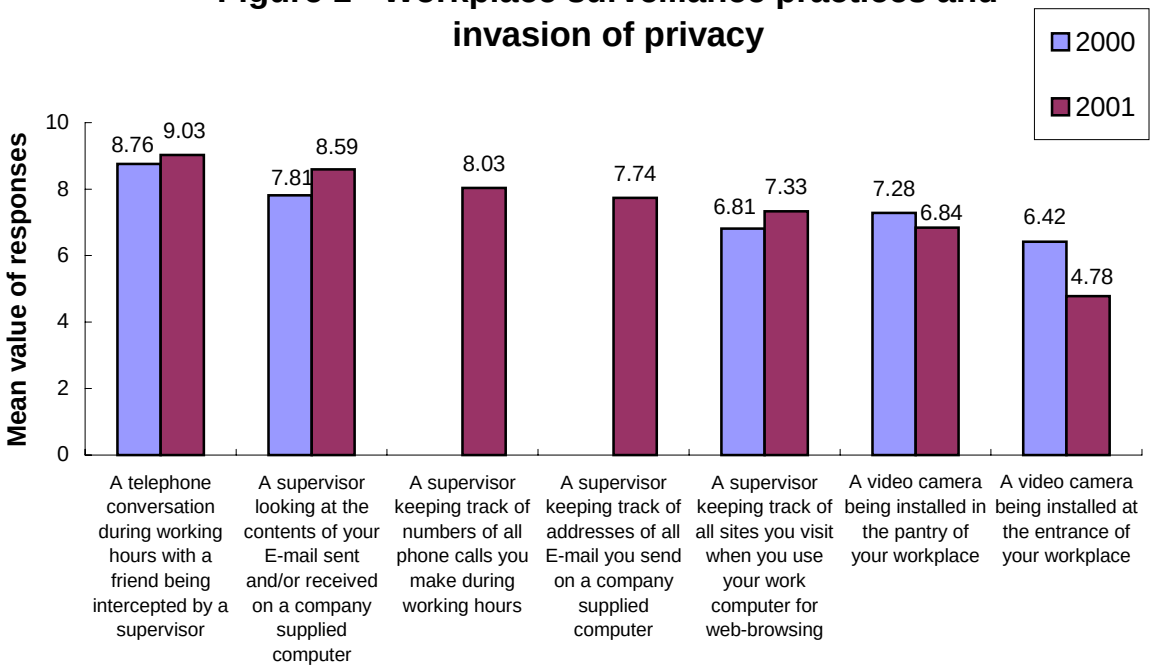
2 Sensitivity towards workplace surveillance

The findings for 2001 were in line with those of the 2000 survey indicating that respondents' opinions towards workplace surveillance practices were consistent.

Respondents in the 2001 survey indicated that they were sensitive towards a variety of activities that could be subsumed under the umbrella of surveillance in the workplace. In general, the public considered the activities listed to be quite invasive.

Respondents were asked to rank various workplace surveillance practices a 0-10 point scale in terms of their invasiveness (Figure 1).

Figure 1 - Workplace surveillance practices and invasion of privacy

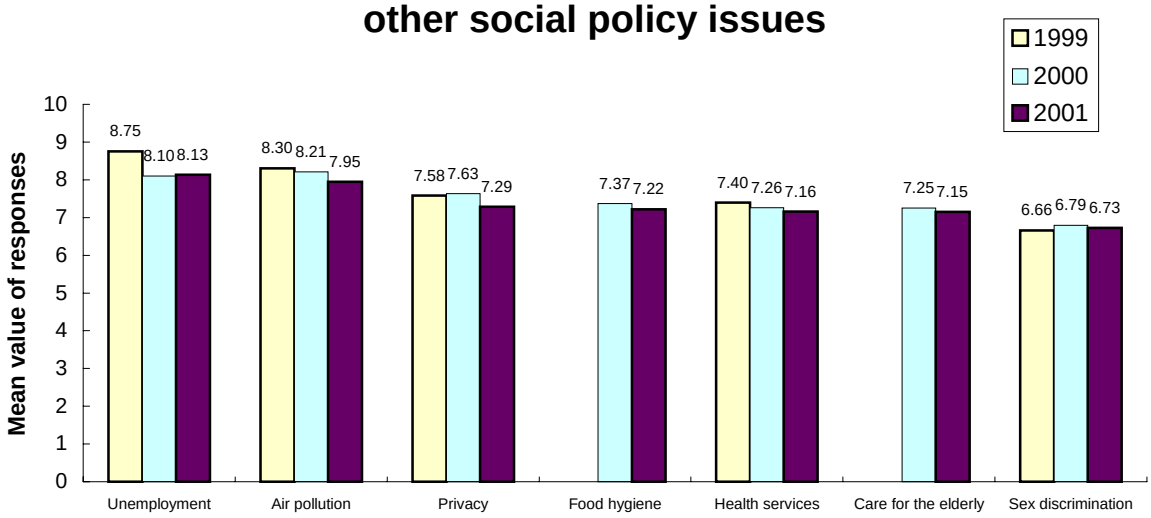


Key 0 = Not an invasion of privacy at all
10 = A very severe invasion of privacy

3 The importance of privacy as a social policy

Consistent with the findings of previous surveys, respondents judged privacy to be less important than unemployment and air pollution, approximately the same as food hygiene, health services and care for the elderly but more important than sex discrimination (Figure 2).

Figure 2 - The importance of privacy in relation to other social policy issues

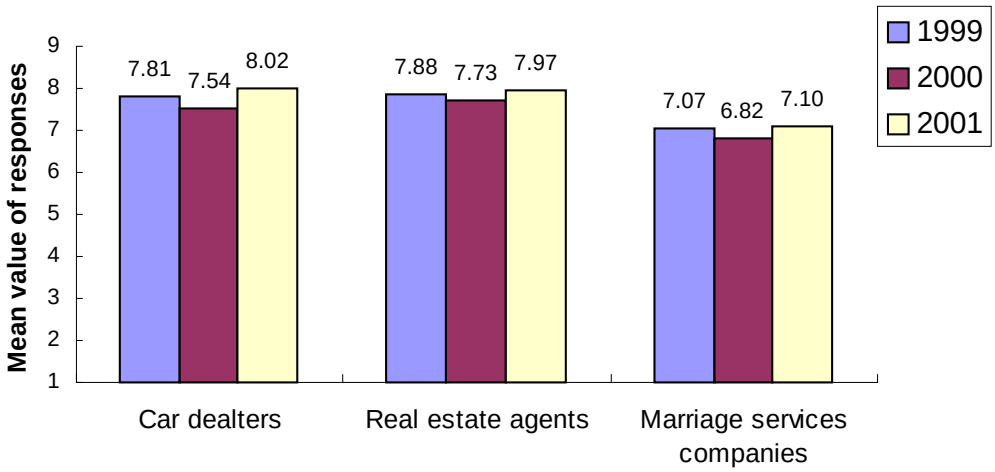


Key 0 = Not important at all
10 = Very important

4 Personal data on public registers

The results indicate a general concern regarding three practices associated with personal data held on public registers. The three mean problem ratings increased slightly when compared with the findings of the 2000 survey. Respondents indicated that they were concerned about three public registers, that could be accessed by car dealers, real estate agents and marriage service companies, in terms of their potential to create personal data privacy problems (Figure 3).

Figure 3 - Public registers: current practices and their potential for causing personal data privacy problems

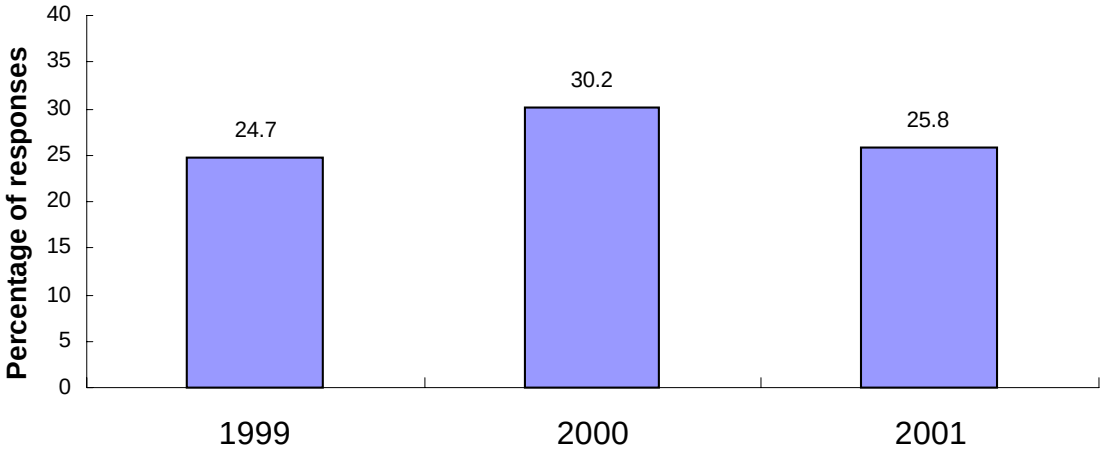


Key 0 = No problem at all
10 = A very serious problem

5 The misuse of personal data

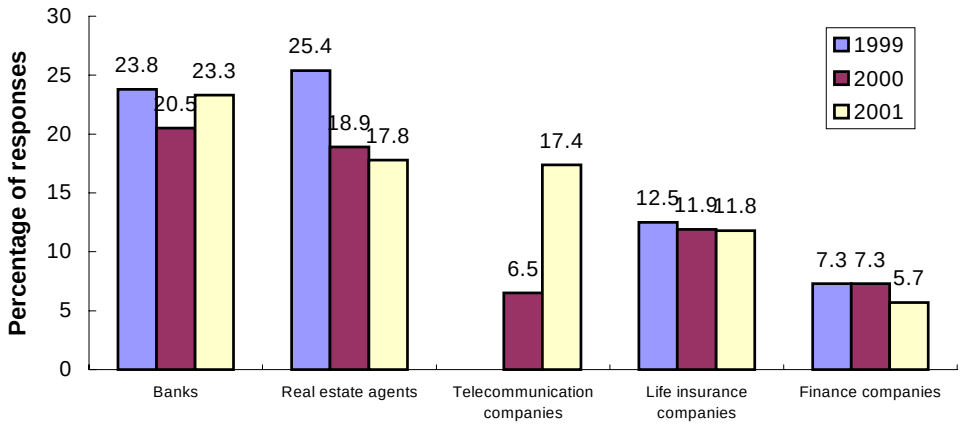
In comparison with the 2000 survey, there was a decrease in the percentage of respondents (30% to 26%) claiming that their personal data had been misused in the twelve months preceding the date of the interview (Figure 4).

Figure 4 - Personal experience of misuse of personal data



Respondents alleged that the most frequent misusers of personal data were banks, real estate agents and telecommunications companies. The pattern of ranking of alleged misusers was very similar between the 2000 and 2001 surveys, apart from the increase in alleged misuse of personal data among telecommunications companies. This increase resulted in telecommunications companies moving from fifth position in 2000 to third position in 2001 (Figure 5).

Figure 5 - Alleged mis-users of personal data by sector



The types of alleged misuse of personal data by banks, finance companies and telecommunications companies were:

~ Sending direct mail materials without the consent of the data subject.

~ Transferring personal data to third parties without the consent of the data subject.

~ No opt out clause in the direct mail material sent to the data subject.

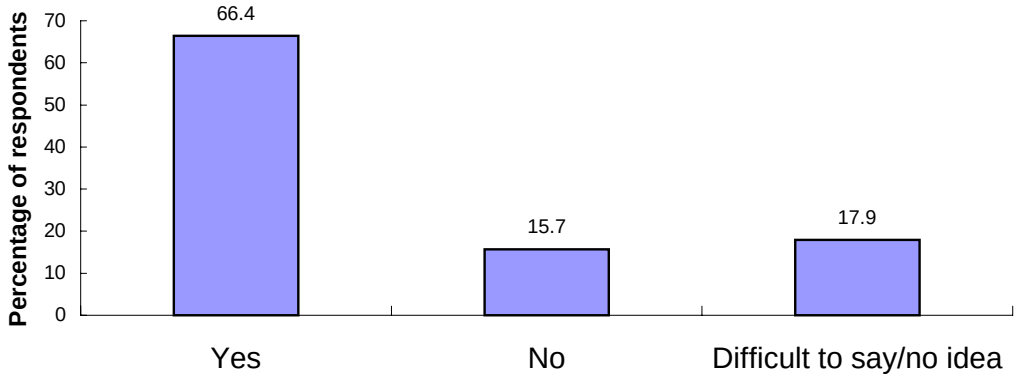
~ The data subject receiving too many marketing calls.

~ Debt collection practices directed towards the data subject.

6 The desire to make complaints in connection with the alleged misuse of personal data

66% of respondents in the 2001 survey indicated that they would certainly complain if they thought their personal data had been misused (Figure 6).

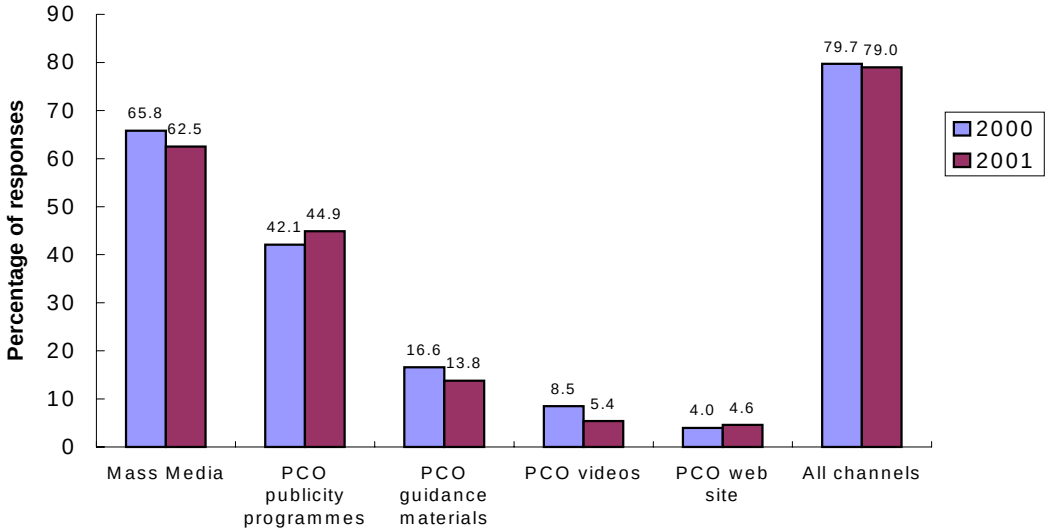
Figure 6 - Would you make a complaint if you thought your personal data had been misused?



7 Channels for learning about the PCO and the effectiveness of the PCO

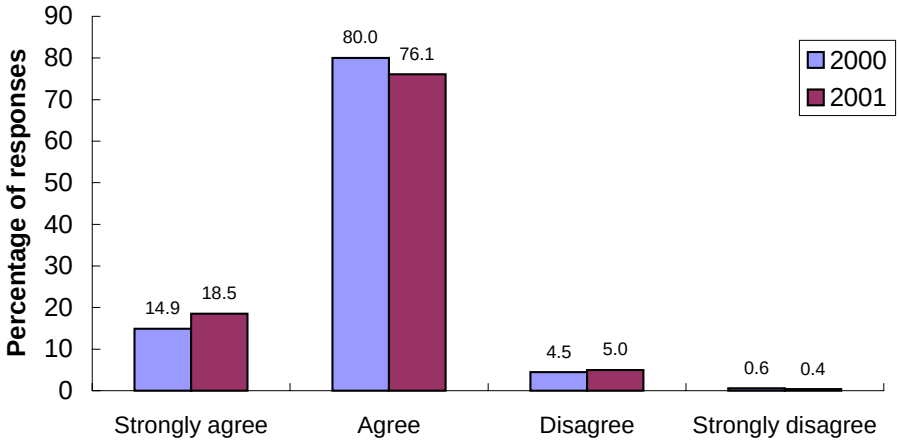
The 2001 survey results indicate that the channels for learning about the PCO and its work were similar to the findings for the 2000 survey. Mass media was most likely to create awareness of the PCO in the community. This was followed by PCO publicity programmes, guidance materials, videos and the website (Figure 7).

Figure 7 - Channels for learning about the PCO and its work



95% of respondents either agreed, or strongly agreed with the view that the PCO had been successful in increasing community awareness of personal data privacy issues (Figure 8).

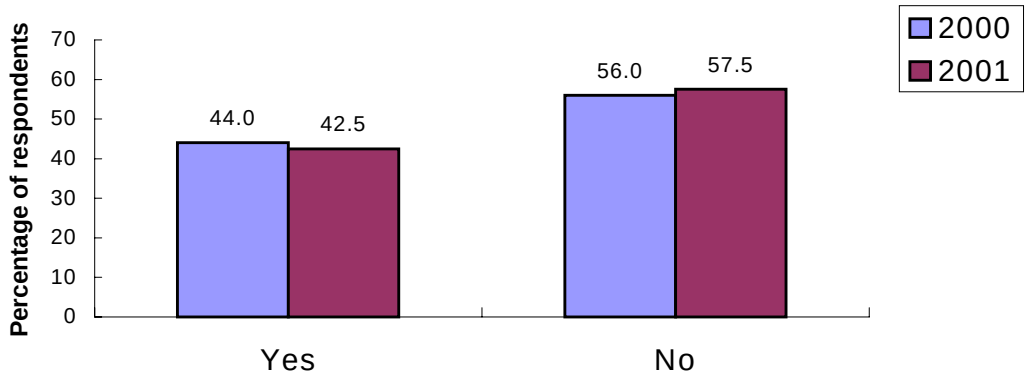
Figure 8 - Responses to the view that the PCO had increased community awareness of personal data privacy issues



8 Usage of the Internet for personal purposes

Similar to the 2000 survey findings approximately 43% of respondents reported that they used the Internet, either at home and/or work, for personal purposes (Figure 9).

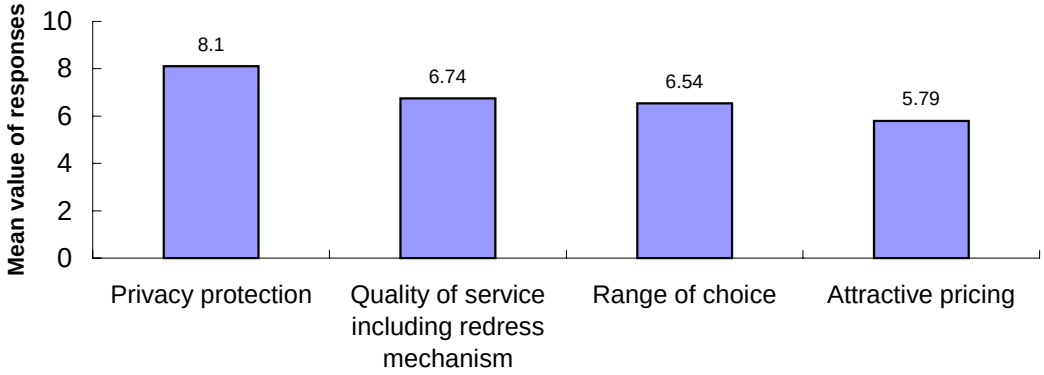
Figure 9 - The use of the Internet for personal purposes



9 Privacy and security concerns about purchasing on the Internet

Those respondents who used the Internet expressed considerable concern about privacy protection when purchasing on the Internet (Figure 10).

Figure 10 - The relative important of factors in making purchase decisions on the Internet



Key 0 = Not important at all
10 = Very important

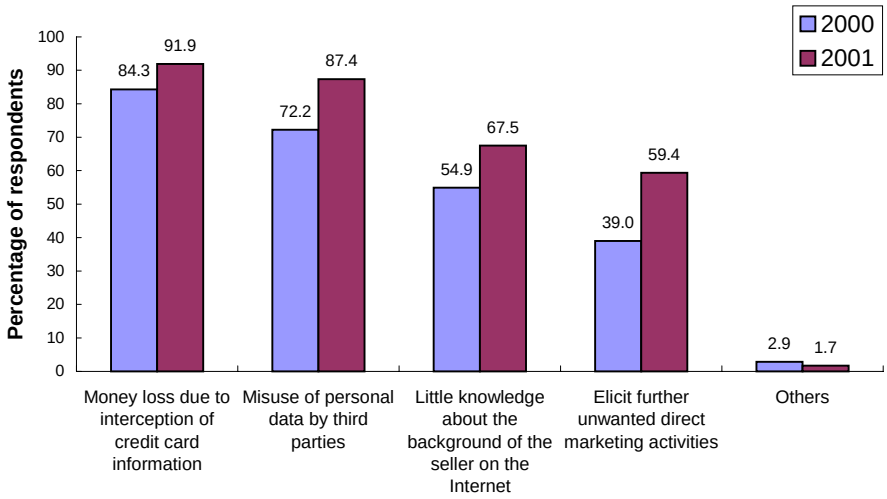
The most important areas of concern where (Figure 11):

~ Money loss due to the interception of credit card information

~ Misuse of personal data by third parties

~ Little knowledge about the background of sellers on the Internet.

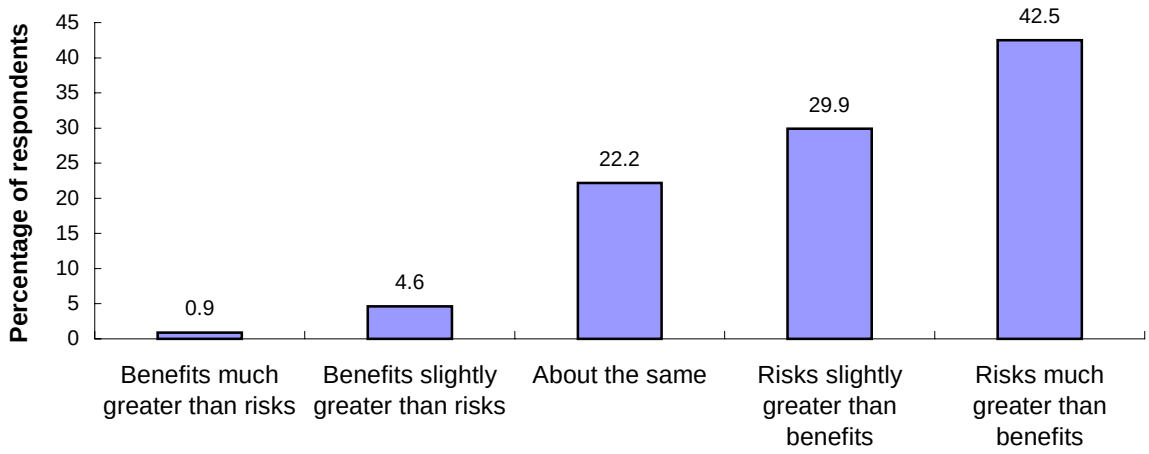
Figure 11 - Areas of privacy concern when purchasing on the Internet



10 Sensitivity towards actions involving personal data on the Internet

72% of respondents agreed with the view that the practice of keeping track of their visits to different Websites by some advertisers i.e. the use of cookies, would bring risks that were greater than the benefits. Only 6% of respondents felt that this practice would bring benefits greater than risks (Figure 12).

Figure 12 - If an advertiser keeps track of your visits to Websites are the risks greater than benefits or, the benefits greater than the risks?



- The End -

2001 Opinion Survey
Personal Data (Privacy) Ordinance
Attitudes and Implementation – Key Findings

II Survey of Organisations – Data Users

1 Introduction

The content of the 2001 data users survey was much the same as that for the 2000 survey. Significant changes were however made to the sampling frame in order to investigate six specific economic sectors: healthcare, banking and finance, insurance, real estate, telecommunications and government departments. One consequence of this change in the sample is that any comparison of results with those obtained in previous years must recognise the nature of the respective sample differences.

The main objectives of the data users survey were as follows.

- To focus upon the attitudes and experience of organisations drawn from the five non-government sectors mentioned and the government sector.

- Secondly, to investigate data users attitudes and the measures taken to implement the provisions of the Personal Data (Privacy) Ordinance ("the PD(P)O"), their sources of assistance (including the PCO) in seeking compliance, and their practices pertaining to employment-related personal data privacy.

- Finally, to study identified practices relating to common personal data problems in non-government sectors e.g. debt collection practices, direct marketing etc.

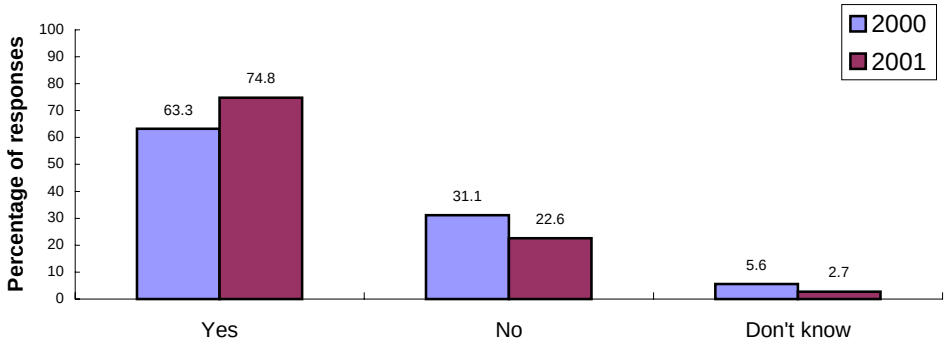
Pre-survey interviews were conducted with two senior officers from the Operations Division of the PCO and five data protection officers from the five non-government sectors to facilitate the design of the data users questionnaire. The fieldwork was conducted between mid-August and late September 2001 using a self-administered mail questionnaire. In total, 228 usable questionnaires were returned giving a response rate of 58.5%.

2 Organizational arrangements to comply with the PD(P)O

Compliance with the PD(P)O

The percentage of respondent organisations claiming that their management had formally adopted *written* policies to comply with the PD(P)O increased from 63.3% in 2000 to 74.8% in 2001 (Figure 1).

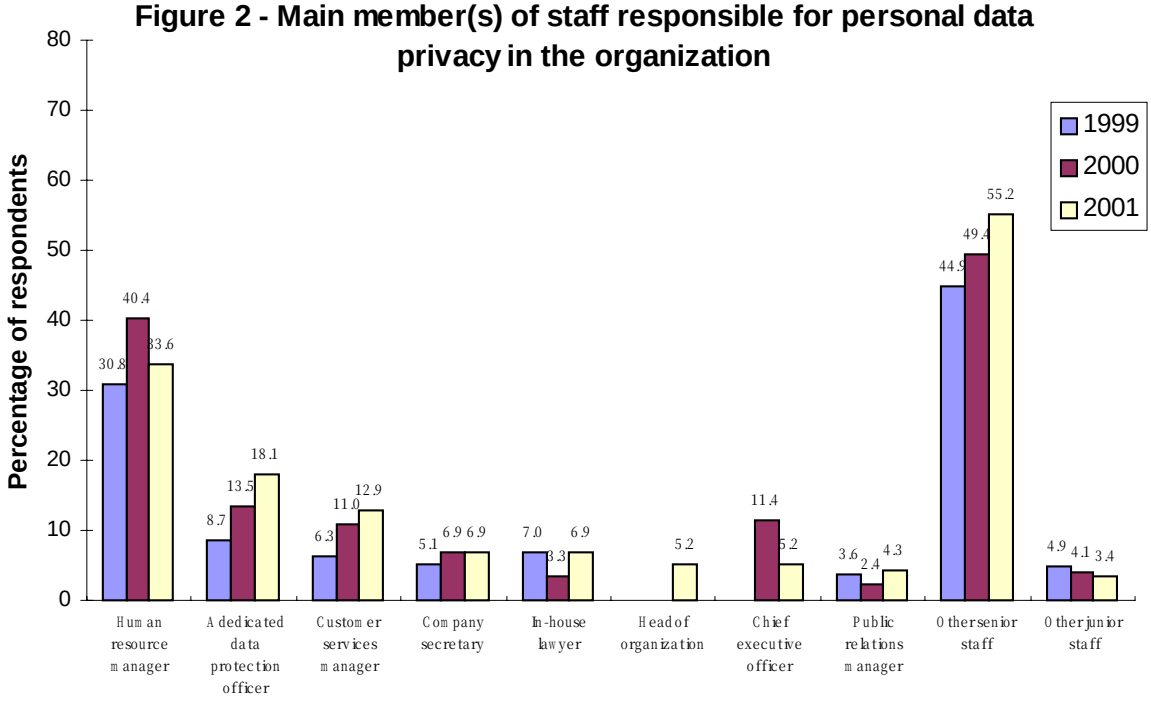
Figure 1 - Organizations that formally adopted written policies to comply with the PD(P)O



Organizational staff arrangements to comply with the PD(P)O

In the 2001 survey 69.9% of non-government respondent organisations had allocated responsibility for personal data privacy to a designated person(s). Among these organisations 33.6% had allocated the responsibility to Human Resource managers and 18.1% had created a dedicated position of Data Protection Officer to handle personal data privacy issues (Figure 2).

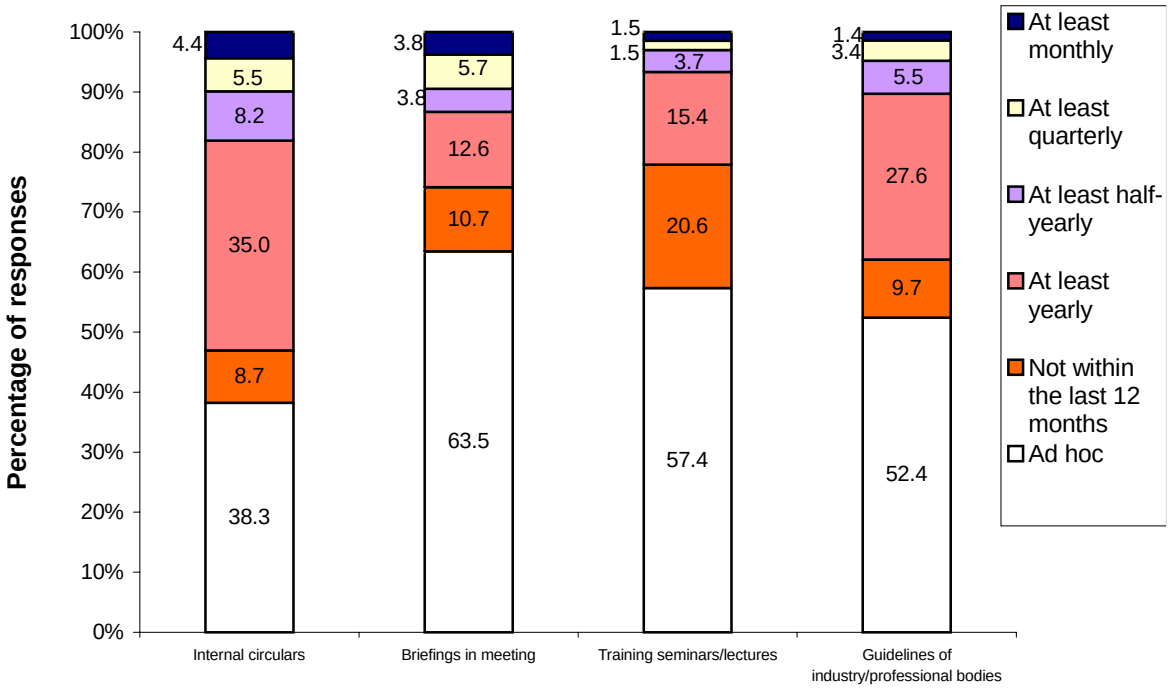
Figure 2 - Main member(s) of staff responsible for personal data privacy in the organization



Formal help provided to organizational staff

Respondent organisations tended to provide help to their staff in coping with the requirements of the PD(P)O on an ad hoc basis. “Internal circulars” and “briefings during meetings” were the more popular forms of assistance offered to staff (Figure 3).

Figure 3 - Frequency of help provided to organizational staff

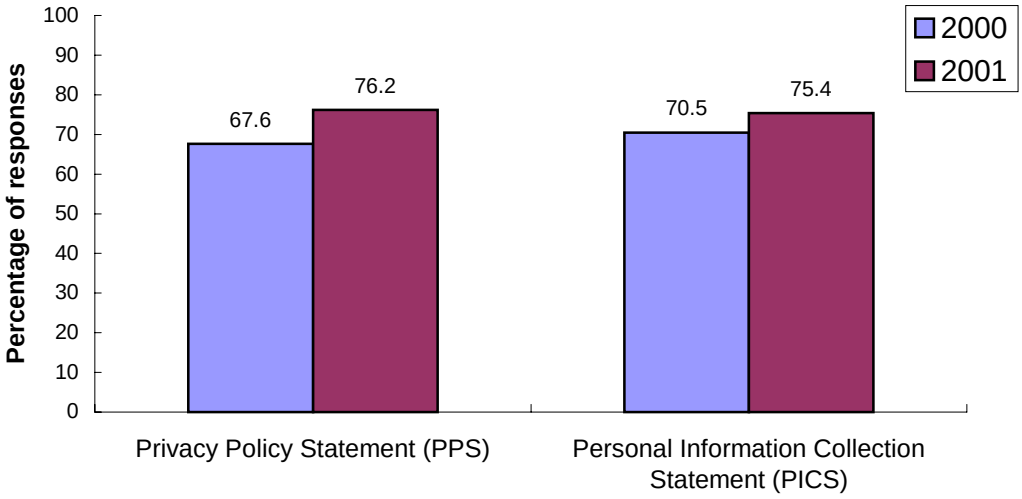


3 Compliance with the provisions of the PD(P)O

Privacy policy statement (PPS) and personal information collection statement (PICS)

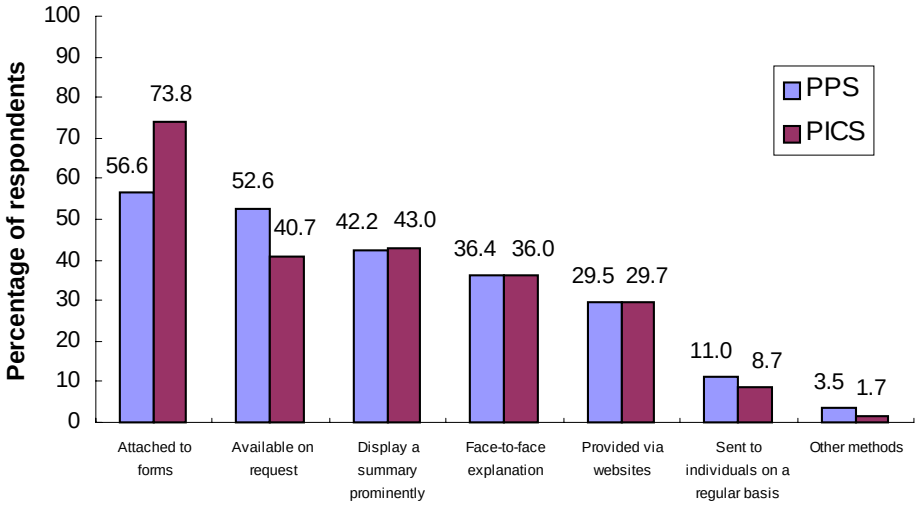
76.2% of respondent organisations had a Privacy Policy Statement (PPS) and 75.4% had a Personal Information Collection Statement (PICS) (Figure 4).

Figure 4 - Organizations having a Privacy Policy Statement (PPS) and Personal Information Collection Statement (PICS)



The relative importance of the methods used to inform the public about the PPS and PICS was quite similar for both statements (Figure 5). The most popular methods were “attached to forms” (56.6% for PPS and 73.8% for PICS) and ”available on request” (52.6% for PPS and 40.7% for PICS).

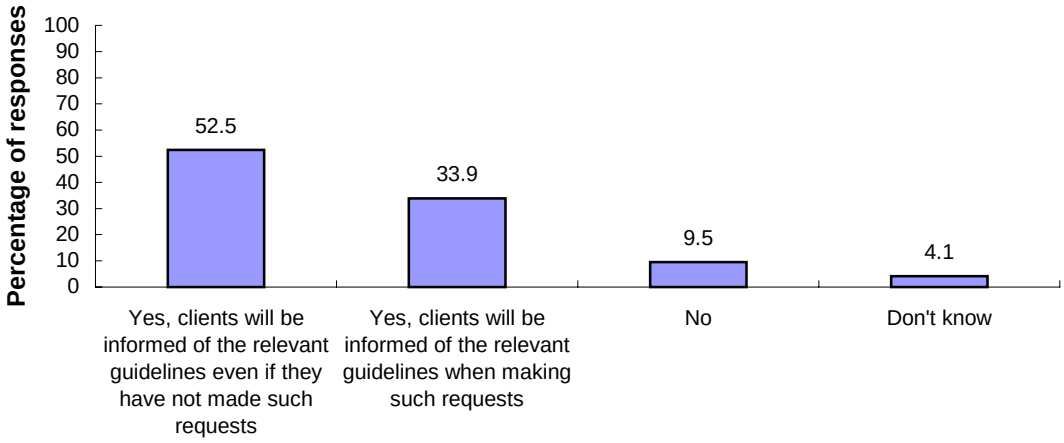
Figure 5 - How were data subjects informed about the organization's PPS and PICS?



Data Access Requests

Figure 6 indicates that 86.4% of respondent organisations notified their clients of their right to request access to, and correction of, their personal data. 52.5% claimed that they would proactively inform their clients of the relevant guidelines, even if their clients had not made a data access request. In contrast, 33.9% indicated a more passive approach in that they would, upon request, inform their clients of the guidelines for data access.

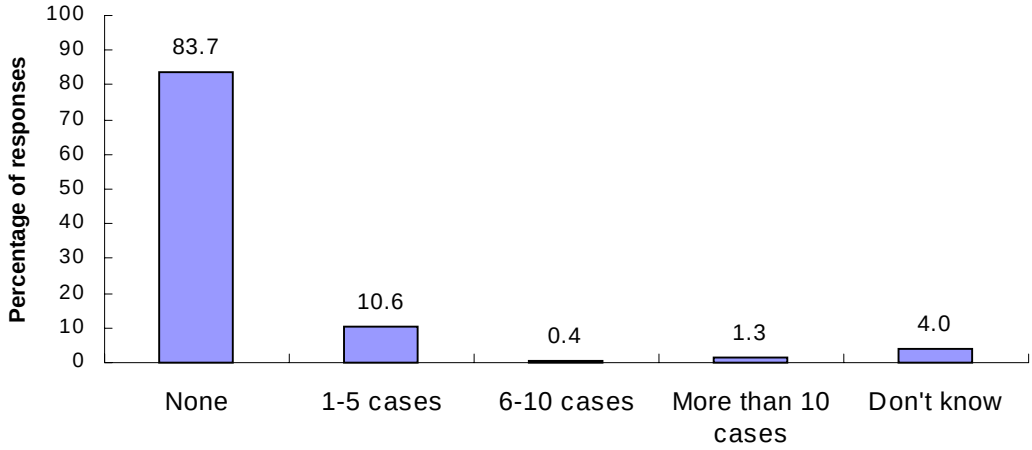
Figure 6 - Are your clients notified of their right to request access to, and correction of, personal data?



Complaints

Figure 7 reveals that 83.7% of respondent organisations claimed that they received no complaints under the PD(P)O between 1st January and 31st of December 2000. 10.6% received between 1 and 5 complaints, 0.4% received between 6 and 10 complaints and 1.3% received more than 10 complaints.

Figure 7 - Number of complaints received between 1st January and 31st December 2000

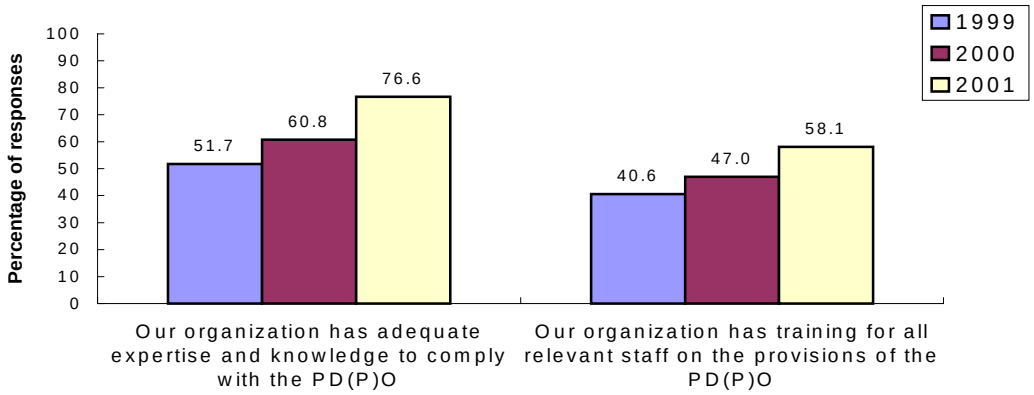


4 Expertise, training and attitudes towards the PD(P)O

Expertise and training

In comparison with the results obtained in the 2000 survey, respondents' confidence in their preparedness for the PD(P)O i.e. possessing adequate expertise and knowledge, rose from 60.8% to 76.6%. Confidence regarding staff training increased from 47% to 58.1% (Figure 8).

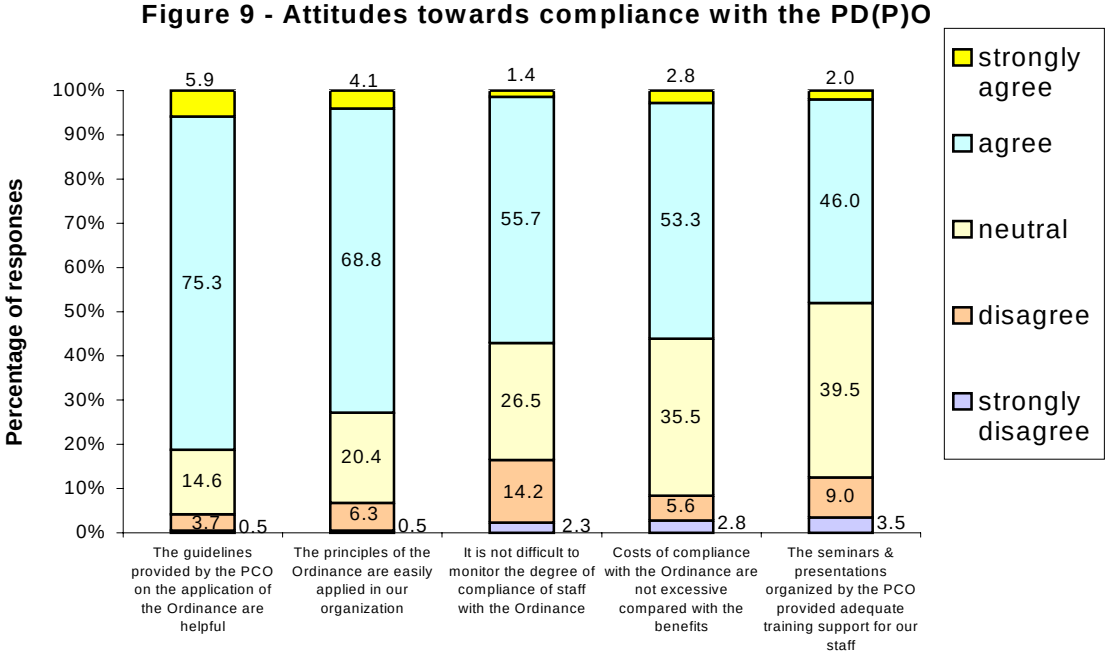
Figure 8 - Preparedness for the Ordinance: Strongly agree/agree



Attitudes towards compliance with the PD(P)O

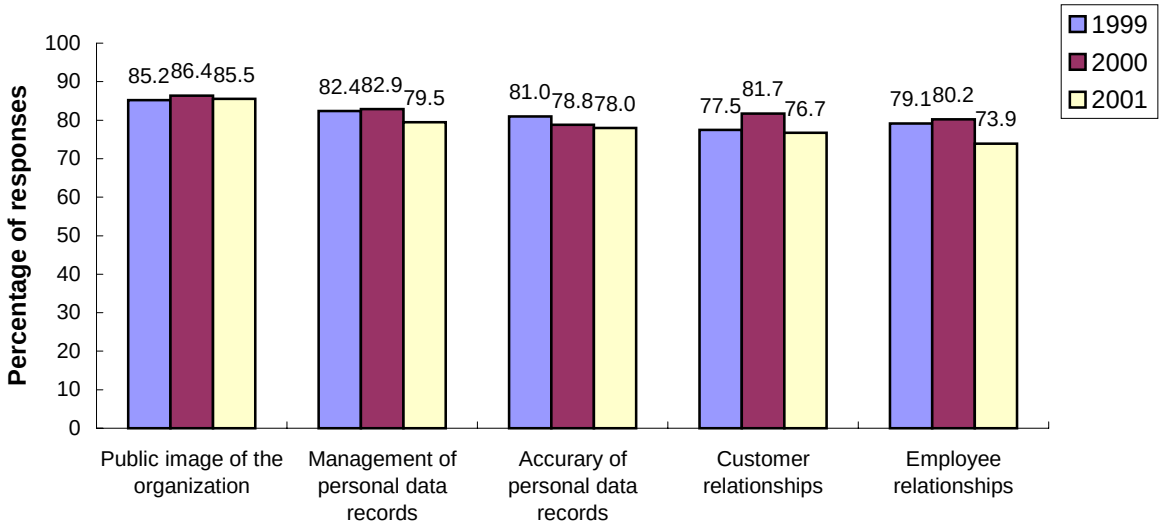
Overall, respondents displayed a positive attitude towards compliance with the PD(P)O. The statement "the guidelines provided by the PCO on the application of the PD(P)O are helpful" received the highest positive percentage of 81.2% (Figure 9).

Figure 9 - Attitudes towards compliance with the PD(P)O



In general there has, over the past three years, been a high level of agreement with the view that compliance with the provisions of the PD(P)O bring long term benefits to an organisation (Figure 10).

Figure 10 - Long-term benefits of the Ordinance: Strongly agree/agree

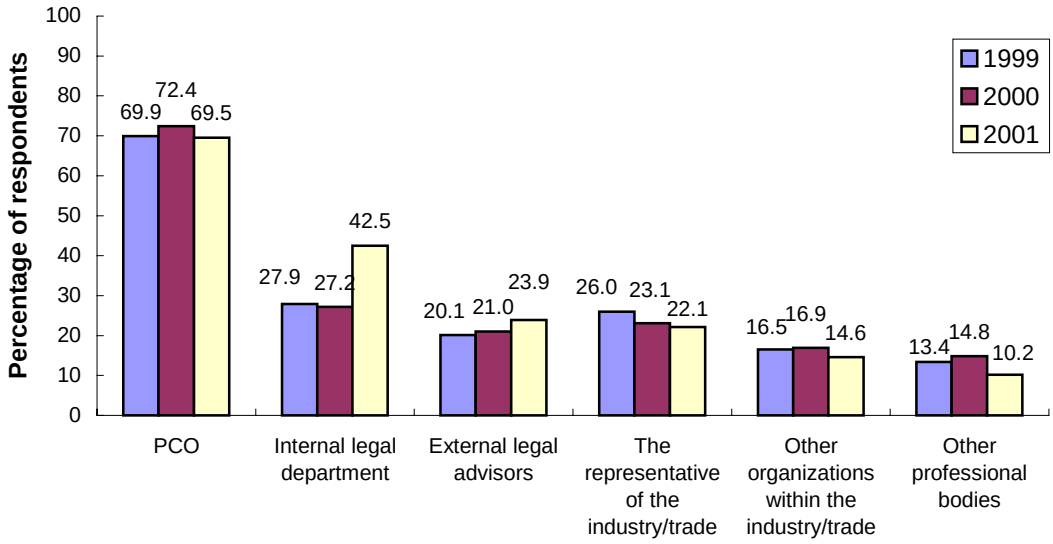


5 Sources of assistance

Sources of assistance for organisations

Consistent with the rankings established in the 2000 survey, the findings in 2001 indicate that the PCO was the most popular source of assistance for organisations (69.5%). Internal legal departments were the second most popular (Figure 11).

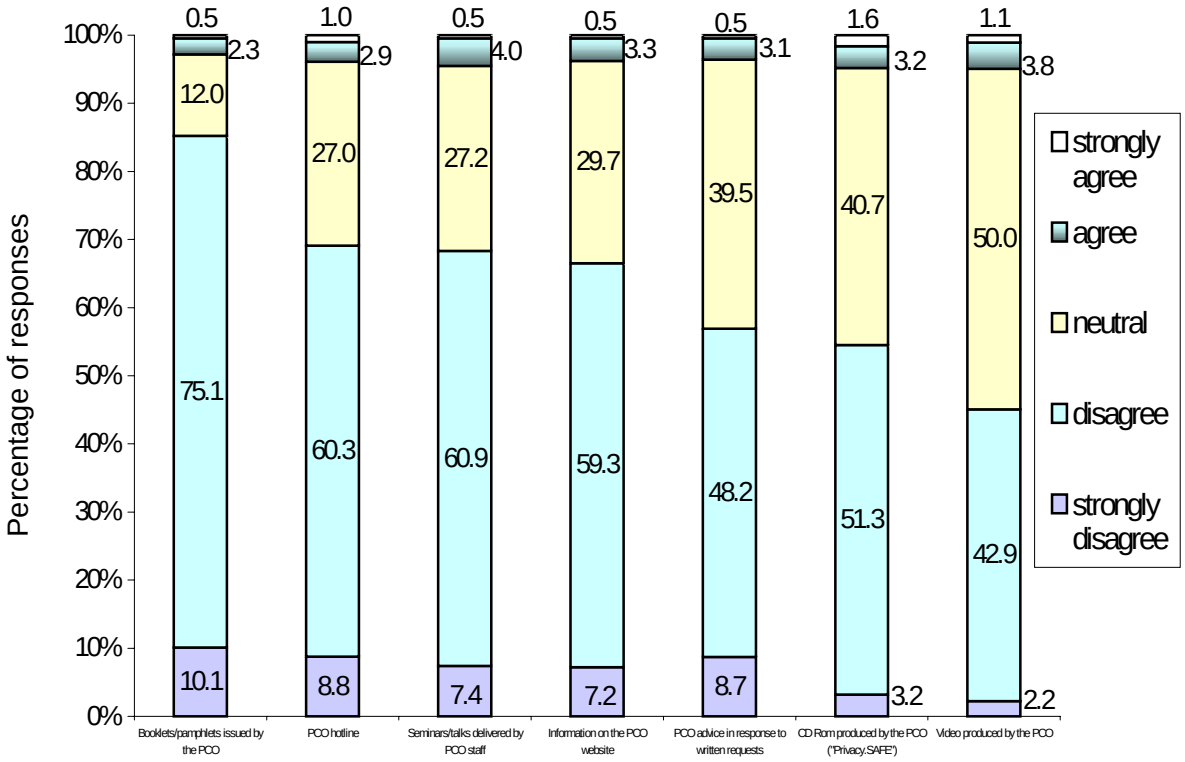
Figure 11 - Who do organizations seek assistance from?



Attitudes towards assistance offered by the PCO

Figure 12 reveals an overall positive attitude towards the usefulness of the resources and services offered by the PCO. “Booklets and pamphlets” received the highest agreement percentage. “Hotline”, “seminars/talks” and “information on the website” all received agreement percentages from more than 67% of respondent organisations.

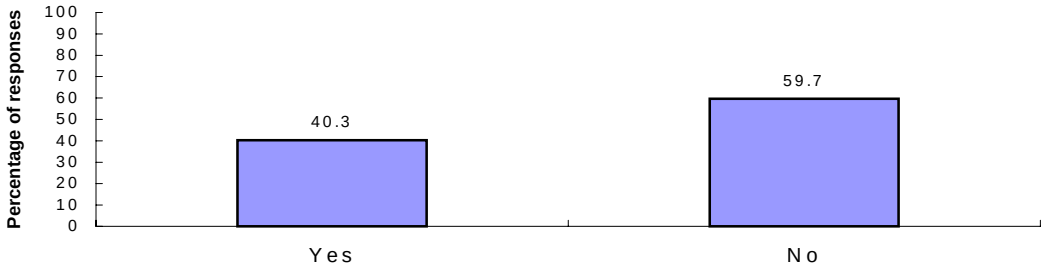
Figure 12 - The usefulness of PCO resources and services



The Data Protection Officers Club

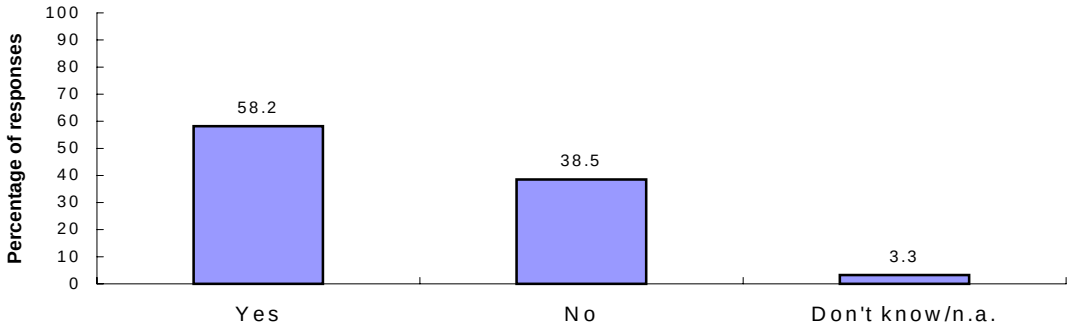
40.3% of respondent organisations were aware of the existence of the PCO’s Data Protection Officers Club (Figure 13).

Figure 13 - Are you aware that the PCO has established a Data Protection Officers Club?



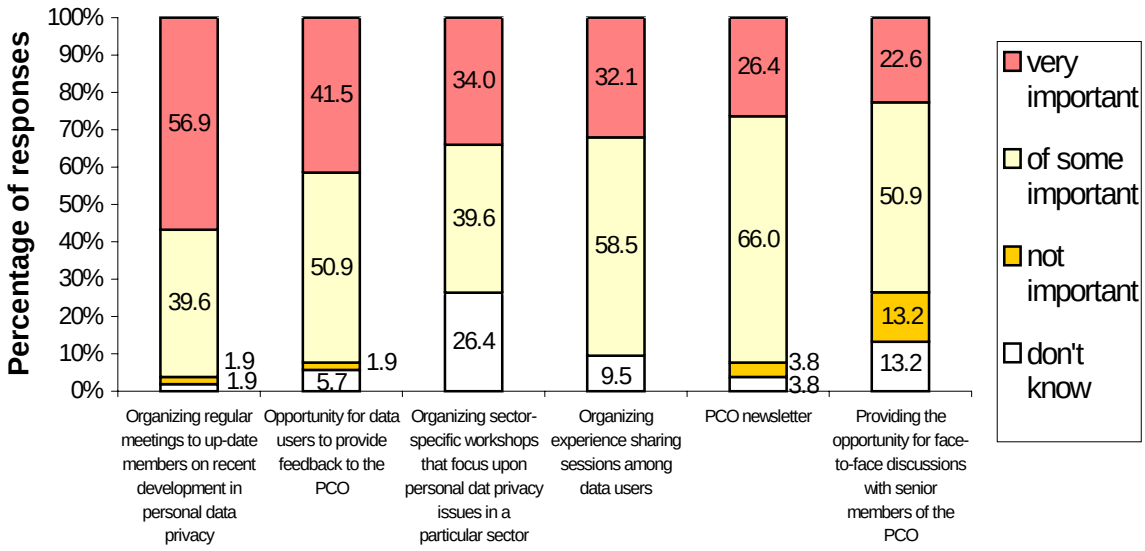
58.2% of respondent organisations that knew of the Club, indicated that they had a representative in it (Figure 14).

Figure 14 - Does your organization have a representative who is a member of the Club?



In general, Figure 15 indicates a positive attitude towards the importance of the activities organised by the Club. “Regular meetings” received the highest percentage from those respondent organisations that had a Club member, with 56.9% indicating that they were “very important”. At least 90% of respondents found “regular meetings for update”, “opportunity for feedback from the PCO”, “experience sharing among data users” and “the PCO’s newsletter” of at least some importance.

Figure 15 - The importance of activities organized by the Data Protection Officers Club

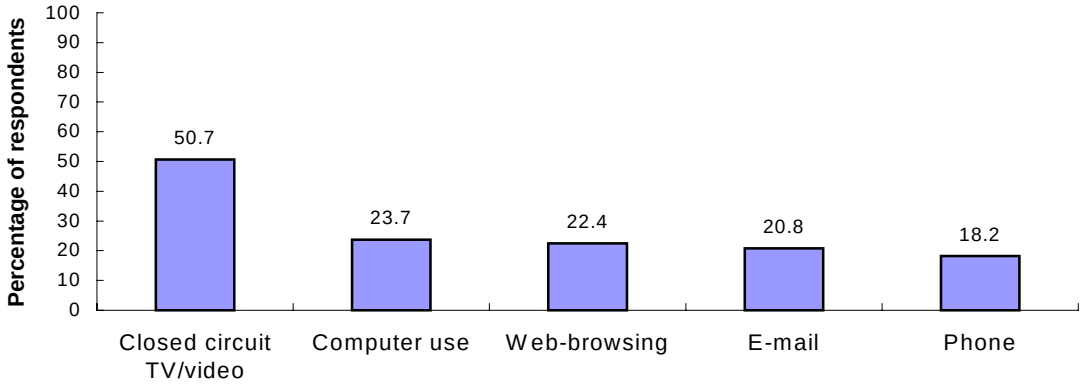


6 Employment-related Personal Data Privacy

Types of surveillance facilities in the workplace

The 2001 survey findings revealed that 63.6% of respondent organisations had installed *at least* one of five alternative types of surveillance equipment in the workplace. The adoption rate for closed circuit TV/video was the highest at 50.7%, and lowest for phone monitoring at 18.2% (Figure 16).

Figure 16 - Adoption of alternative surveillance facilities in the workplace

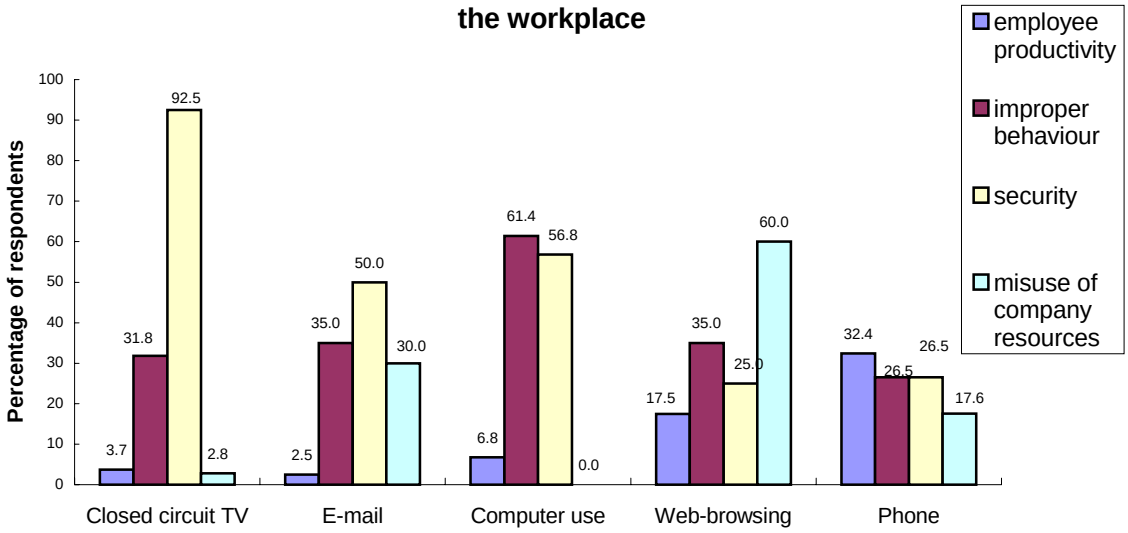


Closed circuit TV/video was most usually installed at main entrances and exits of the workplace (37.3%). Phone monitoring devices were mostly used to keep record of the content of calls (10.1%). E-mail monitoring facilities were largely employed to keep track of the origin and destination of E-mail (17.3%). Monitoring web-browsing activities was mostly used to record the websites visited (17.2%). Computer use monitoring facilities were used to keep a record of file data accessed (14.9%).

The main purposes served by surveillance equipment in the workplace

The most important purposes served by closed circuit TV/video, E-mail and computer monitoring were to safeguard security and deter improper behaviour. On the other hand, web-browsing monitoring was chiefly used to guard against misuse of company resources. Phone monitoring devices were mostly applied to check on the productivity of employees (Figure 17).

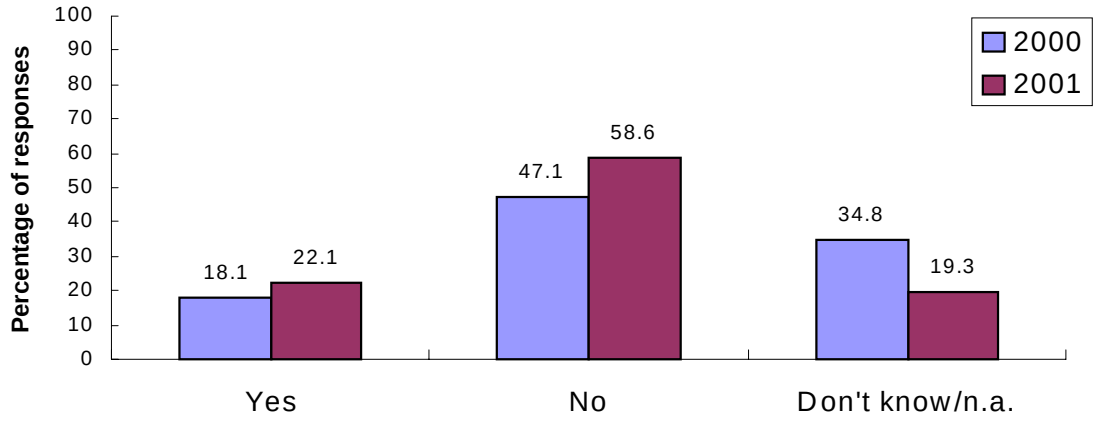
Figure 17 - The main purposes served by surveillance equipment in the workplace



Written policies and code of practice on workplace surveillance

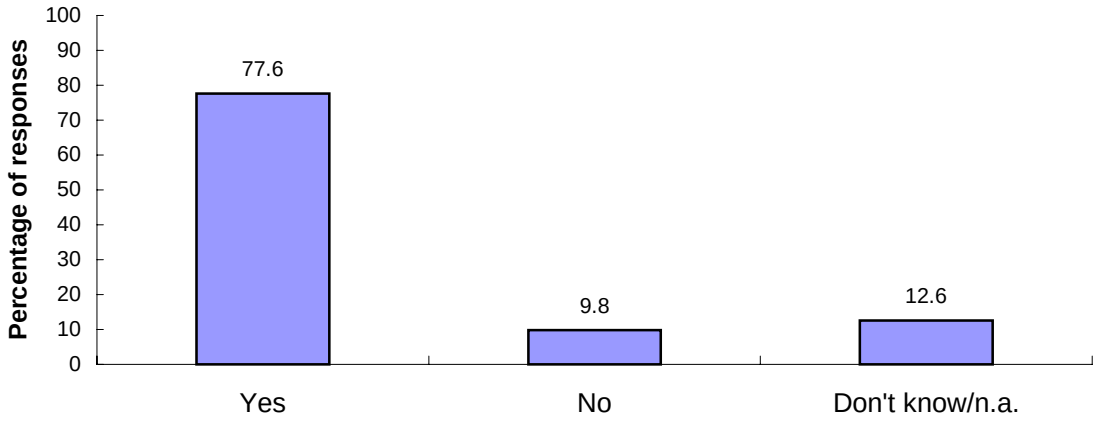
22.1% of respondent organisations had written policies to cover workplace surveillance practices. 58.6% had no such written policy, an increase of 11.5% on the results for 2000 (Figure 18).

Figure 18 - Do you have a written policy covering workplace surveillance practices?



Irrespective of whether respondents had a written policy on workplace surveillance practices, 77.6% showed support for the PCO developing a Code of Practice on Workplace Surveillance (Figure 19).

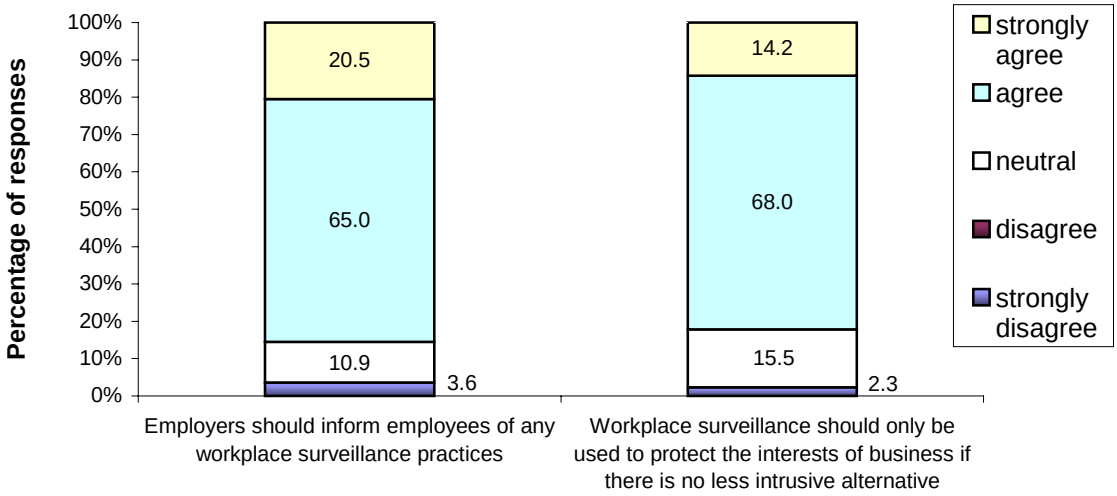
Figure 19 - Would you support the PCO developing a Code of Practice on Workplace Surveillance



Attitudes towards workplace surveillance practices

85.5% of respondent organisations agreed that "employers should inform employees of any workplace surveillance practices". 82.2% agreed that "workplace surveillance should only be used to protect the interests of business if there were no less intrusive alternative" (Figure 20).

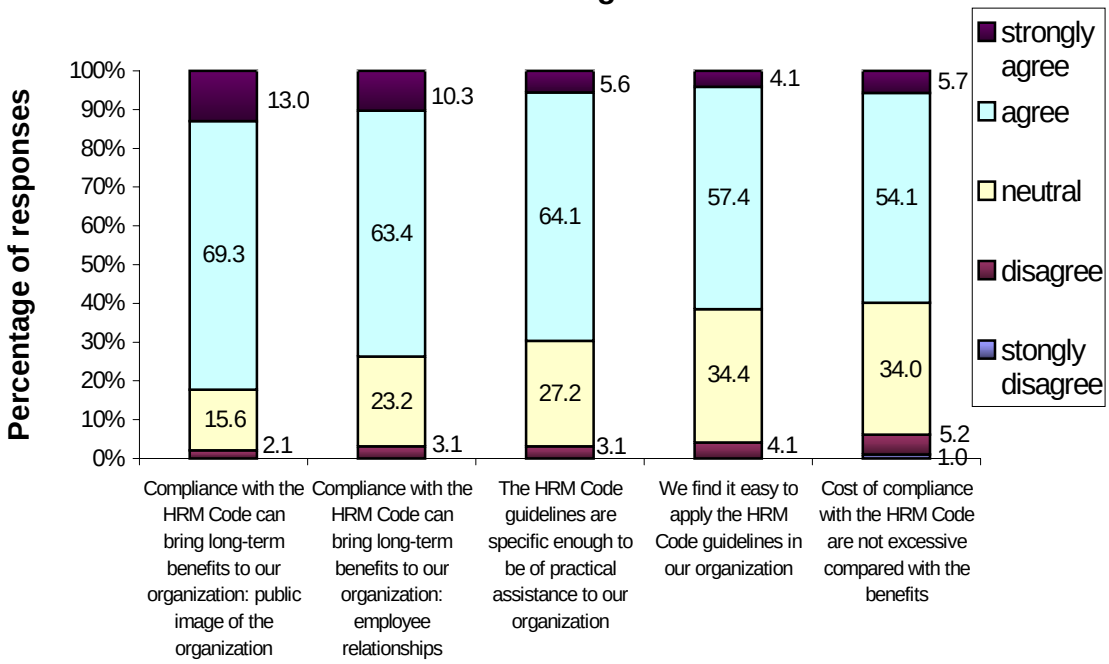
Figure 20 - Attitudes towards workplace surveillance practices



Attitudes towards the Code of Practice on Human Resource Management

In general respondents expressed a positive attitude towards the Code of Practice on Human Resource Management ("the HRM Code") written and published by the PCO. "Long-term benefits" brought about by the HRM Code received the highest positive percentage, with 82.3% agreeing with the benefits to the "public image of the organisation" and 73.7% agreeing "benefits to employee relationships" (Figure 21).

Figure 21 - Attitudes towards the Code of Practice on Human Resource Management



- **The End -**

2001 Opinion Survey

Personal Data (Privacy) Ordinance

Attitudes and Implementation – Key Findings

III Survey of Data Users by Economic Sector

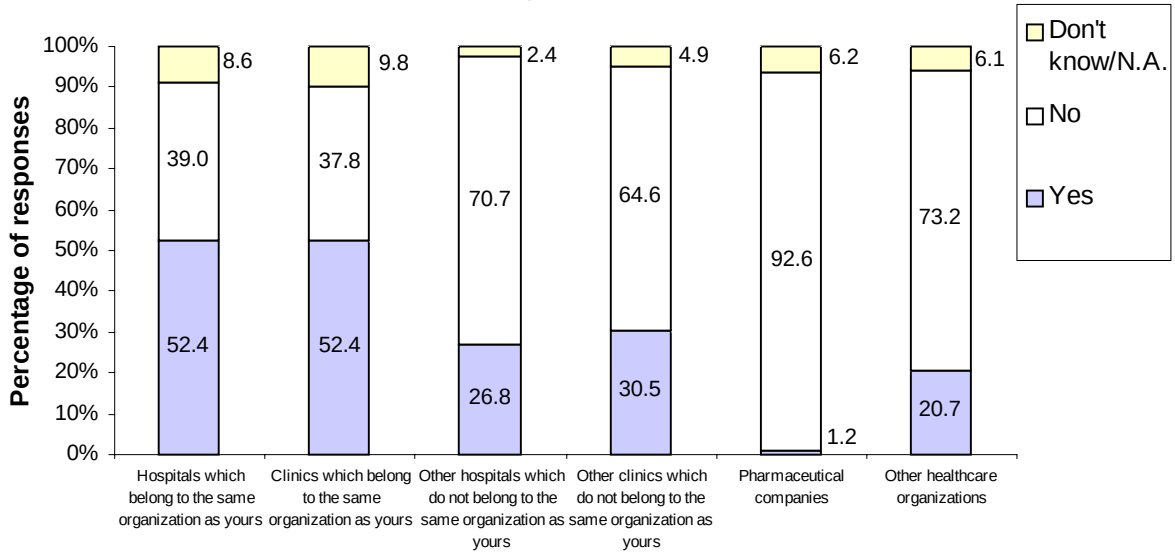
Personal Data Privacy Practices in the Healthcare Sector

1 Practices Relating to the Transfer and Sharing of Personal Data

A total of 147 organizations were sampled in the healthcare sector of which 86 filed a usable return giving a response rate of 58.5%.

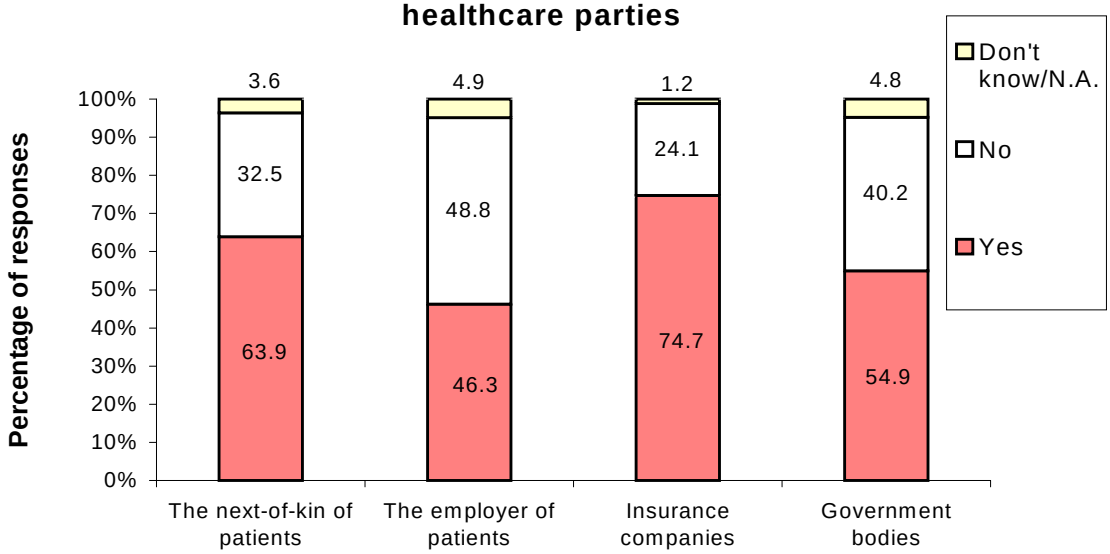
Among respondent organizations in this sector the percentages indicating the transfer of patients' personal data to hospitals or clinics which belonged to the same organization (52.4%) were significantly higher than to a different organization e.g. "other clinics": 30.5%, and "other hospitals" 26.8% (Figure 1).

Figure 1 - The transfer of patient's personal data to healthcare organizations



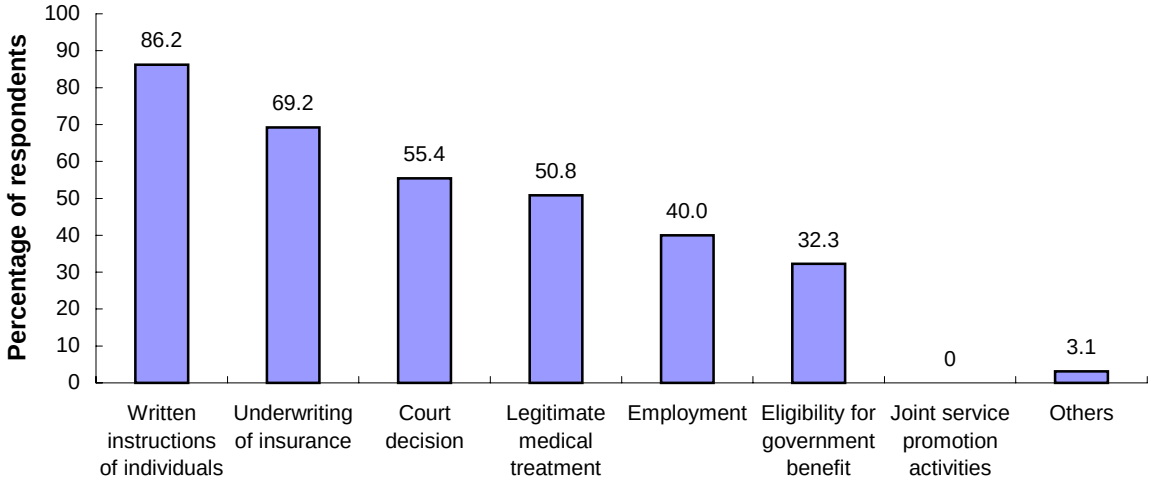
Healthcare organizations transferred patients' personal data to non-healthcare parties, more often than healthcare parties (Figure 2). The percentages were the highest to insurance companies (74.7%) and the lowest to employers of patients (46.3%)

Figure 2 - The transfer of patients' personal data to non-healthcare parties



On the "written instructions of individuals" (86.2%) and "underwriting of insurance" (69.2%) were the two most important reasons for the transfer to non-healthcare parties (Figure 3).

Figure 3 - Reasons for the transfer of patients' personal data to non-healthcare parties



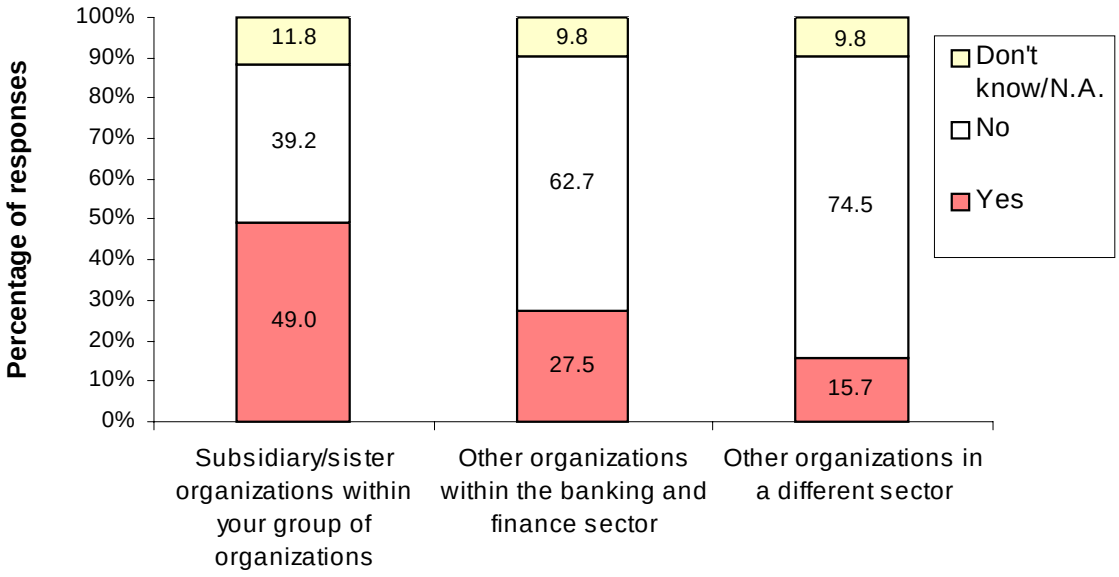
Personal Data Privacy Practices in the Banking and Finance Sector

1 Practices relating to the Transfer of Personal Data

A total of 100 organizations were sampled in the banking and finance sector of which 51 filed a usable return giving a response rate of 51%.

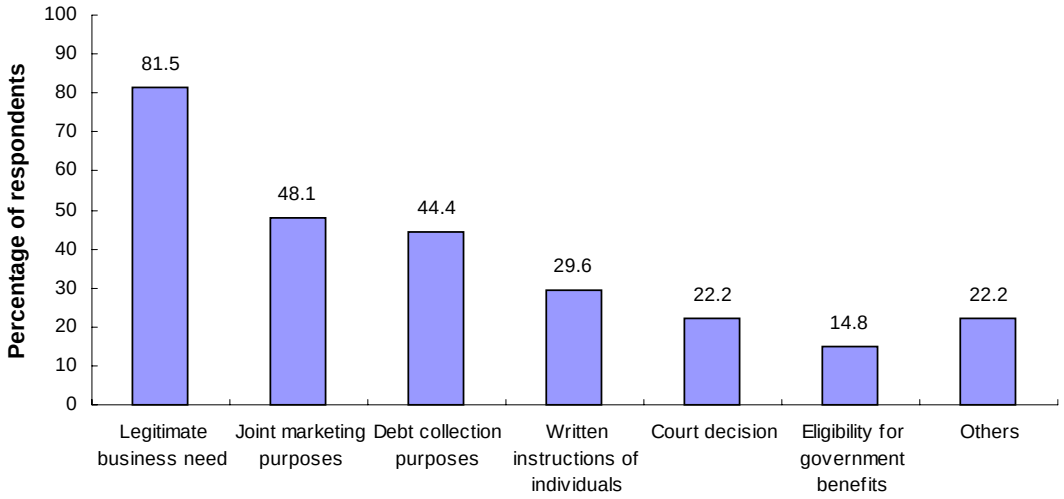
49% of respondent organizations in the banking and finance sector transferred clients' personal data to subsidiary/sister companies. The percentages transferring personal data to other organizations within the same sector, or in a different sector, were much smaller (Figure 4).

Figure 4 - The transfer of clients' personal data



"Legitimate business needs" were reported as a very important factor in transferring clients' personal data (81.5%). Less than half of respondent organizations indicated "joint marketing purposes" and "debt collection purposes" as the reasons for personal data transfer (Figure 5).

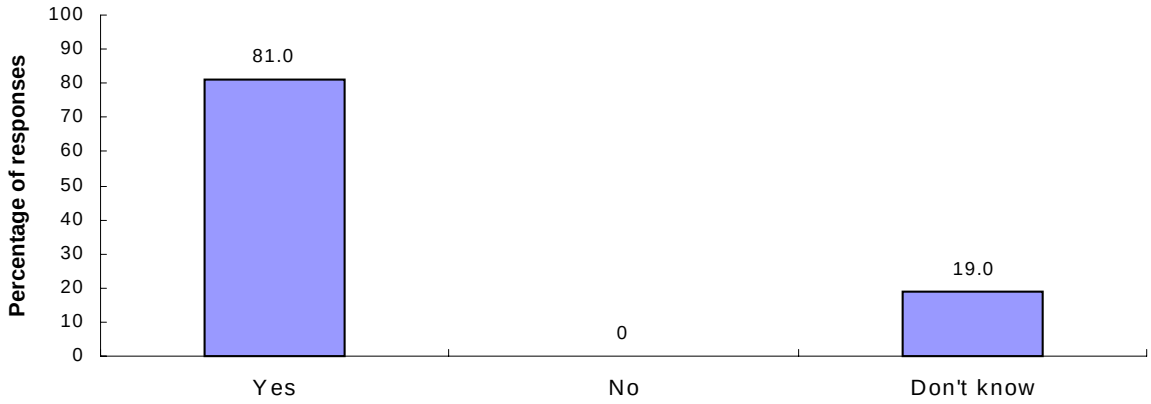
Figure 5 - Reasons for the transfer of clients' personal data



2 Practices relating to Debt Collection

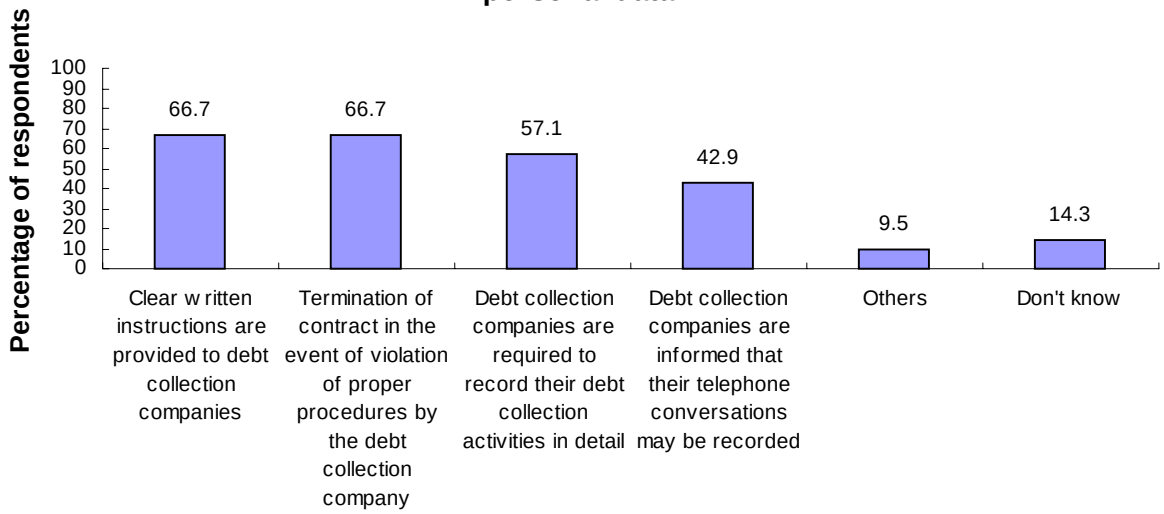
58.8% of respondent organizations in the banking and finance sector did not employ debt collection companies. A very high proportion of those employing debt collection companies (81%) notified individuals of the possibility that their personal data might be supplied to debt collectors (Figure 6).

Figure 6 - Individuals notified of the possibility that their personal data may be supplied to a debt collection company for debt recovery



"Provision of clear written instructions (66.7%) and "termination of contract" (66.7%) were the most popular methods of ensuring that debt collectors complied with instructions regarding the proper use of clients data. 57.1% required debt collection companies to keep a record of their

Figure 7 - How do you ensure that debt collection companies comply with instructions regarding the proper use of clients' personal data?

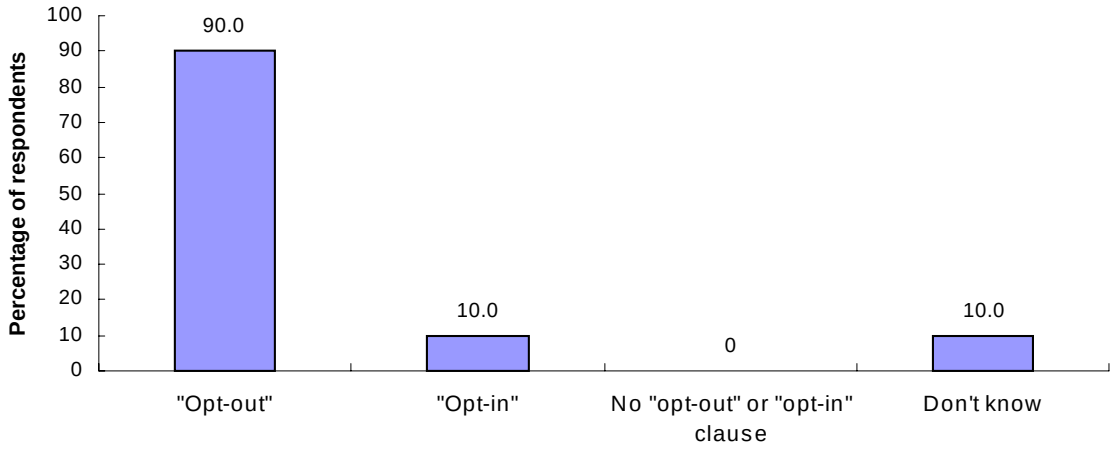


activities (Figure 7).

3 Practices Relating to Direct Marketing

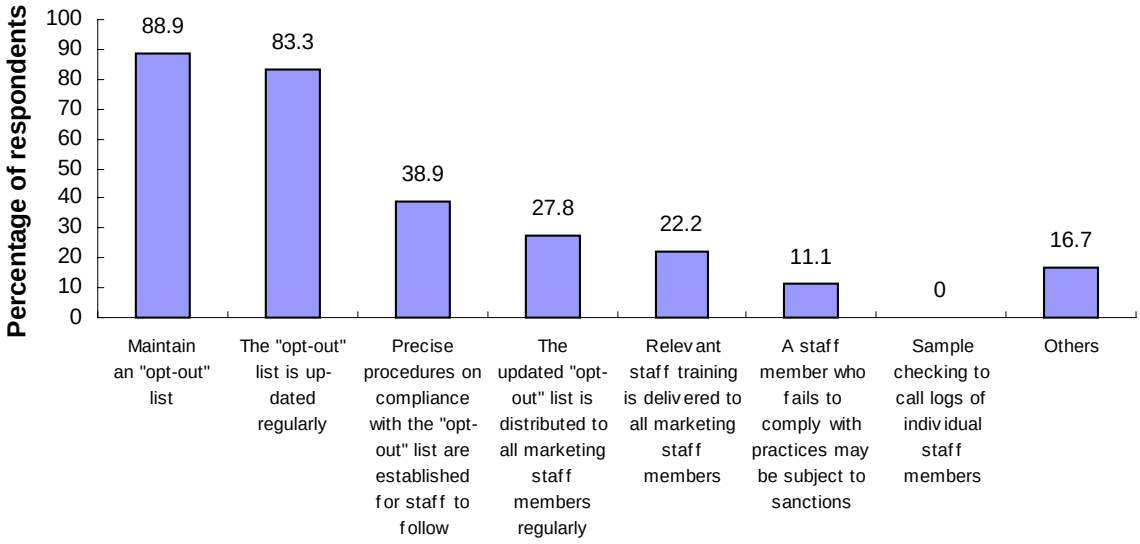
51% of respondent organizations in the banking and finance sector did not engage in direct marketing, and 9.8% did not use personal data for direct marketing. 90% of those using personal data for direct marketing provided an "opt out" clause. Only 10% offered an "opt-in" clause (Figure 8).

Figure 8 - Options provided in connection with direct marketing



All companies which offered an “opt-out” clause indicated that they had a system to ensure that their staff knew whether a client had already refused to receive direct marketing materials. As illustrated in Figure 9, of those claiming that they had such a system, 88.9% maintained an “opt-out” list, and 83.3% indicated that ‘the “opt-out” list was up-dated regularly’.

Figure 9 - Mechanisms to ensure that those who opt-out have their wishes respected



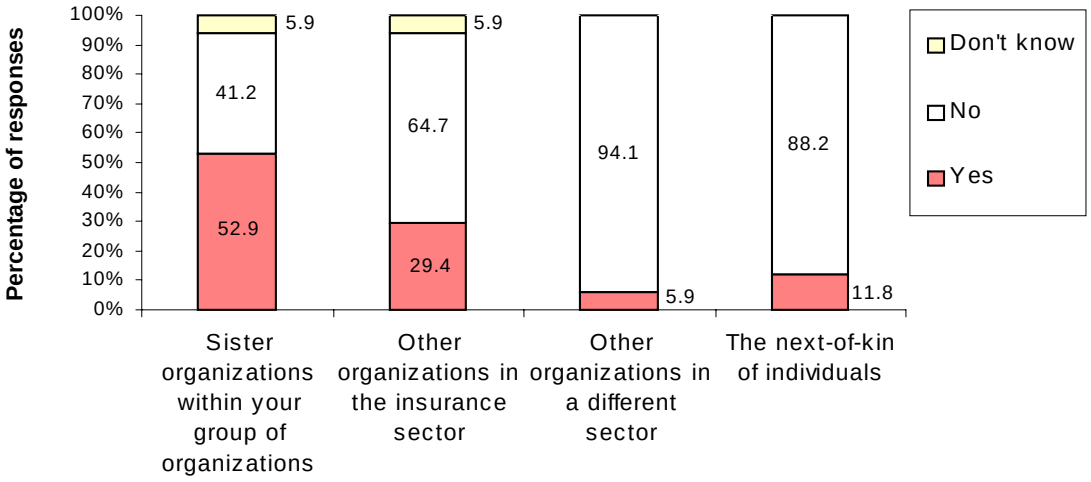
Personal Data Privacy Practices in the Insurance Sector

1 Practices Relating to the Transfer of Personal Data

A total of 41 organizations were sampled in the insurance sector of which 17 filed a usable return giving a response rate of 41.4%.

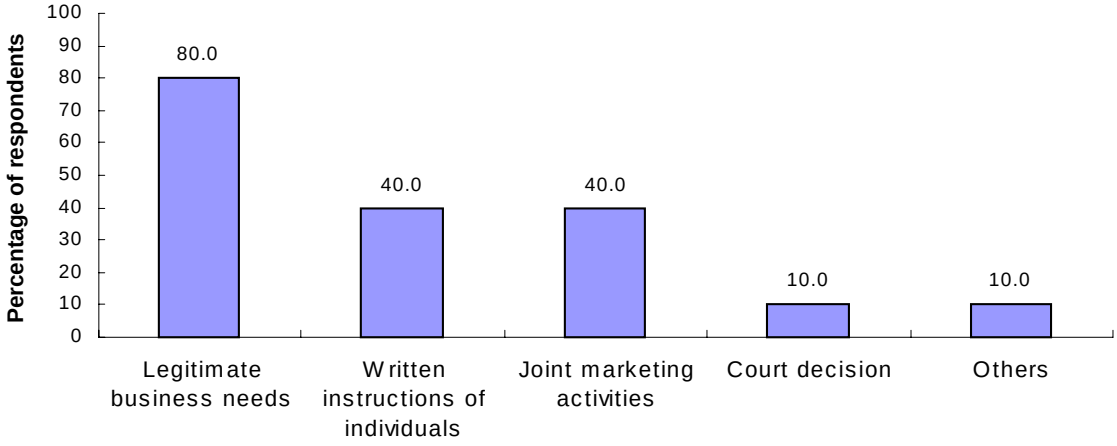
Approximately half of the respondent organizations in the insurance sector (52.9%) transferred clients' data to sister organizations. The percentage figures for transferring personal data to other parties were much lower (Figure 10).

Figure 10 - The transfer of clients' personal data



Many respondent organizations (80%) indicated "legitimate business needs" as a reason for the transfer. Other reasons were less frequently cited (Figure 11).

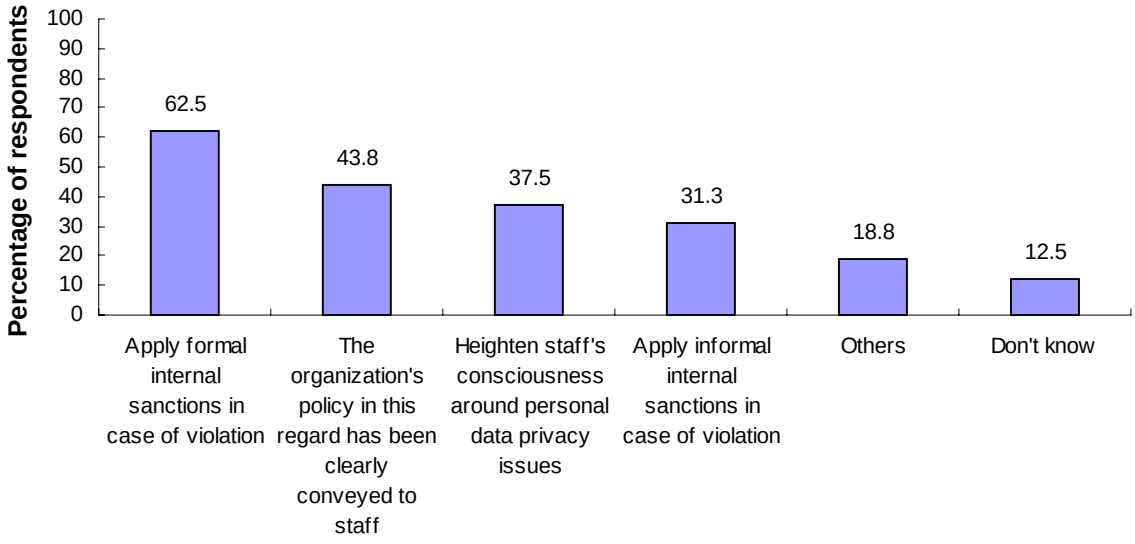
Figure 11 - Reasons for the transfer of clients' personal data



2 Practices Relating to Insurance Policies

There have been occasions when some insurance agents have covered the initial cost of insurance policies for potential clients, without the consent of the latter, for the purpose of meeting a sales quota. In such circumstances 62.5% of respondent organizations indicated that they would apply formal sanctions if this happened (Figure 12).

Figure 12 - Procedures for the prevention of malpractice



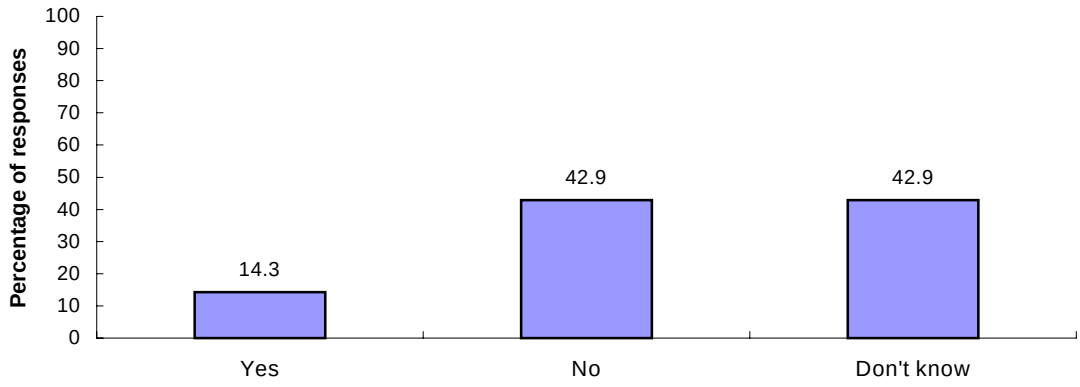
Personal Data Privacy Practices in the Real Estate Sector

1 Practices Relating to Debt Collection

A total of 31 organizations were sampled in the real estate sector of which 12 filed a usable return giving a response rate of 38.7%.

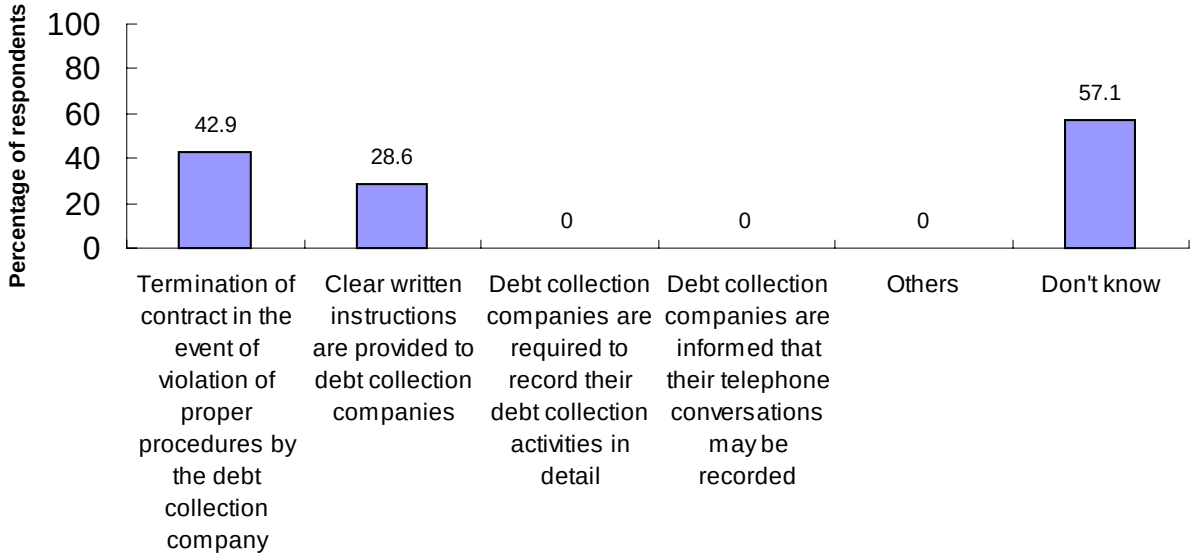
41.7% of respondent organizations in the real estate sector did not employ debt collection companies. Among those employing debt collectors, 42.9% clearly indicated they did not notify individuals of the possibility that their personal data might be supplied to a debt collection company (Figure 13).

Figure 13 - Are individuals notified of the possiblity that their personal data may be supplied to a debt collection company for the recovery of outstanding debts?



More than half the respondent organizations (57.1%) indicated that they did not know of the methods adopted to ensure that debt collectors complied with instructions regarding the proper use of clients' personal data (Figure 14). "Termination of contract" was the most frequently mentioned method (42.9%).

Figure 14 - How do you ensure that debt collection companies comply with instructions regarding the proper use of clients' personal data?



2 Practices Relating to Direct Marketing

Only one respondent organization used personal data for direct marketing, and provided "opt-out" and "opt-in" clauses to individuals. They had a system to ensure their staff knew whether a client had already refused to receive direct marketing materials. The mechanisms included, 'maintain an "opt-out" list', 'the "opt-out' list is updated regularly', and "precise procedures on compliance with the "opt out" list are established for staff to follow'.

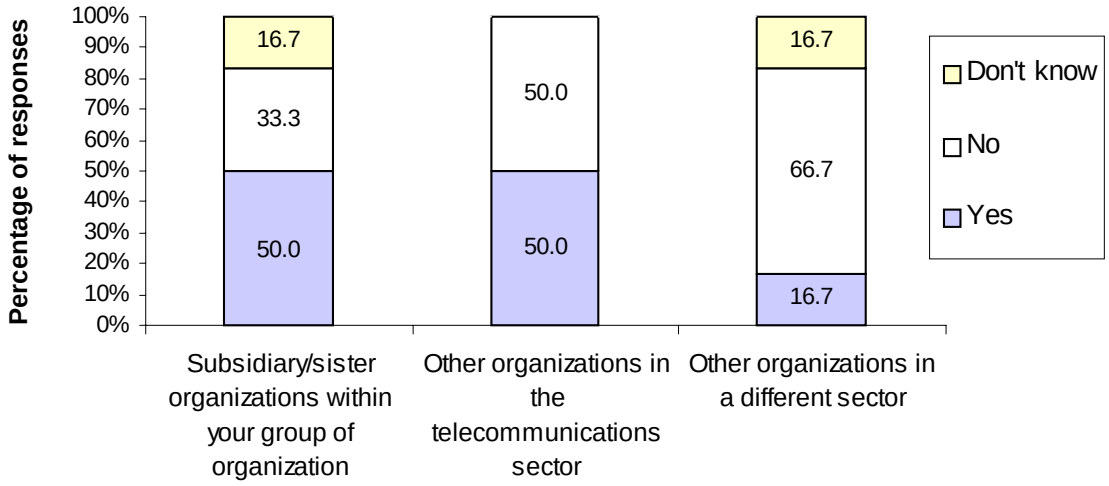
Personal Data Privacy Practices in the Telecommunications Sector

1 Practices Relating to the Transfer of personal Data

A total of 10 organizations were sampled in the telecommunications sector of which 6 filed a usable return giving a response rate of 60%.

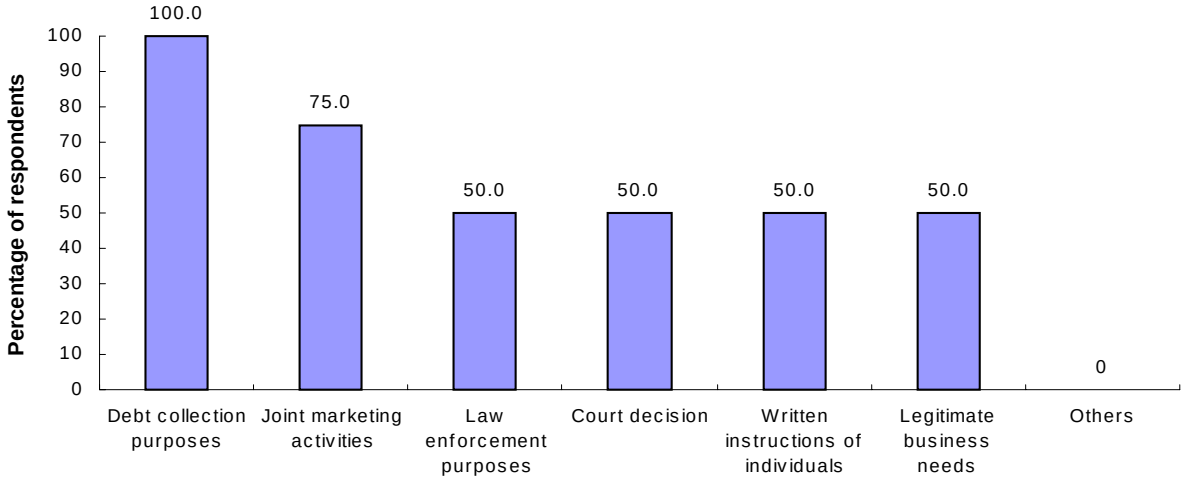
The percentage indicating the transfer of clients' personal data to subsidiary or sister organizations, and other organizations in the telecommunications sector, were both 50% (Figure 15).

Figure 15 - The transfer of clients' personal data



All respondent organizations in the telecommunications sector considered “debt collection” a reason for transfer. 75% made mention of “joint marketing activities” (Figure 16).

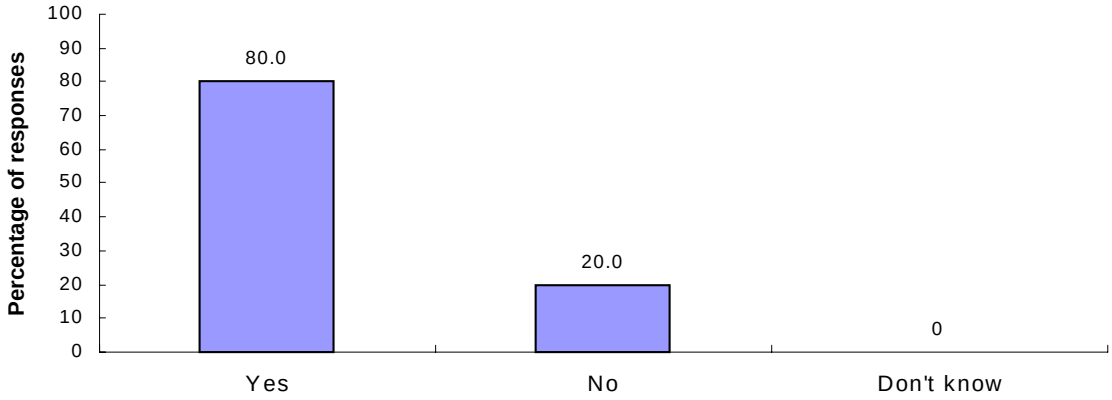
Figure 16 - Reasons for the transfer of clients' personal data



2 Practices Relating to Debt Collection

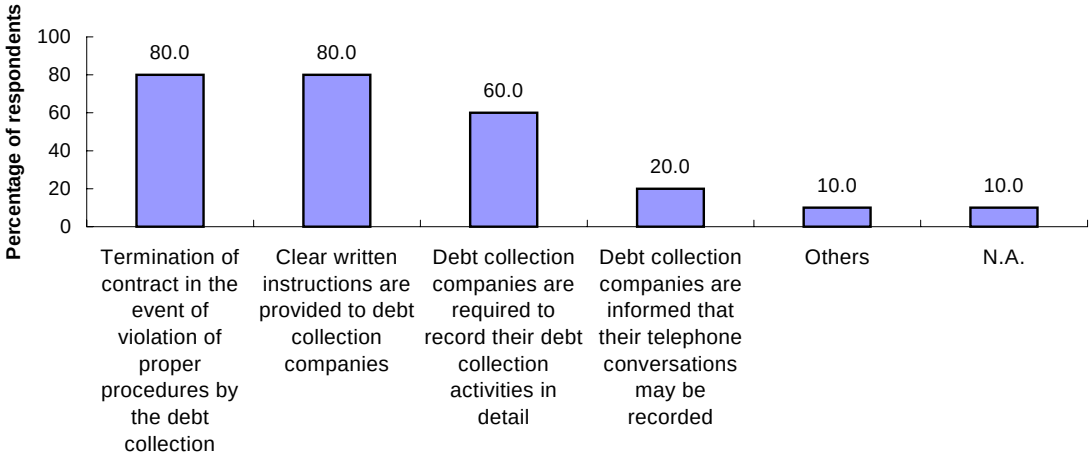
Only 16.7% of respondent organizations did not employ debt collection companies. Among those employing debt collection companies, 80% notified individuals of the possibility that their personal data might be supplied to a debt collector (Figure 17).

Figure 17 - Are individuals notified of the possibility that their personal data may be supplied to a debt collection company for the recovery of outstanding debts?



"Termination of contract" and "clear written instructions" were the most frequently mentioned methods of ensuring that debt collection companies complied with instructions regarding the proper use of clients' personal data (Figure 18).

Figure 18 - How do you ensure that debt collection companies comply with instructions regarding the proper use of clients' personal data?



3 Practices Relating to the Monitoring of Agents

66.7% or respondent organizations employed agents to recruit customers. All of them indicated that they would terminate the contract in the event of a violation of proper procedures by the agent. 75% claimed that "all clients' application forms should be returned to headquarters" (Figure 19).

Figure 19 - How do you ensure that any agent you may employ handles clients' data properly?