

Legislative Council Panel on Constitutional Affairs

Report on the Work
of the Office of the Privacy Commissioner for Personal Data in 2014

Members were briefed annually at the meeting of the Legislative Council Panel on Constitutional Affairs on 15 November 2010, 16 May 2011, 19 March 2012, 21 January 2013 and 17 March 2014 by the incumbent Privacy Commissioner for Personal Data (“**the Commissioner**”) on the accomplishments of his office (“**PCPD**”). This paper serves to update Members of PCPD’s work in 2014.

Enquiries

2. In 2014, the PCPD received a total of 17,328 enquiries, representing a decrease of 28% compared with the figure of 24,161 for 2013. They were mainly concerned with data access requests (11.9%), the use of personal data in direct marketing (11.1%), employment (11.1%), CCTV/video/voice recording (5.9%) and collection / use of Hong Kong identity card numbers or copies (5.2%).

3. There was a sharp increase of 44% in internet related enquiries from 425 cases in 2013 to 611 cases in 2014. They were mainly concerned with cyber-profiling, excessive collection of personal data and cyber-bullying.

Response to Consultations

4. During the year, PCPD provided detailed comments in response to consultations from various government bureaux and departments covering a wide range of subjects, and made submissions on various proposed legislative and administrative measures that have an impact on personal data privacy. Details are set out in **Annex A**.

Electronic Health Record Sharing System Bill

5. In particular, the PCPD took an active part in the deliberations of the Bills Committee on the Electronic Health Record Sharing System Bill as they relate to privacy and data protection. Among other issues, the following major concerns were raised:-

- (a) healthcare professionals should only access health records of a patient on a strictly “need-to-know” basis;
- (b) the need to provide a “safe deposit box” that allows the separate storage of certain particularly sensitive health data (such as psychiatric diseases/mental conditions or hereditary diseases) with enhanced access control by the patient;
- (c) the unreasonable denial of a patient to authorise a representative in writing to exercise his data access and correction rights in respect of his health data kept in the system;
- (d) the unduly wide discretion of the Electronic Health Record Commissioner in allowing registration under the system of bodies who “directly or indirectly provide healthcare” and government bureau or department that “involves providing healthcare”;
- (e) the unacceptable arrangement to relieve the Electronic Health Record Commissioner from the legal obligation to inspect the information systems used by the healthcare providers participating in the system; and
- (f) the need to introduce offences such as civil penalties for unauthorised access of electronic health records by means other than the use of computer and for unauthorised use of the data other than direct marketing.

The Government has agreed to make amendments to the Bill to address all these concerns except the last item.

Complaints

6. In 2014, the PCPD received a total of 1,702 complaints, which represented a slight decrease of 5% compared with the record high figure of 1,792 for 2013.

7. Of the complaints received, 74% were made against the private sector (1,264 cases), 10% against the public sector/government departments (176 cases) and 16% against individuals (262 cases).

8. Among the private sector organisations, the sector which received the most complaints was the financial sector (288 cases), followed by property management (119 cases) and telecommunications (98 cases).

9. As regards the nature of the complaints, 41% of the 1,702 complaints received concerned the use of personal data without the consent of data subjects (694 cases), 37% were about the purpose and manner of data collection (633 cases), 12% were related to data security (197 cases) and 6% were about data access/correction requests (112 cases).

Complaints Related to Direct Marketing

10. The number of direct marketing-related privacy complaints received dropped by 49% from the record high of 538 cases in 2013 to 277 cases in 2014.

11. In a survey commissioned by the PCPD in March 2014, it was revealed that unsolicited direct marketing calls were prevalent and 55% of the respondents reported that more than 40% of calls received by them involved the use of personal data.

12. In some cases involving offer of personal loans, the calls in question were purportedly made by some banks but upon investigation, the banks denied having authorised their staff to make the calls, and other lending institutions as well as intermediaries were identified to have been involved. In many such cases, the calls were made outside Hong Kong using 8-digit numbers assigned by the Office of the Communications Authority (“**OFCA**”) from the numbering plan of Hong Kong, with ‘2’ or ‘3’ as the prefix. Calls made outside Hong Kong have caused difficulties in identifying the Hong Kong companies ultimately responsible for the calls, against which charges of contraventions of the provisions of the Personal Data (Privacy) Ordinance (“**Ordinance**”) may be brought. The difficulties are compounded by the callers' practice to change their numbers on a frequent basis.

13. A multi-pronged approach is required to tackle these problems. In this regard, the Commissioner has appealed to the Secretary for Commerce and Economic Development for the expansion of the Do-not-call registers presently administered by the OFCA to include person-to-person calls. This could be arranged expeditiously by way of an amendment notice published in the Gazette under section 7 of the Unsolicited Electronic Messages Ordinance. Compared with the provisions of the Ordinance which serve as remedy after the fact, the expanded register will provide a preventative one-stop-shop that enables the consumer to opt out of all unwanted telemarketing calls at one go

and at the outset. Further, the PCPD has been working with the Department of Justice and the Police to address the difficulties in criminal investigation caused by calls made outside Hong Kong.

Complaints Related to Use of ICT

14. In line with the large increase in the number of ICT-related enquiries, ICT-related privacy complaints are also on the rise – an increase of 122% from 93 cases in 2013 to 206 cases in 2014.

15. This rising trend is principally attributable to the increasing popularity of smartphones and the prevalent use of the Internet among netizens. Common privacy disputes arose from the use of mobile apps and social networking websites (157 cases), the disclosure or leakage of personal data on the Internet (57 cases), and cyber-bullying (34 cases). **Annex B** is a breakdown of these figures for the past three years.

Compliance Checks and Self-initiated Investigations

16. 70 data breach incidents were brought to light in 2014 (compared with 61 incidents in 2013), affecting 47,000 individuals. The nature of these incidents ranged from unauthorised disclosure of personal data through hacking to inadvertent circulation of lists of personal data to unrelated third parties.

17. With a view to promoting compliance with the requirements under the Ordinance, the PCPD completed 217 compliance checks and 102 self-initiated investigations in 2014, compared with 208 checks and 19 investigations in 2013.

Inspections

18. The PCPD conducted inspections on the Student Financial Assistance Agency's personal data system in respect of four of its financial assistance schemes, and on the Labour Department's personal data system in respect of its employment services. The inspections identified no major problems but there were areas for improvement and recommendations for tightening personal data protection have been made for the two organisations to follow up.

Investigation Reports

19. The Commissioner published 5 investigation reports in 2014 (compared with 6 published reports in 2013). These reports covered:-

- (a) 71 “blind” recruitment advertisements placed in seven major advertising platforms soliciting personal data of job applicants but without revealing the employers’ identities;
- (b) unnecessary collection by six tutorial service agency websites of the private tutors’ Hong Kong identity card numbers and the personal particulars of their contact persons;
- (c) posting on the websites of 10 major employment agencies for domestic helpers of the personal data of overseas job applicants, members of their families and their past employers (including Hong Kong employers), which served no useful purpose for employee screening by prospective employers;
- (d) excessive collection of personal data by two travel agencies from customers when they enrolled for the agencies’ loyalty programme and when making enquiries about the reward points under the programme using the mobile application developed by the agencies; and failure to explain to the application users the purpose of use of the personal data collected; and
- (e) leakage of personal data of the customers of an airline services company through a mobile application running on iOS platform as a result of the failure of the application maintenance contractor in responding to the introduction of a new privacy protection feature on iOS7.

20. The publication of these reports, which received widespread media coverage and entailed serious public discussion, has served to invoke the sanction and discipline of public scrutiny and discourage non-compliant behaviour on the part of the organisations involved in the investigations as well as other organisations facing similar data-protection issues. The effect is particularly pronounced with the adoption since June 2011 of a policy of naming the organisation responsible for the privacy breach. As **Annex C** shows, the number of such reports published in the past five years has increased drastically compared with the past.

Enforcement Action

21. In 2014, the PCPD issued 20 warnings and 90 enforcement notices to organisations, compared with 32 warnings and 25 enforcement notices in 2013. 69 of the enforcement notices were served in connection with the investigation of “blind” recruitment advertisements.

Prosecution

22. The number of cases referred to the Police for criminal investigation and consideration of prosecution in 2014 was the same as in 2013, namely, 20. Of these, 17 cases were related to suspected contraventions involving the use of personal data in direct marketing.

23. Only one conviction was recorded in 2014. This involved an insurance agent’s contravention of section 50B(1)(c)(i) under the Ordinance by making false statements to the Commissioner during an investigation into his misleading the complainant as regards the identity of the issuer of the insurance policy to be sold to the complainant. Together with convictions under other charges, the accused was sentenced to 4 weeks’ imprisonment. Since the Ordinance came into force in 1996, this is the first conviction for misleading the Commissioner in discharging his statutory functions and the first conviction with a custodial sentence.

Legal Assistance Scheme

24. The Legal Assistance Scheme commenced on 1 April 2013 under the Amendment Ordinance. Under the scheme, the PCPD may provide assistance to a person who has suffered damage by reason of a contravention under the Ordinance and intends to institute proceedings to seek compensation from the organisation at fault. The PCPD received in 2014 seven new applications for legal assistance, on top of eight applications brought forward from 2013. Of these applications, one has been granted assistance, nine were rejected, two were withdrawn by the applicants and three are being considered.

Privacy Management Programmes

25. The Commissioner has recognised that privacy and data protection in this era of Big Data and rising public expectation cannot be managed effectively if they are merely treated as a legal compliance issue. It has

advocated that organisations should embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation. This entails the adoption of holistic and encompassing privacy management programmes that ensure robust privacy policies and procedures are in place and implemented for all business practices, operational processes, product and service design, physical architectures and networked infrastructure.

26. In 2014, the Government, together with 25 companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, all pledged to implement privacy management programmes. The Hong Kong Association of Banks also indicated that the banking industry supports the initiative.

Regulating Cross-border Flows of Personal Data

27. Section 33 of the Ordinance provides a very stringent and comprehensive regulation of the transfer of data outside Hong Kong. It expressly prohibits all transfers of personal data ‘to a place outside Hong Kong’ except in specified circumstances such as:-

- (a) the place is specified by the Commissioner as one which has in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance; and
- (b) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be handled in a manner tantamount to a contravention of a requirement under the Ordinance.

However, section 33 has not been brought into force since its enactment in 1995. Hence the current protection for personal data transferred to overseas jurisdictions is weak and far from comprehensive.

28. To encourage the Government to have a renewed focus on section 33 of the Ordinance so that the international status of Hong Kong as a financial centre and a data hub will be preserved, the PCPD has completed in 2013 a survey of 50 jurisdictions and come up with a white list of places which has in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance. A copy of the report has been forwarded to the Government.

29. Further to this initiative, the PCPD has in 2014 published a Guidance which assists organisations to prepare for the eventual implementation of section 33 and enhance privacy protection for cross-border data transfer. In particular, the Guidance contains a set of recommended model data transfer clauses to assist organisations in developing their cross-border data transfer agreement with the overseas data recipients. Organisations are encouraged to adopt the practices recommended in the Guidance as part of their corporate governance responsibility before section 33 comes into operation.

Promotion and Public Education

30. During the year, a total of 20 promotional and education activities were organised with over 140,000 participants (compared with 16 activities and 58,979 participants in 2013). In particular, the “Privacy Campaign for the Retail Industry” was satisfactorily completed, with the intensive participation of 1,295 practitioners from over 180 organisations and the launch of a new online assessment tool tailor-made for the industry. As in previous years, the University Privacy Campaign was held, attracting participation of 35,000 staff and students from the 10 local universities. Further, the “Student Ambassador for Privacy Protection Programme” continued, with participation increased by 57% from 4,840 students in 2013 to 7,593 students in 2014.

31. A total of 245 seminars and workshops were conducted, with a total attendance of 14,845 reaching over 300 organisations. Digital privacy issues remained a major focus of the year, with a new seminar entitled “Developing Mobile Apps with Privacy Protection in Mind” launched to target app developers.

32. Guidance notes and information leaflets issued in 2014 included: (1) Privacy Implications for Organisational Use of Social Network, (2) Guidance for the Banking Industry on the Handling of Customers’ Personal Data, (3) What you need to know about cyber-bullying, (4) Best Practice Guide for Mobile Applications Development, and (5) Guidance on Personal Data Protection in Cross-border Data Transfer.

33. The PCPD website was revamped in 2014 to provide a one-stop portal on privacy protection matters. It has become an increasingly important channel for the PCPD to reach out to the community with its growing wealth of privacy information. It received an average of over 55,000 visits per month.

34. The Data Protection Officers Club has grown in membership, reaching 557 in 2014, an increase of 60% over the preceding year.

35. **Annex D** shows in quantitative terms the stepped-up efforts in promotion and public education in the past five years.

Enhancement of Operational Efficiency

36. **Annex E** also shows that the PCPD has enhanced its operational efficiency in the past 5 years when the complaint intake has been on a rising trend, with 1,001 cases in 2009, increased to 1,486 cases in 2011, reached a peak of 1,792 cases in 2013 and levelled off at 1,702 cases in 2014. In brief,

- (a) the total number of complaint cases closed had increased from 1,076 in 2010 to 1,774 in 2014, in line with the increase in headcount over the same period;
- (b) the percentage of complaint cases closed within 180 days has increased from below 90% in the past 3 years to 95% in 2014;
- (c) the average time taken to conclude simple and complicated cases has shortened from 44 and 148 days respectively in 2010 to 30 and 122 days respectively in 2014; and
- (d) the 2014 year-end complaint backlog hit a historical low of 280 cases compared with the figures for past years.

Removal of Statutory Time Limit to Serve Notice to Refuse Investigation

37. Under section 39(3) of the Ordinance, if the PCPD decides not to initiate a formal investigation after enquiries into a complaint, he has to notify the complainant within 45 days after receiving the complaint. The rationale for imposing this requirement cannot be traced. The Equal Opportunities Commission and the Ombudsman, as well as overseas national privacy authorities, are not subject to such statutory time limit.

38. Currently, upon receipt of a complaint, the PCPD will first determine whether there is a prima facie case of breach of the Ordinance. If affirmative, a formal investigation will commence leading to a determination on whether there is a contravention against the provisions of the Ordinance and where necessary, enforcement action. The establishment or otherwise of a prima facie case involves enquiries with both the complainant and very often the party

complained against. This could be an iterative and time-consuming process dependent on the response of the parties involved. It is not always possible to reach a conclusion within 45 days.

39. In other words, in order to fully satisfy the statutory requirement, some decisions on whether or not to launch a formal investigation will have to be made prematurely. This is not conducive to the fair and effective handling of complaints. For example, as the onus to provide evidence to substantiate a prima facie contravention is on the complainant, the likely decision of the PCPD would be not to proceed with formal investigation in the event of lack of sufficient evidence when the 45-day time limit is due. Alternatively, if the PCPD had chosen to undertake formal investigation prematurely, both the PCPD and the party complained against could be unduly burdened because formal investigation requires a much heavier commitment of time and resources. Either way, the chances of resolving the dispute between the two parties by conciliation (which might be a better alternative for both of them), could be reduced.

40. Accordingly, the PCPD has refrained from a mechanical adherence to the 45-day time frame. Instead, it has been stepping efforts to enhance operational efficiency and attained a high percentage of compliance of the 45-day requirement, albeit short of 100%. The achievements for the past five years are indicated in **Annex E**. Against a performance pledge of 75% compliance which took effect from 1 July 2014, the PCPD achieved 77% compliance for the full year 2014. The pledge for 2015 has been raised to 80% compliance.

41. To ward off any legal or administrative challenge against the PCPD for non-compliance with the statutory time limit, the Commissioner considers that it is necessary to remove the requirement from the Ordinance and for this purpose, has made a submission to the Government. The Government has agreed to proceed with the necessary legislative amendment.

Strategic Focus for 2015

42. The PCPD will continue to face the privacy and data protection challenges by stepping up efforts in enforcement as well as public education. There will be a special focus on:-

- (a) the privacy and data protection issues associated with the prevalent use of mobile apps;
- (b) a survey on the public perception of the PCPD and various topical privacy issues;
- (c) a survey on the protection of personal data contained in public registers maintained by the Government;
- (d) assisting the Government and the private sector in administering privacy management programmes; and
- (e) assisting the Bills Committee in the deliberations of the Electronic Health Record Sharing System Bill as they relate to privacy and data protection.

Office of the Privacy Commissioner for Personal Data
9 February 2015

Responses to Consultations / Vetting of Bills in 2014

PCPD examined a total of 76 bills and regulations published in the Government Gazette and provided comments on the following Bills from the perspective of personal data privacy protection.

- (1) Toys & Children's Products Safety (Additional Safety Standards or Requirements) Regulation
- (2) Marriage (Amendment) Bill 2014
- (3) United Nations Sanctions (Liberia) Regulation 2014
- (4) Pharmacy and Poisons (Amendment) Bill 2014
- (5) United Nations Sanctions (Central African Republic) Regulation
- (6) United Nations Sanctions (Democratic Republic of the Congo) Regulation 2014
- (7) Electoral Legislation (Miscellaneous Amendments) Bill 2014
- (8) Competition (Amendment) Bill 2014
- (9) United Nations Sanctions (Yemen) Regulation
- (10) Electronic Health Record Sharing System Bill
- (11) Property Management Services Bill
- (12) Veterinary Surgeons Registration (Amendment) Bill 2014
- (13) Insurance Companies (Amendment) Bill 2014
- (14) Private Columbaria Bill
- (15) Mandatory Provident Fund Schemes (Amendment) Bill 2014

PCPD also provided comments in response to 7 proposed legislations and government administrative measures listed as follows:-

- (1) Food and Health Bureau : Privacy issues involved in the development of the Electronic Health Record Sharing System
- (2) Commerce and Economic Development Bureau : Privacy issues involved in preparing the Travel Industry Bill
- (3) Financial Services and The Treasury Bureau : Privacy issues involved in the establishment of the Independent Insurance Authority
- (4) Financial Services and the Treasury Bureau : Consultation conclusions on the legislative proposals on improvement of corporate insolvency law
- (5) Marine Department : Legislative Proposal for Requirement of Installation Automatic Identification System on Large Local Passenger Vessels
- (6) Agriculture, Fisheries and Conservation Department : New Legislation for Implementing the Convention on the Conservation of Antarctic Marine Living Resources
- (7) Hong Kong Police Force: Electronic Ticketing for Traffic Fixed Penalty Tickets

Furthermore, PCPD responded to the following public consultations:-

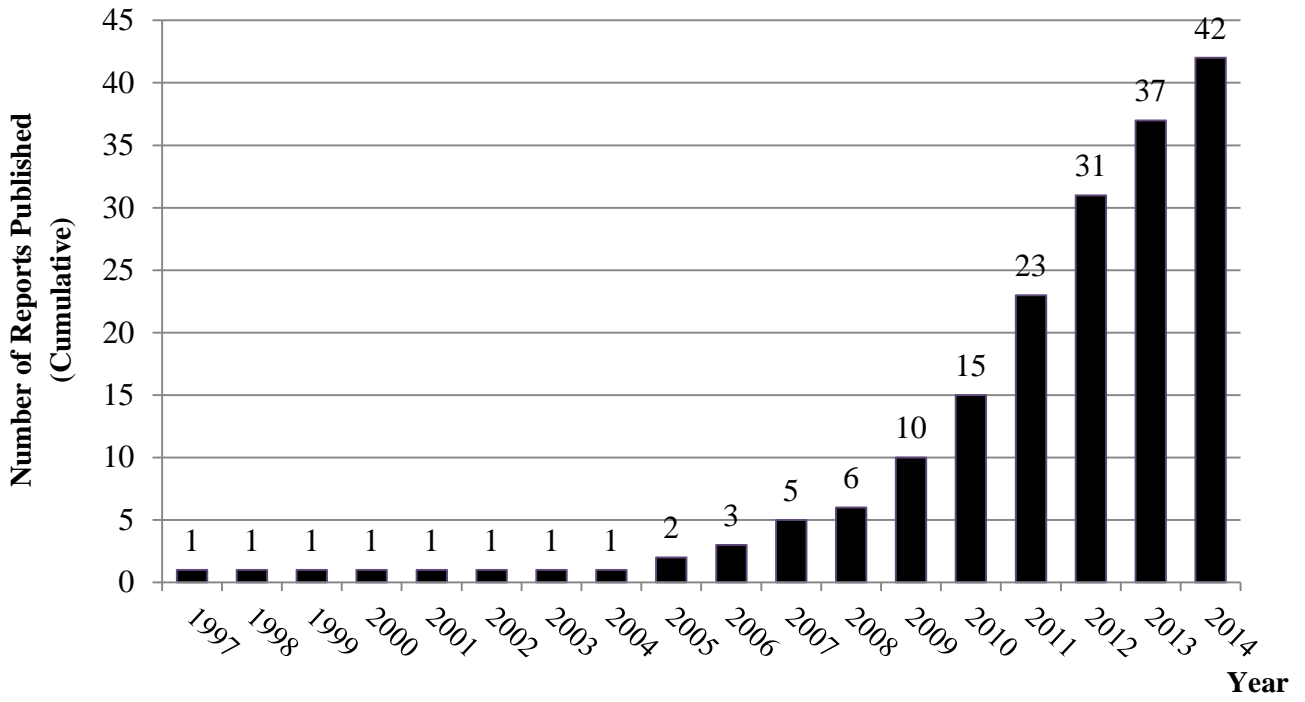
- (1) Public Consultation on RESCUE Drug Testing Scheme
- (2) Interim Report and Consultative Paper on Review of Family Procedure Rules

Privacy Complaints in relation to Use of ICT

Year	Use of social networking websites	Use of smartphone applications	Disclosure or leakage of personal data on Internet	Cyber-bullying	Total*
2012	16	18	12	13	50
2013	45	22	42	6	93
2014	99	58	57	34	206

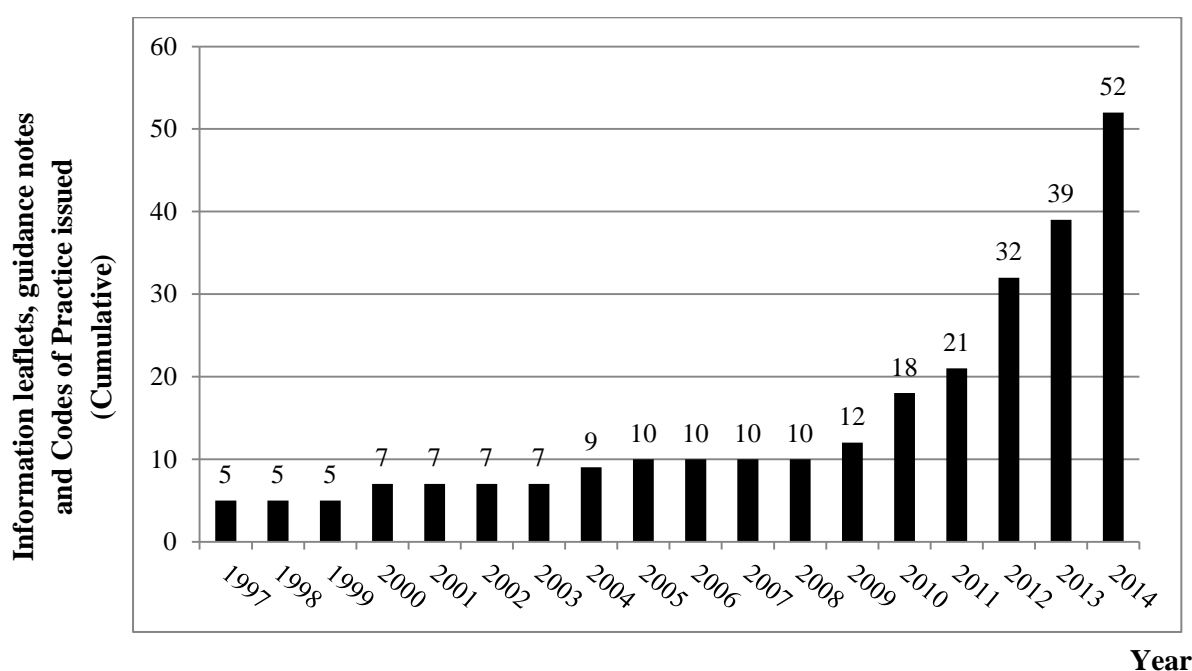
* As a complaint may cut across different categories, figures in the categories added up may exceed the total number of complaints

Publication of Investigation Reports



Promotion and Public Education

	2010	2011	2012	2013	2014
Major Promotional Activities					
- University Privacy Campaign (Participants)	-	2 726	2 570	33 299	35 000
- Student Ambassador for Privacy Protection Programme (Participants)	-	700+	2 000+	4 840	7 593
- Number of Other Activities	26	14	14	14	18
- Total Number of Participants	2 449	17 316	46 657	58 979	141 443
Education					
- Professional Workshops	5	52	71	95	90
- Seminars and Talks	109	212	167	184	155
- Total Number of Participants	8 672	21 141	16 311	20 898	14 845
Industry-specific Campaign (Participants)	2 182	1 158	1 369	1 302	1 018
Data Protection Officers Club (Membership)	362	376	386	357	557
PCPD Websites (Visits per Month)	44 836	39 909	45 192	75 912	55 000
Information leaflets, guidance notes and Codes of Practice issued (Cumulative)	18	21	32	39	52



Annex E**Enhancement of Efficiency in Complaint Handling**

	2010	2011	2012	2013	2014
Complaints received	1 179	1 486	1 213	1 792	1 702
Investigations completed	1 076	1 450	1 268	1 783	1 774
Closing a complaint case within 180 days of receipt (% of cases)	94%	88%	88%	89%	95%
Average time taken to settle a simple complaint case (days)	44	37	39	43	30
Average time taken to settle a complicated complaint case (days)	148	162	219	195	122
Investigations in progress by year-end	362	398	343	352	280
Complaint cases closed within 45 days without commencing formal investigation (% of compliance)	56%	72%	69%	62%	77%