

COMPLIANCE ACTIONS
審查工作

助完善制度 促守法循規
Facilitating the perfection of systems and promoting legal compliance

审查工作

审查工作 Compliance Actions



COMPLIANCE ACTIONS
审查工作

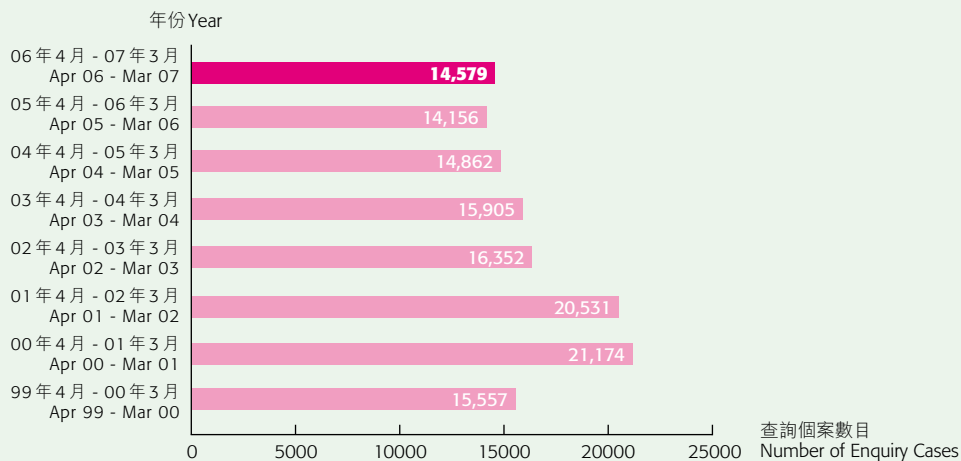
2006-07 年度接獲的查詢 Enquiries Received 2006-2007

在2006-07年度，公署共處理14,579宗查詢個案（較去年上升3%），每日平均處理54宗。查詢的數字上升（儘管百分比輕微），反映公眾對個人資料私隱的意識增加。

A total of 14,579 enquiry cases were handled in 2006-2007 (a 3% increase compared with the previous year). On average, 54 enquiry cases were handled each working day. The slight rise in the number of enquiries reflected the increase in public awareness of personal data privacy.

圖表1 — 每年的查詢個案

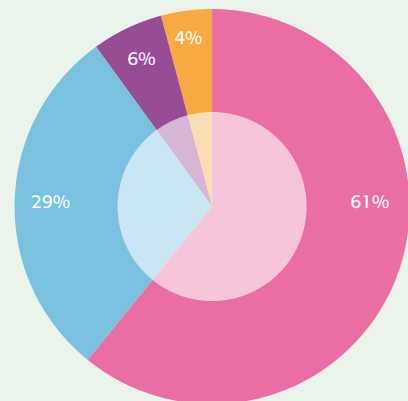
Figure 1 — Annual Enquiry Caseload



圖表2 — 查詢個案的性質

Figure 2 – Nature of Enquiry Cases

個人的私隱權利 Privacy rights of an individual	61%
私隱條例的規定 Requirements of the Ordinance	29%
關於公署的資料 About the PCPD	6%
專員出版的刊物 Publications produced by the Commissioner	4%



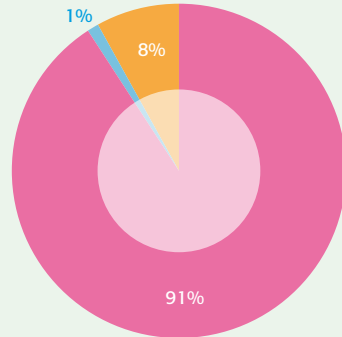
約三分之二的查詢個案（約61%）與個人在個別情況下的私隱權利有關。

Almost two-thirds of the enquiry cases (about 61%) were related to privacy rights specific to an individual's own situation.

圖表 3 — 提出查詢的途徑

Figure 3 – Means by Which Enquiries Were Made

熱線 Hotline	91%
親身查詢 In Person	1%
書面 Written	8%



大部分的查詢個案(約91%)是透過公署的查詢熱線電話(2827 2827)提出的。

The majority of the enquiry cases (about 91%) were made via the PCPD hotline at 2827 2827.

循規查察行動 Compliance Checks

當發現某一機構的行事方式看來有違私隱條例規定時，私隱專員便會展開循規查察行動。在此等情況下，私隱專員會以書面知會有關機構，指出看來與條例規定不符的事宜，並促請有關機構採取適當的糾正措施。

在大多數情況下，有關機構會主動採取即時措施，糾正涉嫌違例事項。在有些情況中，有關機構會就如何採取改善措施，以免重複涉嫌違例事項，向私隱專員尋求意見。在其他情況下，私隱專員會對涉嫌違例事項進行調查，並採取適當的跟進行動，確保有關機構遵從條例的規定(例如，向有關機構發出執行通知，指令它糾正情況)。

在本年報期內，私隱專員共進行了66次循規查察行動，對資料使用者被指違反私隱條例規定的行事方式進行循規查察。

大部分循規查察行動(57次)是與私營機構的行事方式有關，其餘9次則關乎政府部門及法定機構。以下是在年內進行的循規查察行動的一些例子。

A compliance check is undertaken when the Privacy Commissioner identifies a practice in an organization that appears to be inconsistent with the requirements of the Ordinance. In these circumstances, the Privacy Commissioner alerts the organization in writing, pointing out the apparent inconsistency and inviting it, where appropriate, to take remedial actions.

In many cases, the organization takes immediate action to correct the suspected breach. In some instances, advice is sought from the Privacy Commissioner on the measures that should be taken to prevent further breaches. Other times, the Privacy Commissioner would investigate the matter and take action to ensure compliance with the Ordinance. This might include issuing an enforcement notice to the organization directing it to remedy the situation, for example.

During the reporting year, the Privacy Commissioner carried out 66 compliance checks in total in relation to alleged practices of data users that might be inconsistent with the requirements of the Ordinance.

The majority of the compliance checks (57) occurred in the private sector. The remaining 9 related to government departments and statutory bodies. The following examples highlight some of the compliance checks undertaken during the year.



例子 1

Example



一間小學為了記錄出勤情況而以指紋辨識系統收集學生的指紋特徵。

A primary school used fingerprint reader system to collect fingerprint data of its pupils for attendance record purposes.

私隱專員就學校為了記錄出勤情況而以指紋辨識系統收集學生的指紋特徵主動展開調查。

個案中的學生主要介乎6至12歲。在學校經常使用生物辨識系統是非常不當的，因為學生尚未成年，不足以明白提供指紋資料對私隱的不利影響。同時，私隱條例並沒有條文表明可以接受由第三者（例如家長）代表幼童給予訂明同意。

公署進行了調查。私隱專員認為學生並沒有給予真正的通知同意。在考慮到學校的職能或活動，私隱專員認為因記錄出勤情況的行政目的而收集指紋資料並非必要，而且超乎適度。因此，收集學生的有關個人資料是違反私隱條例附表1的保障資料第1(1)原則。

私隱專員向該校送達執行通知，指令它糾正情況。該校其後停止使用指紋辨識系統，並銷毀學生的指紋資料。

A self-initiated investigation was carried out against the school in relation to the use of fingerprint reader system to collect fingerprint characteristics of pupils of the school for attendance record purpose.

The age of the pupils in this case ranged mostly between 6 to 12. The regular use of biometrics in the school was considered to be highly undesirable because the pupils, who were minors of tender age, could not understand the adverse privacy impact on the provision of their fingerprint data. Meanwhile, the Ordinance does not contain provision that accepts the giving of prescribed consent from a third party, e.g. the parents, on behalf of the children.

After an investigation, the Privacy Commissioner was of the opinion that no genuine informed consent was given by the pupils of the school, and the collection of the fingerprint data for the administrative purpose of recording attendance is considered to be unnecessary and excessive having regard to the function or activity of the school. The collection of the personal data of pupils was therefore found to be in contravention of Data Protection Principle 1(1) of Schedule 1 to the Ordinance.

An enforcement notice was served on the school directing it to remedy the situation. Subsequently, the school ceased using the fingerprint reader system and destroyed the fingerprint data of its pupils.

例子 2 Example 2



一間公司要求申請人在面試時提供身分證副本。

A company required job applicants to provide copies of their identity cards during job interviews.

私隱專員聯絡該公司，其管理層承認，在面試時向申請人收集身分證副本是該公司的一貫措施。

The Privacy Commissioner approached the company whose management admitted that it was their established practice to collect the identity card copies from job applicants during job interviews.

該公司在獲悉保障資料第1(1)及1(2)原則的相關規定，以及私隱專員根據私隱條例發出的《身分證號碼及其他身分代號實務守則》第3.1段及《人力資源管理實務守則》第2.2.4段後，立即停止在面試時向申請人收集身分證副本，並銷毀所有之前向落選申請人收集的身分證副本。

After being notified of the relevant requirements under DPP1(1) and DPP1(2), paragraph 3.1 of the Code of Practice on the Identity Card Number and other Personal Identifiers and paragraph 2.2.4 of the Code of Practice on Human Resource Management issued by the Privacy Commissioner under the Ordinance, the company immediately ceased to collect copies of identity card from job applicants at job interviews and destroyed all the identity card copies previously collected from unsuccessful job applicants.





例子 3 Example



部分銀行的顧客雖然在自動櫃員機輸入錯誤的私人密碼，但仍然可以看到他們完整的銀行帳戶號碼。

Customers of some banks could see their full bank account numbers on ATM machine screens even when Personal Identification Numbers (PIN) are incorrectly entered.

本地報章報導，部分銀行的顧客雖然在自動櫃員機輸入錯誤的私人密碼，但仍然可以看到完整的銀行帳戶號碼。

根據公署向銀行查詢的結果，自動櫃員機在核實私人密碼之前，在螢光幕顯示帳戶號碼是系統的標準常規，顧客是不能夠進一步以錯誤的私人密碼進行任何交易的。為了回應公眾的關注，有關銀行確認會遮蓋帳戶號碼的部分數字，以提高自動櫃員機的保安功能。

According to local newspaper reports, customers of some banks could see their full bank account numbers when using ATM machines even if the wrong PIN is entered.

The banks said it was their standard practice to display account numbers on the ATM machine screen before the PIN is verified but that customers cannot continue with any transactions if the PIN is incorrect. To address the public's concerns, the banks stated that certain digits of an account number would be omitted to enhance security when using ATM machines.

資料使用者登記計劃 Data User Registration Scheme

依據私隱條例第IV部，私隱專員有權指明某些類別的資料使用者必須呈交資料使用者申報表，該申報表須載有條例附表3指明的資訊，例如有關資料使用者所持有個人資料的種類及使用目的。條例容許私隱專員酌情決定實施這項規定的規模及時間。

自條例頒布以來，個人資料私隱權利的意識已在社會上紮根。公署接獲的投訴及查詢亦顯示公眾對收集及使用個人資料的機構在責任方面所抱的期望日益增加。

很多私隱或資料保障法例，尤其是在歐盟國家，均包含登記制度，收集、持有及使用個人資料的機構必須向監管機構登記，表明所持有的個人資料的性質，以及述明個人如何行使其權利，例如查閱及改正資料。

公署最近以問卷形式就登記制度的運作向22個歐盟國家進行調查。從歐盟國家的正面經驗，私隱專員認為現在是實施資料使用者登記計劃的時候，該計劃可以令機構採取更開放透明的制度，讓資料當事人得知其個人資料是如何被收集、處理及使用。

2007年5月，公署向香港政府呈交一份討論文件，建議落實資料使用者申報表的條文，並根據條例第14至16條設立資料使用者登記冊，供公眾查閱。

公署現計劃向目標行業進行簡介及諮詢，然後向立法會報告結果，預計這個計劃將於2008年實施。

Pursuant to Part IV of the Ordinance, the Privacy Commissioner has a power to specify classes of data users required to submit data user returns containing information specified in Schedule 3 to the Ordinance, e.g. descriptions of the kinds of personal data held by the data user concerned and the purposes for which they are used. The Ordinance leaves to the discretion of the Privacy Commissioner the scope and timing of the introduction of this requirement.

Since the enactment of the Ordinance, awareness of personal data privacy rights is firmly established in the community. The complaints and enquiries received by the PCPD also indicate an increasing public expectation on the responsibilities of organizations that collect and use their personal data.

Many precedent privacy or data protection laws, particularly in the European Union (“EU”), have included a registration regime whereby organizations collecting, holding and using personal data are required to register with a supervisory authority, declaring the nature of the personal data they hold as well as setting out how individuals can go about exercising their rights such as access and correction.

A survey by way of questionnaires to 22 EU countries on how the registration systems are operated was recently conducted. Learning from the positive experience of the EU countries, the Privacy Commissioner considers that the time is now ripe for the implementation of a Data User Registration Scheme (“DURS”) which will induce organizations to adopt systems that are more open and transparent in informing data subjects on how their personal data are being collected, processed and used.

In May 2007, the PCPD issued a discussion paper to the Hong Kong Government proposing the activation of the provisions of data user returns and a consequential public register of such returns under sections 14 to 16 of the Ordinance.

An exercise is being planned to brief and consult the target sectors and report the outcome to the Legislative Council. It is envisaged that the DURS will be launched in 2008.

私隱循規評估 Privacy Compliance Assessment

私隱循規屬於公司管治的問題。要確保機構的私隱循規架構符合私隱條例規定的標準，以及就機構的私隱循規狀況提供意見，便應該進行私隱循規評估。

2007年3月，私隱專員接受入境事務處（下稱「入境處」）的邀請，以獨立身份對智能身份證系統進行私隱循規評估。該系統是入境處於2003年推出，以取代舊有的人事登記系統。為了確保入境處持有的所有個人資料是按照私隱條例的規定處理，香港政府向立法會承諾，在諮詢私隱專員後制定列明收集、使用及查閱智能身份證資料規則的實務守則，對智能身份證系統進行私隱循規評估，並向立法會提交私隱循規評估報告。

為了減低私隱專員在進行私隱循規評估的身份與他在私隱條例下的規管角色之間的潛在矛盾，雙方制定了諒解備忘錄，以書面明確述明私隱專員作為主管當局的法定權力及其作為商業立約人的雙重身份。

由入境處撰寫的《智能身份證資料實務守則》（下稱「實務守則」）將會是公署進行私隱循規評估的基礎。私隱循規評估完成後，實務守則會加入觀察所得的資料及改善建議，然後由私隱專員按照條例第12條正式核准。

私隱專員預計有關的私隱循規評估將於2008年上半年進行。

Privacy compliance is a corporate governance issue. To ensure that an organization's privacy compliance frameworks satisfy the standards established by the Ordinance, and to provide the organization with an opinion on its privacy compliance status, Privacy Compliance Assessment ("PCA") should be initiated.

In March 2007, the Privacy Commissioner accepted an invitation from the Immigration Department ("ImmD") to act as an independent party to conduct a PCA on the Smart Identity Card System ("SMARTICS"). SMARTICS was implemented by the ImmD in 2003 to supersede the old Registration of Persons System. To ensure that all personal data held by the ImmD are handled in accordance with the provisions of the Ordinance, the Hong Kong Government undertook to the Legislative Council ("LegCo") to draw up a code of practice in consultation with the Privacy Commissioner setting out the rules on the collection, use of and access to smart identity card data, to conduct a PCA on the SMARTICS and to provide a copy of the PCA report to LegCo.

To minimize the potential conflicts between the Privacy Commissioner's role in carrying out the PCA and its regulatory role under the Ordinance, a Memorandum of Understanding has been drawn up so that the Privacy Commissioner's statutory power to act as a competent authority and his dual capacity as a commercial contracting party can be expressly acknowledged in writing.

A Code of Practice on Smart Identity Card Data ("COP") written by the ImmD will form the basis of the PCA to be conducted by the PCPD. At the conclusion of the PCA, any observations and recommendations for improvement will be factored into the COP which can then be formalized and approved by the Privacy Commissioner in accordance with section 12 of the Ordinance.

The Privacy Commissioner expects that the PCA will be carried out in the first half of 2008.

核對程序 Matching Procedures

在本年報期內，私隱專員共收到 11 宗新的核對程序申請，以及 35 宗繼續進行核對程序的重新申請。

所有 11 宗新申請均來自公營機構。經審閱後，其中 2 宗不屬私隱條例釋義所指的核對程序及另外 2 宗其後撤回申請。私隱專員根據私隱條例賦予的權力，在有條件的情況下批准餘下 7 宗申請。35 宗繼續進行核對程序的重新申請中，其中 1 宗不予續批，另外 1 宗撤回申請，其餘 33 宗均獲續批。

During the reporting year, the Privacy Commissioner received 11 new applications for approval to carry out matching procedures and 35 requests for re-approval of matching procedures undertaken in previous years.

All 11 new applications were requested by public sector organizations. Upon examination, 2 were found not to be a matching procedure under the Ordinance, and 2 were withdrawn. The remaining 7 applications were approved subject to conditions imposed by the Privacy Commissioner under the Ordinance. Of the 35 requests for re-approval, 1 was refused and 1 was withdrawn. The remaining 33 were approved.

提出要求者 Requesting Parties	獲准的有關核對程序 Related Matching Procedures that were Approved
破產管理署 Official Receiver's Office	將破產管理署為執行破產條例而收集得的個人資料與入境事務處為出入境事宜而收集得的個人資料作出比較，以識別未能依從破產條例要求而曾經離境的破產人士。 To identify bankrupts who have left Hong Kong without complying with the requirements of the Bankruptcy Ordinance by comparing the personal data collected by Official Receiver's Office for administering the Bankruptcy Ordinance with the personal data collected by the Immigration Department for immigration clearance.
選舉事務處 (2宗申請) Registration and Electoral Office (two requests)	將選舉事務處所收集得的選民個人資料與(1)房屋署及(2)香港房屋協會所收集的資助房屋租戶／業主的個人資料進行比較，以確保選民在適當的選區投票。 To ensure electors to vote in their geographical constituencies corresponding to their up-to-date addresses by comparing personal data of registered electors collected by Registration and Electoral Office with personal data of tenants/owners of subsidized housing collected by (1) the Housing Department; and (2) the Hong Kong Housing Society.
社會福利署 Social Welfare Department	將社會福利署就綜合社會保障援助(以下簡稱「綜援」)申請所收集得的個人資料與勞工處處理紡織及製衣業人力發展計劃的再培訓津貼而收集得的個人資料作出比較，以防止領取綜援人士詐騙或濫用有關的社會保障福利。 To prevent fraud and abuse of social security benefits in relation to retraining allowance for recipients of Comprehensive Social Security Assistance ("CSSA") by comparing the personal data collected by the Social Welfare Department for administering the CSSA scheme with personal data collected by the Labour Department for administering the retraining allowance under the Manpower Development Plan for the textiles and clothing industry.
康樂及文化事務署 Leisure and Cultural Services Department	將康樂及文化事務署所收集得的有過期欠款記錄的圖書館使用者的個人資料與入境事務處人事登記處所持有的個人資料作出比較，以更新該些過期欠款者的地址並進行相關的追討行動。 To update the addresses of library patrons who failed to pay their overdue library fees by comparing the personal data of the library patrons in default with the personal data maintained by the Registration of Persons Office of the Immigration Department, so as to facilitate the Leisure and Cultural Services Department to take recovery actions.
學生資助辦事處 (2宗申請) Student Financial Assistance Agency (two requests)	將學生資助辦事處從學前教育學券計劃申請人所收集得的(1)學生及(2)監護人及其配偶的個人資料與社會福利署從綜援／幼兒中心繳費資助計劃受益人所收集得的個人資料進行比較，以防止有人申領雙重資助。 To prevent double subsidies by comparing the personal data of (1) the students and (2) the guardians and their spouses collected by the Student Financial Assistance Agency from applicants of Pre-primary Education Voucher Scheme with the personal data collected by the Social Welfare Department from the recipients of CSSA/Child Care Centre Fee Assistance Scheme.