



# 協助改善資料系統

HELP IMPROVE DATA SYSTEMS

COMPLIANCE ACTIONS  
審查工作



## 查詢服務 Enquiries Services

在個人資料方面保障個人的私隱應是香港每間機構的標準政策。這不單只是因為條例規定，亦因為可以帶來更佳客戶及僱傭關係、更好的資料質素，以及有效的資料處理。公署致力加強這個訊息，並透過查詢服務，就保障資料的良好行事方式，向公私營機構提供指導及意見。

**The protection of the privacy of the individual in relation to personal data should be a standard policy for every organization in Hong Kong. Not just because of the legal requirements of the Ordinance, but because it leads to benefits in terms of better customer and employment relations, improved data quality and efficiency of data processing. The PCPD strives to reinforce this message and provide guidance on good data protection practices to all public & private organizations, large and small.**

### 例子 Example

1

#### 與香港保安業協會會面 *Meeting with Hong Kong Security Association ("HKSA")*

2009年8月12日，公署高層人員與香港保安業協會行政總裁及六名代表會面，回應該協會就使用生物辨識科技作身份識別及保安用途所提出的關注。會議具成果。私隱專員按該會要求，以書面回覆該協會提出的問題，供該協會會員傳閱參考。

On 12 August 2009, the Commissioner's senior staff met with the Executive Director and six representatives from HKSA and addressed the concerns raised by HKSA over the use of biometrics for identification and security purposes. The meeting turned out to be productive. On the request of HKSA, the Commissioner provided a written reply to the questions raised by HKSA for reference and circulation to its members.

### 例子 Example

2

#### 大埔區校園驗毒試驗計劃 *Trial Scheme on School Drug Testing in Tai Po District ("the Scheme")*

2009年10月15日，私隱專員與來自保安局禁毒處、教育局及律政司的十二位代表會面。私隱專員在會上對該計劃的各範疇給予意見及評論。此外，副私隱專員於2009年11月27日向該計劃的兩位項目主任簡介私隱條例，讓兩位項目主任深入認識條例的規定。

On 15 October 2009 the Commissioner had a meeting with twelve representatives from the Narcotics Division of the Security Bureau, Education Bureau and Department of Justice. During the meeting, the Commissioner gave his views and comments on various aspects of the Scheme. Besides, the Deputy Commissioner held a briefing session on the Ordinance for two Project Officers of the Scheme on 27 November 2009. The briefing provided the Project Officers with a deeper insight and understanding of the requirements of the Ordinance.

## 例子 Example

3

### 運輸署要求公署提供協助

#### *Request for Assistance from Transport Department (“TD”)*

2008年，運輸署建議實施新計劃(下稱「該計劃」)，協助駕駛人士預先籌劃行程，避免交通擠塞。該計劃涉及在經揀選的新界快速道路安裝行車速度屏，顯示交通擠塞的程度。運輸署會收集即時的交通資訊，然後把車速發送至行車速度屏。

為應付該計劃的私隱問題，運輸署要求該計劃的投標者提交私隱影響評估報告，以支持其建議的收集數據技術。

運輸署邀請私隱專員提供協助，對投標者提交的私隱影響評估報告作出評核及評分。私隱專員答應協助，並於2009年12月7日向運輸署提供對該計劃的意見。

In 2008, TD proposed to implement a new project (“the Project”) to help motorists plan their journeys ahead to avoid traffic congestion. It involved the installation of speed map panels along selected strategic corridors in the New Territories to display traffic congestion levels. Real time information of vehicles would be collected before disseminating the speeds on the speed map panels.

To tackle the privacy issues of the Project, TD required every tenderer for the Project to submit a Privacy Impact Assessment (“PIA”) report to support its proposed technology in data collection.

TD invited the Commissioner to assist in assessing and grading all PIA reports submitted by the tenders. The Commissioner agreed to assist and provided TD with his comments on the Project on 7 December 2009.

## 例子 Example

4

### 閉路電視監察指引

#### *Guidance on Closed Circuit Television (“CCTV”) Surveillance*

公署人員於2009年12月10日及2010年3月8日出席由深水埗區議會、警方、消防處及屋宇署聯合舉辦的兩個關於樓宇保安的公開講座。出席人士為深水埗居民及商戶。在講座中，公署人員從私隱規管者角度提供在公共地方進行閉路電視監察的實用指引。

The Commissioner’s officers took part in two public seminars on building security on 10 December 2009 and 8 March 2010, which were jointly held by Sham Shui Po District Office, Hong Kong Police Force, Fire Services Department and Buildings Department. The audiences were residents and shop owners in Sham Shui Po. During the seminars, the Commissioner’s officers provided useful guidance on CCTV surveillance in public place from the perspective of a privacy regulator.

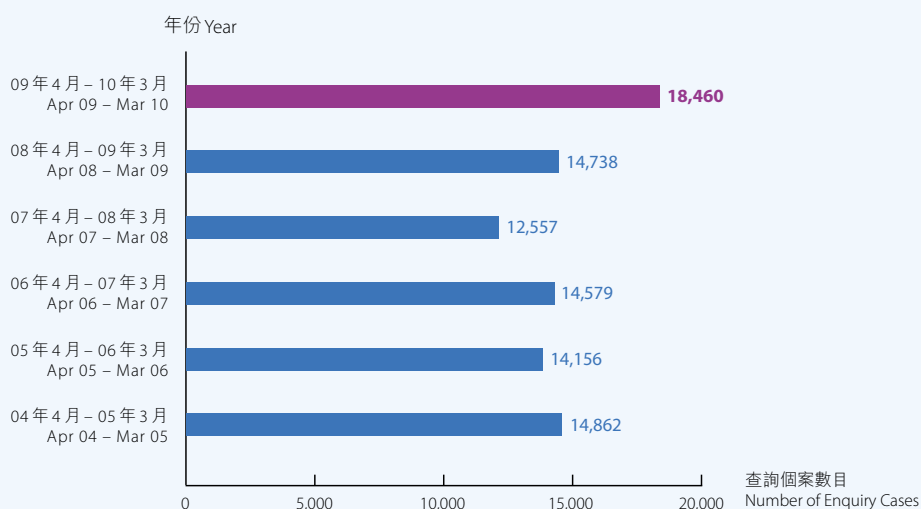
## 在二零零九至一零年度接獲的查詢 Enquiries Received during 2009-2010

在2009-2010年度，公署共處理18,460宗查詢個案(較去年增加25%)，每日平均處理74宗。

A total of 18,460 enquiry cases were handled in 2009-2010 (a 25% increase compared with the previous year). On average, 74 enquiry cases were handled each working day.



每年的查詢個案  
Annual Enquiry Caseload



圖表 FIGURE

2

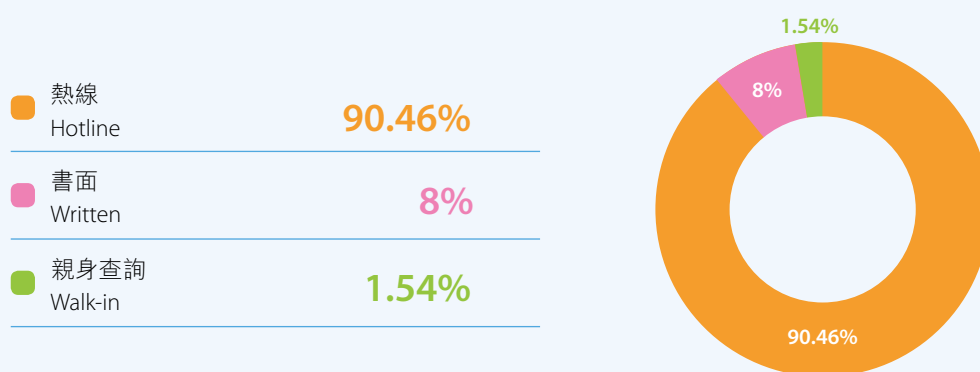
## 查詢個案的性質 Nature of Enquiry Cases

人力資源管理實務守則 Code of Practice on Human Resource Management	13%
僱主監察僱員活動 Workplace Surveillance	5%
生物辨識科技 Biometrics	4%
個人信貸資料實務守則 Code of Practice on Consumer Credit Data	1%
直接促銷 Direct Marketing	5%
身分證號碼及其他身分代號實務守則 Code of Practice on the Identity Card Number and other Personal Identifiers	5%
查閱資料要求 Data Access Request	8%
追收債款 Debt Collection	2%
與互聯網有關 Internet Related	2%
其他 Others	55%

圖表 FIGURE

3

## 提出查詢的途徑 Means by Which Enquiries Were Made



大部分的查詢個案(約90%)是透過公署的查詢熱線電話 2827 2827 提出的。

The majority of the enquiry cases (about 90%) 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）。

在年報期內，私隱專員共進行了111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行動。

大部分循規查察行動（72次）是與私營機構的行事方式有關，其餘（39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 Commissioner identifies a practice in an organization that appears to be inconsistent with the requirements of the Ordinance. In these circumstances, the 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 Commissioner on the measures that should be taken to prevent further breaches. Other times, the 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 Commissioner carried out 111 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 (72) occurred in the private sector. The remaining (39) related to government departments and statutory bodies. The following examples highlight some of the compliance checks undertaken during the year.



## 例子 Example

1

一個政府部門經檔案分享軟件在互聯網上洩漏個人資料

### *A Government Department Leaked Personal Data on the Internet Through a File-sharing Software*

2009年2月，本地報章廣泛報道，超過60份屬於一個政府部門（下稱「該部門」）的限閱文件經檔案分享軟件“Foxy”在網上外洩。事件涉及的個人資料（下稱「該等資料」）包括受影響人士的姓名、出生日期、職級、職銜及工作表現評核等。

公署對該部門進行了循規查察行動。結果顯示，該部門三名高級人員把該等資料儲存於辦公室的一台電腦中。但他們被調職後，卻沒有從電腦中刪除該等資料，引致該等資料被未經授權人士查閱，最後更被Foxy用戶刻意下載。

為了補救情況，該部門首長對有關人員採取紀律處分，並向私隱專員簽署正式承諾書，承諾該部門會制定新指引，禁止所有職員使用裝有檔案分享軟件的電腦處理載有個人資料的辦公文件，並會採取所有切實可行的步驟，確保職員遵從新指引。2010年3月1日，私隱專員向該部門發出書面警告。

In February 2009, it was widely reported by local newspapers that more than 60 restricted government documents belonging to a government department (“the Department”) were leaked on the Internet through a file-sharing software called “Foxy”. The personal data (“the Data”) involved in this incident included affected officers’ names, dates of birth, ranks, post titles and performance appraisals.

A compliance check was carried out against the Department. The check revealed that three senior officers had stored the Data on a computer in an office of the Department. Unfortunately the Data were not deleted from the computer after the said officers were posted out. As a result, the Data were accessed by unauthorized parties and subsequently shared among Foxy users.

To remedy the situation, the Head of the Department took disciplinary action against the said officers and signed a formal undertaking with the Commissioner confirming that the Department would formulate new guidelines prohibiting all staff from using computers with file-sharing software to handle official documents containing personal data, and would take all practicable steps to ensure that the new guidelines are complied with. On 1 March 2010, the Commissioner issued a written warning to the Department.



## 例子 Example

2

一間物業管理公司向停車場使用者收集租約副本

### *A Property Management Company Required Collection of Copies of Tenancy Agreements from Carpark Users*

一間物業管理公司(下稱「該公司」)實施新措施，要求使用其停車場人士提供租約副本作為住址證明，以核實他們使用停車場的資格。

鑑於租約內載有大量個人資料，公眾普遍認為該公司的新措施高度侵犯私隱。2009年10月5日，一個政黨的代表到公署，向私隱專員遞交請願信，要求私隱專員對事件展開調查。

私隱專員認為資料使用者可因合法目的而收集個人資料，但必須小心評估收集有關資料在達至收集目的來說，是否必要及不超乎適度。

私隱專員經初步查詢後向該公司表示，該公司向申請停車場許可證人士收集租約副本很大可能違反保障資料原則。該公司接納私隱專員的意見，並以書面承諾不會向停車場使用者收集租約副本。2010年3月1日，私隱專員向該公司發出書面警告。

A property management company ("the Company") imposed new measure to verify the eligibility of its carpark users by requesting them to provide, inter alia, copies of their tenancy agreements for residential proof purpose.

Tenancy agreements often contain massive amount of personal data. The community reacted negatively to the new measure in view of its high privacy-intrusiveness. On 5 October 2009, a political party visited this Office and petitioned the Commissioner to investigate the Company.

The Commissioner considers that while a data user may have legitimate purposes to collect personal data, the data user must carefully assess whether collection of such data is necessary but not excessive for achieving the purpose of collection.

After a preliminary inquiry, the Commissioner advised the Company that by collecting copies of tenancy agreements from individuals applying for carpark permits, the Company was likely to breach the data collection principle. The Company accepted the Commissioner's advice and undertook in writing that it would not collect copies of tenancy agreements for residential proof purpose. On 1 March 2010, the Commissioner issued a written warning to the Company.



## 例子 Example

3

### 一間廟宇向購買骨灰龕人士收集身分證副本

#### *A Temple Collected Copies of Hong Kong Identity Cards ("HKIC") from Buyers of Columbarium Niches*

粉嶺一間廟宇(下稱「該廟宇」)要求購買骨灰龕人士提供身分證副本，這項規定載於由客戶填寫的登記表格中。該廟宇解釋，收集身分證的目的是核實身分及作記錄用途。

經公署向該廟宇解釋保障資料第1原則及私隱專員根據條例發出的《身分證號碼及其他身分代號實務守則》的相關規定後，該廟宇立即停止向客戶收集身分證副本，並以書面承諾銷毀之前所收集的身分證副本及刪除登記表格上的有關規定。2009年12月23日，私隱專員向該廟宇發出書面警告。

A temple in Fanling ("the Temple") required people buying columbarium niches to provide HKIC copies and such requirement was blatantly stipulated in a registration form to be filled by the customers. The Temple explained that the HKIC copies were collected for the purposes of identity verification and record keeping.

After being notified of the relevant requirements under DPP1 and the Code of Practice on the Identity Card Number & other Personal Identifiers issued by the Commissioner under the Ordinance, the Temple immediately ceased its practice to collect HKIC copies from its customers, and undertook in writing to destroy all HKIC copies previously collected and remove such requirement from its registration form. On 23 December 2009, the Commissioner issued a written warning to the Temple.

## 例子 Example

4

### 網上銷售個人資料 Online Sale of Personal Data

這個循規查察個案源於一個促銷個人資料的投訴。投訴人表示收到一間有限公司(下稱「該公司」)的直接促銷電郵，以1,288元向她兜售一份載有一千名經理級人士的個人資料的名單。出售的個人資料包括公司名稱、業務性質、聯絡人士、職銜、電話號碼、電郵地址(下稱「該等資料」)。

公署的初步查詢顯示，該公司收集了網上新聞訂戶的個人資料，然後編纂該等資料出售。

考慮過該公司收集該等資料的目的後，私隱專員在2009年11月致函該公司表達其初步意見，認為該公司把該等資料出售圖利違反了保障資料第3原則。

該公司對私隱專員的意見作出了積極的回應，並向私隱專員書面承諾會即時停止編纂個人資料作銷售的做法。2009年12月21日，私隱專員向該公司發出書面警告。

This compliance check case deals with a report alleging direct sale of personal data. According to the informant, she received a direct marketing email from a limited company ("the Company") inviting her to buy a list containing the personal data of 1,000 managerial people at a price of \$1,288. The personal data on sale included company names, business natures, contact persons, titles, telephone numbers, e-mail addresses ("the Data").

Initial enquiries by PCPD revealed that the Company had collected personal data from its online news subscribers and then compiled the data so collected for subsequent sale.

In November 2009, the Commissioner issued a letter to the Company expressing his preliminary view that having regard to the purpose for which the Data were collected, its practice of selling the Data for financial gain had contravened DPP3.

In response to the preliminary view letter, the Company provided a written undertaking to the Commissioner in which the Company confirmed that it would desist the practice of compiling personal data for sale purpose. On 21 December 2009, the Commissioner issued a written warning to the Company.



## 例子 Example

5

### 遺失載有學生的個人資料的USB記憶體

#### *Loss of USB Flash Drive Containing Personal Data of Students*

2009年2月，本地一間大學（下稱「該大學」）向私隱專員報告遺失一個沒有加密的USB記憶體，內載該大學超過3,900名學生的個人資料。該USB記憶體屬於該大學的一名僱員，內載的個人資料包括受影響學生的姓名及香港身份證號碼。

在回應私隱專員的書面查詢時，該大學的校長於2010年2月11日向私隱專員書面承諾會檢討有關使用私人手提電子裝置的政策及措施，以及會採取所有合理地切實可行的步驟，確保該大學聘用的職員是可靠、審慎及具辦事能力。

In February 2009, a local university ("the University") reported to the Commissioner the loss of an unencrypted USB flash drive containing the personal data of over 3,900 students of the University. The personal data stored on the flash drive, which was privately owned by an employee of the University, included names and Hong Kong identity card numbers of the affected students.

In response to the Commissioner's written enquiry, the Vice Chancellor of the University provided the Commissioner with a written undertaking on 11 February 2010 confirming that it would review its policies and practices in relation to the use of private portable electronic devices, and would take all reasonably practicable steps to ensure that the staff entrusted by the university are reliable, prudent and competent.

## 例子 Example

6

### 載有銀行客戶個人資料的電腦列印文件被用來包裝鮮花

#### *Printouts Containing Personal Data of Bank Customers were Used to Wrap Flowers*

一間商業銀行（下稱「該銀行」）發現一些載有該銀行客戶資料的廢棄電腦列印文件被一間位於灣仔的花店用作包裝紙。有關文件原本屬於該銀行的按揭部，在廢棄後由該銀行的廢紙承辦商收集及銷毀。

在回應私隱專員的查詢時，該銀行的副行政總裁於2009年5月4日簽署承諾書，承諾該銀行會採取所有切實可行的步驟，防止事件再發生。該銀行會制定新政策，規管處理載有個人資料的廢棄機密文件，並要求其廢紙承辦商嚴格遵守條例的規定。

公署人員亦與該花店的負責人會面，並獲其書面承諾日後不會使用載有個人資料的紙張作包裝用途。

A commercial bank ("the Bank") discovered that some obsolete computer printouts containing the Bank's customer data were found being used as wrapping paper in a floral shop operating in Wanchai. The printouts were originally generated by the Bank's Property Loans Department. After they became obsolete, they were collected by a waste contractor for destruction.

In response to the Commissioner's inquiry, the Bank's Deputy Chief Executive personally signed an undertaking on 4 May 2009 confirming that the Bank would take all practicable steps to prevent a recurrence by formulating a new policy governing the handling of obsolete confidential documents containing personal data, and requiring its waste contractor to strictly observe the provisions of the Ordinance.

The operator of the floral shop was interviewed and she undertook in writing not to use wrapping paper containing personal data for packaging in future.

## 例子 Example

7

前保險代理人被裁定沒有刪除不再需要的個人資料

**Former Insurance Agent Convicted for Failing to Erase Personal Data that were No Longer Required**

一名保險代理人(下稱「該代理人」)在1988至2004年受聘於不同保險公司期間收集了大量有關客戶資料的文件副本。他於2004年破產，喪失其保險代理人牌照。雖然他沒有銷售保單的有效牌照，但他仍然保留該批文件副本。

2008年11月，該代理人在其住宅的梯間棄置三箱載有超過二千名人士的個人資料的文件副本。該代理人的鄰居報警求助，該批文件副本被警方檢走。

由於涉及大量個人資料，警方因此通知私隱專員。私隱專員立即派員協助警方審查該批文件及處理該案。

經過一輪調查及檢控程序後，該代理人被控違反條例第26條的規定。案件於2009年7月在裁判處審理，該代理人承認控罪，被判罰款。而該批文件副本亦被充公。

An insurance agent ("the Agent") collected a large quantity of copy documents from his clients during his employ in various insurance companies from 1988 to 2004. He became bankrupt in 2004 and lost his insurance agent licence. Though he had no valid licence for selling insurance policies, he continued to keep the copy documents.

In November 2008, the Agent abandoned 3 cartons of copy documents containing personal data of over 2,000 individuals at the staircase next to his home premises. The Agent's neighbor sought Police assistance and the copy documents were seized.

As massive amount of personal data were involved, the Police informed the Commissioner who immediately assigned his officers to assist the Police in examining the documents and handling the case.

Upon investigation and prosecution, the Agent was summonsed for contravention of section 26 of the Ordinance and the case was brought to a Magistrate's Court in July 2009. The Agent pleaded guilty to the summons and was fined. The copy documents were confiscated.

## 主動調查 Self-initiated Investigations

如資料違規事件引起公眾極大關注，私隱專員可根據條例第 38 (b) 條主動對事件作出調查，而無需等待投訴人提出投訴。此外，如在循規查察行動時發現有嚴重的違規情況，私隱專員亦會主動調查，以決定應否向有關的資料使用者發出執行通知，指令它改正某行為或採取適當的補救措施。

在截至 2010 年 3 月 31 日的年度，由私隱專員根據第 38 (b) 條主動作出的調查共 9 宗。

Where there is a data breach incident of great public concern, the Commissioner may initiate an investigation into the matter under section 38(b) of the Ordinance without waiting for a complainant to come. Also, if serious breach is found during a compliance check, a self-initiated investigation will follow to determine as to whether an enforcement notice should be issued to the data user concerned requiring it to correct certain behavior or adopt appropriate remedial measures.

For the year ended 31 March 2010, the Commissioner had initiated a total of 9 investigations under section 38(b) of the Ordinance.

### 招聘網站洩漏 39,000 名網上求職者的個人資料

### A Recruitment Website Leaked the Personal Data of 39,000 Online Job seekers

一個招聘網站洩漏了 39,000 名在該網站登記的求職者的個人資料，外洩資料包括姓名、身份證號碼、住址、電話號碼及履歷等（下稱「該等資料」）。該招聘網站是由一間本地有限公司（下稱「該公司」）經營。

A recruitment website operated by a local limited company ("the Company") leaked the personal data of 39,000 individuals who had registered on the website to look for jobs. The leaked data included their names, identity card numbers, residential addresses, telephone numbers and resumes ("the Data").

由於事件涉及大量求職者的個人資料，私隱專員為了公眾利益，決定根據條例第 38 (b) 條對該公司展開正式調查。

Given that the incident involved a large quantity of job seekers' personal data, the Commissioner decided that it was in the public interest to initiate a formal investigation against the Company under section 38(b) of the Ordinance.

調查顯示，資料外洩是由於該公司使用真實的個人資料作應用測試，但在使用後卻將該等資料遺留在網絡伺服器，沒有理會。該公司沒有實施加密或認證方法，防止該等資料避免未經准許的查閱。因此，一個互聯網搜尋引擎成功標引該等資料，供公眾查閱。

Investigation revealed that the data breach was due to the Company using real personal data for the purpose of application testing, and leaving the Data on the web server unattended after use. There was no encryption or authentication method implemented to prevent the Data from unauthorized access. As a result, an Internet search engine crawler successfully indexed the Data for public access.

事件曝光後，該公司立即採取補救行動，從其網絡伺服器移除該等資料，並要求互聯網搜尋引擎公司刪除該等資料。2009年8月12日，該公司向私隱專員承諾會採取保安措施及所有合理地切實可行的步驟，防止類似事件再發生。

私隱專員認為事件影響39,000名求職者，是嚴重的網上資料外洩事件，該公司違反了保障資料第4原則的規定。

考慮到該公司已採取補救行動及簽署承諾書，私隱專員決定在本個案不發出執行通知。不過，私隱專員在2009年9月15日向該公司發出警告信，表示如該公司日後沒有遵守條例的相關規定，私隱專員會考慮發出執行通知，指令該公司採取依從條例規定所需的步驟。

The Company took immediate remedial actions to remove the Data from its web server and request the Internet search engine company to delete the Data from the cache. On 12 August 2009, the Company provided an undertaking to the Commissioner stating that it would step up security measures and take all reasonably practicable steps to prevent recurrence of similar incidents.

The Commissioner considered that this was a serious online data security breach incident affecting 39,000 job seekers and found the Company in contravention of the requirements under DPP4.

Having regard to the remedial actions taken by the Company and the written undertaking signed by it, the Commissioner decided not to issue an enforcement notice in the present case. However, the Commissioner issued a warning letter to the Company on 15 September 2009 stating that if the Company failed to observe the relevant requirements of the Ordinance in future, the Commissioner may consider serving an enforcement notice directing the Company to take such steps as are necessary to comply with the Ordinance.

政府自2003年起簽發智能身份證以取代舊身份證。為確保由入境事務處（下稱「入境處」）持有及處理的所有個人資料合乎條例的規定，政府向立法會承諾，在諮詢私隱專員後制定實務守則，訂明收集、使用及查閱智能身份證資料的規則，以及對智能身份證系統進行私隱循規審核。

私隱循規審核旨在評估入境處依從條例規定的程度、識別入境處資料保障系統的潛在弱點，及向入境處提供改善其資料保障系統的建議。

為消除私隱專員在進行私隱循規審核及履行條例下的規管角色兩者之間可能出現的矛盾，私隱專員與入境處處長（下稱「處長」）簽署諒解備忘錄，訂明私隱專員作為規管者的法定權力不會受到影響。

私隱循規審核於2009年6月開始。期間，公署人員審閱數以千計的入境處文件、到訪19個入境處辦事處／管制站、會見333名智能身份證申請者，並向65名職級由助理處長至入境事務助理員的入境處人員索取資料。此外，公署人員於2009年11月到入境處進行問卷調查，就收集、持有、處理或使用智能身份證資料的措施及原則，向300名受訪者收集意見。所有受訪者均是入境處的職員，來自16個不同的辦事處／管制站。

私隱循規審核於2010年2月完成。2010年3月31日，私隱專員向處長發出一份私隱循規審核報告草擬本，待處長回應。私隱專員會把全部或部分回應納入私隱循規審核的最後報告中。如有需要改善的地方，會將之納入實務守則。實務守則正式定稿後，會由私隱專員根據條例第12條核准及發出。

The Government has been issuing smart identity cards to replace the old identity cards since 2003. To ensure that all personal data held by the Immigration Department ("ImmD") are handled in accordance with the provisions of the Ordinance, the Government undertook to the Legislative Council to draw up a code of practice in consultation with the Commissioner setting out the rules on the collection, use of and access to smart identity card data, and to conduct a Privacy Compliance Audit ("PCA") on the Smart Identity Card System.

The PCA aimed at assessing ImmD's level of compliance with the requirements of the Ordinance, identifying potential weaknesses in ImmD's data protection system, and providing recommendations for a review of ImmD's data protection system.

To obviate any possible conflicts between the Commissioner's role in carrying out the PCA and his regulatory role under the Ordinance, a Memorandum of Understanding was entered into by the Commissioner and the Director of ImmD ("the Director") wherein it was acknowledged that the Commissioner's statutory power to act as a regulator would not be prejudiced or compromised.

The PCA commenced in June 2009. During the course of the PCA, the Commissioner's officers examined thousands of pages of ImmD documents, visited 19 ImmD offices/control points, interviewed 333 smart identity card applicants, and obtained information from 65 ImmD officers ranking from Assistant Director to Immigration Assistant. In addition, an on-site questionnaire survey was conducted in November 2009 to collect 300 participants' perception on practices and principles in relation to the collection, holding, processing or use of smart identity card data. All surveyed participants were serving ImmD employees scattering over 16 offices/control points.

The PCA was completed in February 2010. On 31 March 2010, the Commissioner sent a draft PCA report to the Director for his response. The Commissioner will incorporate into the final PCA report all or any part of the response. Areas requiring improvements, if any, will be factored into the code of practice which will then be formalized and approved by the Commissioner in accordance with section 12 of the Ordinance.



## 核對程序 Matching Procedures

在本年報期內，私隱專員共收到 53 宗核對程序申請，3 宗來自公共事業公司，其餘 50 宗來自公營機構。

經審閱後，其中 6 宗撤回或終止申請。私隱專員根據條例賦予的權力，在有條件的情況下批准 44 宗申請。截至 2010 年 3 月 31 日，餘下 3 宗申請正由私隱專員考慮。

以下為部份核准的核對程序個案：

During the reporting year, the Commissioner received 53 applications for approval to carry out matching procedures. 3 applications were made by public utilities companies and the remaining 50 applications came from public sector organizations.

Upon examination, 6 applications were subsequently withdrawn or discontinued. 44 applications were approved subject to conditions imposed by the Commissioner under the Ordinance. As at 31 March 2010, the remaining 3 applications were under the consideration of the Commissioner.

The following are some of the matching procedures that were approved by the Commissioner :

提出要求者 Requesting Parties	獲准的有關核對程序 Related Matching Procedures that were Approved
房屋協會 Hong Kong Housing Society	<p>公署同意房屋協會進行核對程序，將房屋協會、市區重建局、屋宇署與房屋委員會就「樓宇更新大行動」及相類資助計劃所收集的個人資料互相比較，以避免有人獲得雙重津貼的情況。</p> <p>Consent was given to Hong Kong Housing Society to carry out a matching procedure to prevent double benefits by comparing personal data collected by Hong Kong Housing Society, Urban Renewal Authority, Buildings Department and Housing Authority under the Operation Building Bright and similar subsidy schemes.</p>
市區重建局 Urban Renewal Authority	<p>公署同意市區重建局進行核對程序，將房屋協會、市區重建局與屋宇署就「樓宇更新大行動」及相類資助計劃所收集的個人資料互相比較，以避免有人獲得雙重津貼的情況。</p> <p>Consent was given to Urban Renewal Authority to carry out a matching procedure to prevent double benefits by comparing personal data collected by Hong Kong Housing Society, Urban Renewal Authority and Buildings Department under the Operation Building Bright and similar subsidy schemes.</p>
學生資助辦事處 Student Financial Assistance Agency	<p>公署同意學生資助辦事處進行一次性的核對程序，將 2009/10 學年內的學生受助人的個人資料，與社會福利署的綜合社會保障援助計劃下的學生受助人的個人資料互相比較，以防止一筆過的開學津貼被雙重發放。</p> <p>Consent was given to Student Financial Assistance Agency to carry out a one-off matching procedure to prevent double subsidy by comparing the personal data collected from student-recipients of financial subsidies in the 2009/10 school year with the personal data collected by Social Welfare Department from student-recipients of the Comprehensive Social Security Assistance scheme.</p>

提出要求者 Requesting Parties	獲准的有關核對程序 Related Matching Procedures that were Approved
香港警務處 Hong Kong Police Force	<p>公署同意香港警務處進行核對程序，將牽涉道路交通案件人士的個人資料，與入境事務處人事登記資料庫內的個人資料互相比較，以更新有關人士的地址並向該些人士送達法庭傳票。</p> <p>Consent was given to Hong Kong Police Force to carry out a matching procedure to compare the personal data of individuals involved in road traffic cases with the personal data held in the Registration of Persons database of the Immigration Department, in order to obtain updated addresses for serving court summons to the relevant individuals.</p>
強制性公積金計劃管理局 Mandatory Provident Fund Schemes Authority	<p>公署同意強制性公積金計劃管理局進行核對程序，將強積金中介人及申請人的個人資料，與其它八個規管機構／組織所持有的個人資料互相比較，以確定他們符合強積金中介人及申請人的資格。</p> <p>Consent was given to Mandatory Provident Fund Schemes Authority to carry out a matching procedure to determine the eligibility of applicants for and registrants of Mandatory Provident Fund intermediaries by comparing their personal data with personal data held by eight other monitoring authorities/ bodies.</p>
香港鐵路有限公司 MTR Corporation Limited	<p>公署同意香港鐵路有限公司進行核對程序，將「殘疾人士車費推廣計劃」申請者／受助人的個人資料，與社會福利署從傷殘津貼及綜合社會保障援助計劃所收集的受助人個人資料互相比較，以確認他們符合有關資格。</p> <p>Consent was given to MTR Corporation Limited to carry out a matching procedure to determine the eligibility of the applicants for or recipients of Fare Promotion for Persons with Disabilities scheme by comparing their personal data with personal data collected by the Social Welfare Department under the Disability Allowance and Comprehensive Social Security Assistance schemes.</p>
懲教署 Correctional Services Department	<p>公署同意懲教署進行核對程序，將部門宿舍的申請人及住戶的個人資料，與房屋署為提供公共房屋所收集的個人資料互相比較，以避免有人獲得雙重房屋福利的情況。</p> <p>Consent was given to Correctional Services Department to carry out a matching procedure to prevent double housing benefits by comparing personal data of applicants for or occupants of departmental quarters with personal data collected by Housing Department for the provision of public housing.</p>

### 新核對程序表格

2010年3月12日，公署在憲報刊登根據條例第31(1)條提出核對程序要求的新表格，以取代2007年6月刊憲的表格。新表格是私隱專員依據條例第67條所指明的。資料使用者在2010年3月31日以後向私隱專員提出核對程序申請時，必須填妥新表格。

### New Matching Procedure Form

On 12 March 2010, a new form for making a matching procedure request under section 31(1) of the Ordinance was published in the Gazette for public notice. The new form is specified by the Commissioner pursuant to section 67 of the Ordinance to supersede the form gazetted in June 2007. Data users are required to complete the new form when making a request for the Commissioner's consent to the carrying out of a matching procedure after 31 March 2010.