保障私隱 全面貫徹
Privacy by Design, Privacy by Default

3 審查工作 Compliance Actions

最佳監管夥伴 — 香港金融管理局(金管局)

根據《銀行業條例》界定的認可機構加強了它們在收集及使用客戶個人資料的控制。金管局在此方面的監督確實功不可抹。

Best Regulatory Partner - Hong Kong Monetary Authority (HKMA)

Authorized Institutions (as defined in the Banking Ordinance) have strengthened their control over their collection and use of customers' personal data. HKMA has played an important role of oversight. It also assisted PCPD in early 2011 in amending the Code of Practice on Consumer Credit Data to improve Authorized Institutions' credit risk management, whilst safeguarding personal data privacy.

左: 香港金融管理局助理總裁(銀行操守)戴敏娜女士
Left: Ms. Meena Datwani, Executive Director (Banking Conduct), Hong Kong Monetary Authority

諮詢工作
CONSULTATION

「$6,000計劃」

政府的「$6,000計劃」向每名年滿18歲持有有效香港永久性居民身份證的人士發放6,000元。私隱專員關注非政府組織為協助市民登記該計劃而發起的活動。由於這些活動涉及收集及使用個人資料，因此條例的保障資料原則適用。

私隱專員認同這些活動的好意，但希望提醒登記人留意下述事宜，以保障其個人資料私隱權利：

- 不當處理資料的風險
- 了解收集資料的目的
- 不要提供超乎適度的個人資料
- 保留相關記錄

私隱專員亦建議非政府組織遵從條例的規定：

- 確保所收集的資料是與其收集目的相關的
- 避免過度及不公平地收集個人資料
- 通知登記人收集資料的目的及資料會被轉移予的人士
- 確保個人資料的使用符合收集目的
- 確保不會將不再需要的個人資料保留過久
- 確保個人資料安全

SCHEME $6000

The Commissioner was concerned about the campaigns launched by non-governmental organizations ("NGOs") offering to provide assistance to individuals in registering for the Government's Scheme to give $6,000 to each holder of a valid Hong Kong Permanent Identity Card aged 18 or above. As such efforts involved the collection and use of personal data, the Data Protection Principles under the Ordinance apply.

While recognizing the good intentions of the campaigns, the Commissioner advised registrants to note the following to safeguard their personal data privacy rights:

- The risk of data mishandling
- Understand the purpose of data collection
- Do not provide excessive personal data
- Keep relevant records

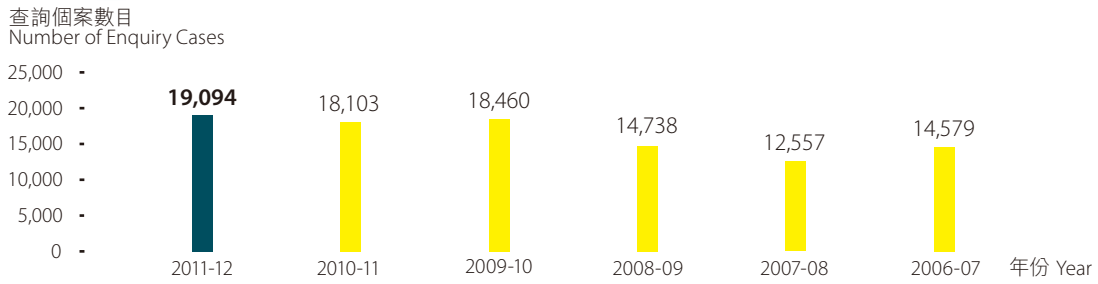
The Commissioner also advised the NGOs to comply with the requirements under the Ordinance by:

- ensuring the relevance of the data collected;
- avoiding excessive and unfair collection of personal data;
- informing the registrants of the purpose of the data collection and to whom the data would be transferred;
- ensuring the use of personal data in line with the collection purpose;
- ensuring there would be no excessive retention of personal data that was no longer required; and
- ensuring the security of the personal data they collected.

在二零一一至一二年度間接獲的查詢
ENQUIRIES RECEIVED IN 2011-2012

圖表 Figure 1

每年的查詢個案
ANNUAL ENQUIRY CASELOAD



在本年度，公署共處理19,094宗查詢個案（較去年上升5.5%），每日平均處理78宗。

A total of 19,094 enquiry cases were handled during the year (an increase of 5.5% compared with the previous year). On average, 78 enquiry cases were handled each working day.

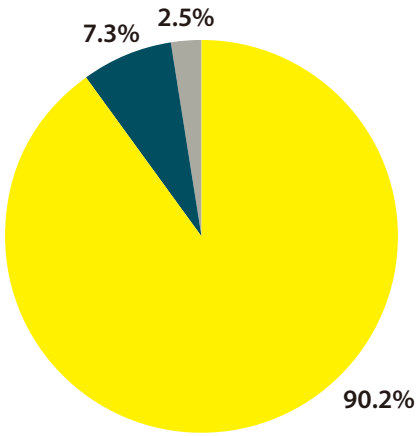
圖表 Figure 2

查詢個案的性質
NATURE OF ENQUIRY CASES

13%	人力資源管理實務守則	Code of Practice on Human Resource Management
4%	僱主監察僱員活動	Workplace Surveillance
1%	生物辨識科技	Biometrics
2%	個人信貸資料實務守則	Code of Practice on Consumer Credit Data
7%	直接促銷	Direct Marketing
5%	身份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
9%	查閱資料要求	Data Access Requests
2%	追收債款	Debt Collection
2%	與互聯網有關	Internet Related
55%	其他	Others
34%	條例條文及保障資料原則的一般查詢	General enquiries on provisions of the Ordinance and DPPs
14%	公署的資訊／聯絡公署人員	Information about the PCPD/Contact PCPD staff
4%	私隱但不屬個人資料私隱的事宜	Privacy other than personal data privacy
3%	與公署職能無關	Unrelated to PCPD functions

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 (2827 2827).

循規查察行動
COMPLIANCE CHECKS

當私隱專員發現某一機構的行事方式看來有違條例下的規定時，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或有所不足的事宜，並於適當時促請有關機構採取適當的糾正措施。

The Commissioner conducts compliance checks into practices that appear to be inconsistent with the requirements of the Ordinance. In these cases, the Commissioner alerts the organization in writing, pointing out the apparent inconsistency or deficiency and inviting the organization, where appropriate, to take remedial action.

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。在部份個案中，有關機構會就如何採取改善措施向私隱專員尋求意見，以免重複涉嫌違例事項。在其他情況下，私隱專員會對涉嫌違例事項進行調查，並採取適當的執法行動，確保有關機構遵從條例的規定。行動包括向有關機構發出執行通知，指令它作出糾正。

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. In other cases, the Commissioner investigates the matter and takes appropriate enforcement action to ensure compliance with the Ordinance. This may include issuing an enforcement notice to the organization directing it to remedy the situation.

在年報期內，私隱專員就資料使用者可能違反私隱條例下的規定的行事方式進行了共144次循規查察行動。

During the reporting year, the Commissioner carried out 144 compliance checks in relation to practices of data users that may be inconsistent with the requirements of the Ordinance.

大部分循規查察行動（103次）是與私營機構的行事方式有關，其餘41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。

The majority of the compliance checks (103) were conducted in relation to the private sector. The remaining 41 related to government departments and statutory bodies. The following examples highlight some of the compliance checks conducted during the year.

PlayStation® Network的資料外洩事件

Data Breach by Sony PlayStation® Network

個案 CASE 1

2011年4月，PlayStation® Network（下稱「**PSN**」）受黑客入侵。因這次非法及未經授權的入侵，PSN的帳戶資料遭洩露。

In April 2011, the Sony PlayStation® Network ("**PSN**") was hacked and the PSN user account information was compromised due to the illegal and unauthorized intrusion.

PSN全球估計有7,700萬個帳戶，其中400,000個為香港帳戶。帳戶中一些敏感個人資料，例如信用卡資料，可能受影響。

The PSN was estimated to hold 77 million global customer accounts, of which 400,000 were Hong Kong accounts. Some of the sensitive personal data in the customer accounts included credit card information, might be at stake.

鑑於事態緊急，私隱專員迅速與Sony Computer Entertainment香港有限公司（下稱「**SCEH**」）的管理層會面。私隱專員亦下令對這次資料外洩事件進行查詢，以確定Sony是否已採取所有切實可行的步驟，保障其客戶資料免受黑客入侵。

To ascertain the situation as a matter of urgency, the Commissioner swiftly met with the management of Sony Computer Entertainment Hong Kong Limited ("**SCEH**") after the incident. The Commissioner also ordered an enquiry into this data breach incident with a view to ascertaining whether Sony had taken all practicable steps to protect its customer data against hacking.

查詢顯示被洩露的帳戶資料包括PSN帳戶持有人的姓名、地址、國家、電郵地址、出生日期、PSN密碼、登入名稱及PSN在線名稱。

Enquiry revealed that the account information compromised included the name, address, country, email address, birthdate, PSN password and login, as well as the PSN online identity of PSN account holders.

SCEH為作出補救，立即通知所有受影響的香港帳戶持有人，並提供電話熱線回答公眾查詢。私隱專員亦要求SCEH在恢復PSN服務之前，提升PSN的保安至令人滿意的程度，以確保類似事件不會再發生。

To remedy the situation, SCEH took immediate action to notify all Hong Kong account holders affected in the incident and provided a telephone hotline to answer public enquiries. The Commissioner also required SCEH, before resumption of the PSN services, to upgrade the security protection of the PSN to a satisfactory level to prevent recurrence of the incident.

SCEH其後通知私隱專員，Sony已找出導致黑客入侵的原因，並已採取足夠及適當的補救措施，以防止事件再度發生。SCEH補充，他們沒有收到客戶報稱其個人資料因這次資料外洩事件而遭濫用。

SCEH later informed the Commissioner that Sony had identified the cause of the intrusion, and taken adequate and appropriate remedial measures to prevent further exploitation of the same vulnerability, adding that SCEH had received no reports of misuse of their customers' personal information as a result of the data breach.

2011年6月，私隱專員決定不會對SCEH恢復PSN服務採取執法行動，但會密切監察Sony調查入侵事件的最終結果。

In June 2011, the Commissioner decided not take any enforcement action against SCEH for their resumption of the PSN services but would closely monitor Sony's finalization of its investigation into the intrusion incident.

循規查察行動
COMPLIANCE CHECKS

本地銀行收集"Cookies"

Collection of "Cookies" by Local Banks

個案
CASE

傳媒報道11間本地銀行規定其客戶如要使用其網上銀行服務，須接受cookies*。報道指稱有關銀行並沒有通知客戶cookies會收集甚麼資料及收集目的。

It was reported in the mass media that 11 local banks required their customers to accept cookies* in order to use their Internet banking services. It was alleged that these banks did not inform their customers what data were to be collected through the use of cookies and the purpose of the collection.

基於公眾對資料私隱的關注，私隱專員對有關銀行展開循規查察。

Given the public concern about data privacy, the Commissioner commenced compliance checks on the banks concerned.

有關銀行在回應公署的查詢時，提供了一些資訊，關於儲存於cookies內的資料及向客戶提供網上銀行服務時收集cookies的目的。

In response to the PCPD's enquiries, the banks provided the PCPD with information relating to the data stored in the cookies and the purposes for which cookies were collected when providing Internet banking services to their customers.

根據這些銀行提供的資訊，並沒有明顯證據證明這些銀行透過cookies收集個人資料。無論如何，cookies是儲存在客戶自己的終端機內，而不是銀行的網絡伺服器。不過，由於在技術上cookies可以與銀行持有的其他資料結合而顯示個別客戶的身份及網上銀行習慣，私隱專員認為，作為良好的行事方式，銀行應通知其客戶，他們會透過cookies收集甚麼資料及有關收集的目的，並向不希望其網上銀行習慣被cookies收集的人士提供拒絕服務安排。

Based on the information provided by the banks, there was no apparent evidence suggesting that the banks had collected personal data through the cookies. In any event, the cookies were kept or stored in the customers' own terminals, not at the bank's webservers. However, given that it was technically possible for the cookies to be combined with other information held by the banks to reveal the individual customer's identity and Internet banking habits, the Commissioner took the view that, as a matter of good practice, the banks should inform their customers what information they would collect through the cookies and the purpose of such collection, and provide an opt-out arrangement for those who do not want their Internet banking habits to be collected through cookies.

為了提醒機構資料使用者在進行網上追蹤前應考慮的事宜，私隱專員決定製作《網上行為追蹤》資料單張，闡釋網上追蹤、個人資料與條例之間的關係。這資料單張預計於2012年中發出。

To provide pointers to organizational data users on what they should consider before they deploy online tracking in their websites, the Commissioner decided to publish an information leaflet entitled "Online Behavioural Tracking" to explain the relationship between online tracking, personal data and the Ordinance. It is expected that the information leaflet will be released in mid-2012.

* *當某人從瀏覽器(包括流動電話瀏覽器)進入一個網站時，該網站可以發出一個cookie(細小檔案)，儲存於該瀏覽器內。網站很多時會在cookie內儲存到訪者的偏好(例如語言、字體大小等)或瀏覽行為(例如到訪的網頁或網頁類別)。每個網站可以向瀏覽器發送自己的cookies，但瀏覽器只可容許某網站查閱之前曾向該瀏覽器發送的cookies。*

* *When a visitor accesses a website from a browser (including a mobile phone browser), the website can send a cookie (a small text file) to be stored in the browser. Websites often store preferences (e.g. language and font size) or browsing behaviour (e.g. pages or categories of pages visited) of the visitor in the cookie. Each website can send its own cookies to the browser but the browser only permits a website to access the cookies it has sent to the browser previously.*

個案 CASE 3

銀行向儲蓄戶口申請人收集超乎適度的個人資料

Excessive Collection of Personal Data by Banks from Savings Account Applicants

2011年12月，私隱專員發表一份調查報告，關於恒生銀行向儲蓄戶口申請人收集「教育程度」及「婚姻狀況」的資料（下稱「**該等資料**」）。私隱專員認為恒生銀行沒有採取所有切實可行的步驟，告知儲蓄戶口申請人該等資料屬非必須資料，因而違反了條例的保障資料第1(3)(a)(i)原則的規定。

為了解恒生銀行這種手法在銀行業界是否普遍，私隱專員在2011年9月向19間銀行進行了循規查察。查察發現，（19間銀行中）共有九間銀行要求儲蓄戶口申請人提供該等資料，但他們均沒有在相關申請表中註明該等資料是必須提供，抑或可自願提供，而其實該等資料屬非必須資料，收集該等資料一般是用以了解客戶。

為補救情況，全部九間銀行接受了公署的建議，修改了相關的申請表，清楚註明提供該等資料與否全屬自願。

In December 2011, the Commissioner published an investigation report on Hang Seng Bank in relation to its collection of "education level" and "marital status" information ("**the Data**") from savings account applicants. The Commissioner found that Hang Seng Bank had failed to take all practicable steps to inform the savings account applicants that the supply of the Data was not obligatory, thereby contravening DPP1(3)(a)(i) of the Ordinance.

To ascertain whether the Bank's practice was common in the banking industry, the Commissioner conducted compliance checks on 19 retail banks in September 2011. It was found that a total of nine (out of 19) banks had requested savings account applicants to supply the Data but did not indicate in the relevant application forms whether the Data were obligatory or optional, when in fact the Data were optional information and the collection of the Data was generally for their "know-your-customer" process.

To remedy the situation, all nine banks took the PCPD's advice and revised the relevant application forms to indicate clearly that the supply of the Data was wholly optional.

招聘機構收集超乎適度的個人資料

Excessive collection of personal data by a recruitment agency

個案 CASE 4

一間招聘機構在招聘面試中收集面試者的年齡、婚姻狀況、身高及體重的資料，並拍下面試者的照片。

該機構表示，向求職者收集身高、體重及照片是為客戶揀選最佳應徵者，而收集婚姻狀況是為了進一步認識求職者的背景。

因應公署的循規查察行動，該機構迅速停止向求職者收集超乎適度的個人資料，並修改了求職表格。

該機構亦接受公署的建議，改善其《收集個人資料聲明》，清楚指明收集個人資料的類型、收集目的，以及有關保留資料、查閱資料要求及改正資料要求的政策。

At a job interview, a recruitment agency collected an interviewee's age, marital status, height and weight, and took pictures of the interviewee.

According to the agency, the collection of height, weight and pictures from job seekers was for the purpose of selecting the best candidates for their clients, while the collection of marital status was for better understanding of the job seekers' background.

In response to the PCPD's compliance action, the agency promptly ceased the practice of collecting excessive personal data from job seekers and revised its job application form accordingly.

The agency also took the PCPD's advice to refine its Personal Information Collection Statement by specifying clearly the types of personal data to be collected, the purposes of collection, and its policy relating to data retention, data access requests and data correction requests.

個案 CASE 5

醫院管理局屢次遺失USB記憶體

Repeated loss of USB flash drives by the Hospital Authority

2008年，醫院管理局(下稱「**醫管局**」)轄下多間醫院發生連串遺失便攜式儲存裝置(例如USB記憶體)內的病人資料事件，引起人們極為關注醫管局保障病人資料的資料保安系統是否足夠，尤其是以電子形式持有的病人資料。為促進醫管局遵守條例的規定(尤其是「**資料保安原則**」)及提出有用的建議，私隱專員依據條例第36條對醫管局進行視察。

In 2008, a spate of incidents involving the loss of patients' data stored in portable storage devices ("**PSDs**") such as USB flash drives by individual hospitals under the management of the Hospital Authority ("**HA**") raised grave concern about the adequacy of the HA's data security system for protecting patients' data, in particular, patients' data held in electronic form. In order to promote compliance by the HA with the requirements of the Ordinance, in particular the "Data Security Principle", and to give useful recommendations, the Commissioner carried out an inspection of the HA pursuant to section 36 of the Ordinance.

在視察之後，私隱專員向醫管局提出37項建議，以提高對病人資料的保安。儘管如此，公立醫院及診所在年報期內繼續發生涉及便攜式儲存裝置的遺失資料事件。因此公署對醫管局採取進一步的循規執法行動。

As a result of the inspection, the Commissioner made 37 recommendations to the HA to enhance its patients' data security. Despite this, data loss incidents involving PSDs continued to occur in public hospitals and clinics during the reporting year. Hence, the PCPD took further compliance enforcement action against the HA.

在回應公署的查詢時，醫管局解釋該局已制定了內部政策，規管有關使用便攜式儲存裝置的個人資料保安。不過，鑑於醫管局僱員屢次遺失資料，私隱專員關注個別職員沒有徹底遵從醫管局所制定的政策，建議應採取額外步驟，防止事件再度發生及保障病人資料免受進一步的披露或未經授權的使用。

In response to the PCPD's enquiries, the HA explained that it had in place internal policies governing personal data security relating to the use of PSDs. However, in view of the repeated data loss incidents by HA employees, the Commissioner was concerned that the HA's policies in place had not been followed through by individual staff and advised that additional steps be taken to prevent recurrence and to protect patients' data from further disclosure or unauthorized use.

對於私隱專員的關注，醫管局於2011年對該局的所有個人電腦安裝「端點安全軟件」，強制所有載有個人資料的便攜式儲存裝置加密，從而提高資料保安及管控。

In light of the Commissioner's concerns, in 2011 the HA deployed an "Endpoint Security Software" on all of the HA's personal computers to mandate encryption of data on all PSDs containing personal data, thereby enhancing data security and control.

循規查察行動
COMPLIANCE CHECKS

涉及一間餐廳1,158名僱員的電郵資料外洩事件

Email data leak involving 1,158 employees of a restaurant

個案 CASE 6

一間日本餐廳向私隱專員通報，其人力資源部在一封內部電郵（下稱「**該電郵**」）中意外披露全部1,158名僱員的個人資料。有關個人資料包括員工的姓名、性別、身份證號碼、薪金及聯絡資料（下稱「**該等資料**」）。

A Japanese restaurant reported to the Commissioner that its Human Resources Department had inadvertently disclosed the personal data of all its 1,158 staff members in an internal email ("**the Email**"). The personal data involved included the name, gender, Hong Kong identity card number, salary and contact information ("**the Data**") of each staff member.

在回應公署的書面查詢時，該餐廳解釋其中一名僱員從支薪系統(原本用於人力資源管理)輸出該等資料到一個Excel電子表格，以擬備該餐廳51名僱員參加歌唱比賽的名單。在編製名單後，該僱員把該電郵發送給全體職員，卻忘記從該電郵刪除載有該等資料的電子表格。因此，該等資料被錯誤地披露予該餐廳全體職員。

In response to the PCPD's written enquiries, the restaurant explained that an employee had exported the Data from the payroll system, which was originally used for human resources management, into an Excel spreadsheet for the preparation of a name list for a singing contest in which 51 of the restaurant's employees were to participate. After compiling the name list, that employee forgot to remove the spreadsheet containing the Data from the Email and sent it to all staff by email. As a result, the Data were wrongfully disclosed to all of the restaurant's staff.

在事件發生後，該餐廳採取連串補救行動，以減低資料外洩程度及防止日後再發生類似事件，包括：

(a) 要求全體職員刪除該電郵；
(b) 停止利用支薪系統的個人資料編製名單，除非有關使用與原本的收集目的一致；
(c) 建立存取資料的控制，以保障僱員的個人資料；及
(d) 修改相關的內部政策，把僱員個人資料的使用限制於收集資料的原本目的。

After the incident, the restaurant took the following remedial action to mitigate the leak and to prevent recurrence of similar incidents in future:–

(a) requesting all staff members to delete the Email;
(b) ceasing to use the personal data in the payroll system to generate name lists unless the use is consistent with the original purpose of collection;
(c) setting up access control to protect its employees' personal data; and
(d) revising the relevant internal policies by confining the use of employees' personal data to the original purpose for which the data were collected.

主動調查
SELF - INITIATED INVESTIGATIONS

私隱專員根據條例第38(b)條獲賦權主動對事件作出調查，而無需等待投訴人提出投訴。如發生資料違規事件而引起公眾廣泛關注，私隱專員大多會主動作出調查。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，指令它改正某程序或採取適當的補救措施。

The Commissioner is empowered under Section 38(b) of the Ordinance to initiate an investigation without waiting for any complainant to come forward. He may often do so where there is a data breach incident raising widespread public concern. Also, if a serious breach is found during a compliance check, a PCPD-initiated investigation will follow to determine whether an enforcement notice should be issued requiring the data user in question to correct certain procedures or adopt appropriate remedial measures.

在年報期內，私隱專員根據條例第38(b)條作出了11宗主動調查，並發表了兩份主動調查報告。該兩宗主動調查與兩間銀行的個人資料措施有關，涉案銀行分別是中信銀行國際有限公司（下稱「**中信銀行**」）及恒生銀行有限公司（下稱「**恒生銀行**」）。

During the reporting year, the Commissioner initiated 11 investigations under Section 38(b) of the Ordinance. Of these investigations, two compliance investigation reports on the personal data practices of two banks, namely CITIC Bank International Limited ("**CITIC**") and Hang Seng Bank Limited ("**Hang Seng**"), were published by the Commissioner.

對「大埔區校園驗毒試行計劃」(「該計劃」)進行的視察行動
INSPECTION ON THE TRIAL SCHEME OF SCHOOL DRUG TESTING IN TAI PO DISTRICT ("THE SCHEME")

該計劃是在香港首次實施。該計劃由政府(由保安局禁毒處及教育局牽頭)與大埔區23間公營中學合作推行。政府及公眾對該計劃抱有期望,希望成功打擊青少年吸毒問題。該計劃屬試驗性質,對日後制定及施行任何校園驗毒計劃,是重要的先例及參考。

The Scheme was the first of its kind ever implemented in Hong Kong. It was a joint initiative of the Government (led by the Narcotics Division of the Security Bureau and the Education Bureau) and 23 public sector secondary schools in Tai Po. The Government, as well as the general public, had high hopes of its success in the battle against the youth drug-abuse problem. It was a pilot scheme which would serve as an important precedent and reference for the formulation and implementation of any future school drug-testing schemes.

鑑於驗毒計劃所收集及處理的個人資料屬於高度敏感個人資料,及公眾對該計劃表達了各方面的關注,尤其是有關私隱保障方面,私隱專員作為監管保障個人資料私隱的規管者,認為依據條例第36條對該計劃所使用的個人資料系統進行視察(下稱「**該視察**」),以便對日後進行同類校園驗毒計劃的各方作出建議,是適合的做法。

Given the high sensitivity of the personal data collected and processed in the drug-testing program and the various public concerns expressed about the project, particularly as regards privacy protection, the Commissioner considered it appropriate to carry out an inspection of the personal data system ("**the Inspection**") used under the Scheme pursuant to section 36 of the Ordinance for the purpose of making recommendations to these parties who would carry out similar school drug testing programmes in the future.

該視察涵蓋資料處理的過程,包括由「徵求同意參與」至「把結果通知學生/家長/監護人」及「銷毀所有載有個人資料的相關記錄」。該視察包括五項主要工作,分別是查詢、文件審查、現場視察、訪談及問卷調查。私隱專員在視察報告中考慮作出建議時,是集中於該視察的結果,並參考條例附表1的六項保障資料原則的規定。

The Inspection covered the data-processing cycle, from "soliciting consent to participate" to "result notification to the students/parents/guardians" and "destruction of all the relevant records containing personal data". It encompassed five major types of works including enquiries, documentation review, site inspections, interviews and surveys. In considering the recommendations to be made in the Inspection report, the Commissioner focused on the results of the Inspection with reference to the requirements under the six Data Protection Principles in Schedule 1 of the Ordinance.

該視察已於2012年初完成。私隱專員欣悉該計劃的個人資料系統並沒有大的缺點。不過公署發現資訊科技及通訊系統和裝置的保安方面有一些缺點,需要作出補救行動。私隱專員將於2012年中發表視察報告,羅列視察結果及建議。

The Inspection was completed in early 2012. The Commissioner is pleased to find that there was no material deficiency in the personal data system used under the Scheme. However, the PCPD did spot, among other things, some deficiencies in the security safeguards of the information technology and communication systems and devices, which called for remedial action. A full Inspection report setting out the results of the Inspection and recommendations arising from the Inspection will be published in mid-2012.

資料使用者申報計劃
DATA USER RETURN SCHEME ("DURS")

根據條例第IV部，私隱專員獲賦權可指明資料使用者的類別，要求他們呈交載有條例附表3指明的「訂明資訊」的申報表，例如資料使用者持有的個人資料的類別，及使用該等個人資料的目的。專員須使用該等申報表，以備存一份資料使用者登記冊（下稱「該登記冊」），內載由該等資料使用者提供的訂明資訊詳情。該登記冊須公開予公眾查閱。條例讓私隱專員可酌情決定這計劃的範疇及推行時間。

Pursuant to Part IV of the Ordinance, the Commissioner is empowered to specify classes of data users and require them to submit data user returns containing information specified in Schedule 3 of 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 Commissioner shall use the Returns to maintain a register of data users ("the Register") containing particulars of the prescribed information supplied by the data users. The Register shall be made available for inspection by the public. The Ordinance leaves to the discretion of the Commissioner the scope and timing of the introduction of Scheme.

自條例於1996年實施以來，社會對個人資料私隱權利的意識日益提高。在這個趨勢下，再加上近幾年發生連串為傳媒廣泛報道的重大資料外洩事件，促使機構資料使用者需要制定負責任的資料政策及措施，而且有關政策及措施必須公開及具透明度。因此私隱專員準備分期實施該計劃，初期會涵蓋：(1)公營機構；(2)三大受規管行業，即銀行、電訊及保險業；及(3)擁有龐大會員（例如客戶忠誠計劃）的機構。私隱專員於2011年7月發出諮詢文件，徵詢代表屬於指明類別的資料使用者的團體的意見。公署曾諮詢政制及內地事務局（公營機構的統籌者）、香港銀行公會、存款公司公會、香港通訊業聯會及香港保險業聯會。公私營機構的持份者亦分別就這議題提出精闢的見解和意見。

Since the Ordinance came into operation in 1996, awareness of personal data privacy rights has been growing in the community. This trend, coupled with a series of major data breaches in recent years which gained widespread media attention, has underlined the need for organizational data users to have in place responsible data policies and practices, and to be open and transparent about them. The Commissioner, therefore, planned to introduce the DURS in phases. Initially, it will cover (1) the public sector, (2) three large regulated industries, namely, banking, telecommunications and insurance, and (3) organizations with a large database of members (e.g. customer loyalty schemes). He issued a consultation document in July 2011 to engage bodies representative of the specified classes of data users and to solicit their views. The Constitutional and Mainland Affairs Bureau (as the coordinator for the public sector), the Hong Kong Association of Banks, the Hong Kong Association of Restricted Licence Banks and Deposit-taking Companies, the Communications Association of Hong Kong, and the Hong Kong Federation of Insurers were consulted for their views and comments. Stakeholders from public and private sectors also provided insightful views and comments on the topic.

私隱專員會根據這次諮詢所收集的意見及評論，決定未來的路向。

The Commissioner will decide the way forward based on the views and comments received from the consultation.

核對程序
MATCHING PROCEDURE

在本年報期內，私隱專員共收到31宗核對程序申請，全部來自公營機構。

During the reporting year, the Commissioner received 31 applications for approval to carry out matching procedures. All of the applications came from public sector organisations.

經審閱後，私隱專員根據條例賦予的權力，在有條件的情況下批准8宗申請。2宗申請其後被申請人撤回。截至2012年3月31日，餘下21宗申請正由私隱專員考慮。

Upon examination, eight applications were approved subject to conditions imposed by the Commissioner under the Ordinance, whereas two were subsequently withdrawn by the applicants. As at 31 March 2012, the remaining 21 applications were under consideration by the Commissioner.

以下為私隱專員核准的部份個案：

Following are some of the matching procedures 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**
民政事務局 Home Affairs Bureau	公署同意民政事務局進行核對程序，將從「$6,000計劃」申請人所收集的個人資料，與入境事務處從持有香港身份證的人士所收集的個人資料互相比較，以確定申請人符合領取「$6,000計劃」的款項。 Consent was given to the Home Affairs Bureau to carry out a matching procedure to compare the personal data collected from "Scheme $6,000" applicants with the personal data collected by the Immigration Department from holders of the Hong Kong Identity Card, so as to establish the applicants' eligibility for payments under "Scheme $6,000".
勞工處 Labour Department	公署同意勞工處進行核對程序，將申領「鼓勵就業交通津貼計劃」下的交通津貼的申請人個人資料，與申領「交通費支援計劃」下的在職交通津貼的申請人個人資料互相比較，以避免向申請人發放雙重津貼。 Consent was given to the Labour Department to carry out a matching procedure to compare the personal data collected from the applicants for transport subsidies under the Work Incentive Transport Subsidy Scheme with the personal data collected from the applicants for transport subsidies under the On-the-job Transport Allowance under the Transport Support Scheme, so as to avoid double payment to the applicants.
社會福利署 Social Welfare Department	公署同意社會福利署進行核對程序，將社會福利署向「綜合社會保障援助計劃」的受惠人及「公共福利金計劃」下的高額傷殘津貼受助人所收集的個人資料，與教育局向特殊寄宿學校寄宿生所收集的個人資料互相比較，以避免向福利受助人發放超額津貼。 Consent was given to the Social Welfare Department to carry out a matching procedure to compare the personal data collected by the Social Welfare Department from the beneficiaries of the Comprehensive Social Security Assistance Scheme and the recipients of the Higher Disability Allowance under the Social Security Allowance Scheme with the personal data collected by the Education Bureau from boarders of special boarding schools, so as to avoid overpayment to the welfare recipients.
選舉事務處 Registration and Electoral Office	公署同意選舉事務處進行核對程序，將選舉事務處向登記選民所收集的個人資料與房屋署向資助房屋住戶所收集的個人資料互相比較，以確保選民登記冊的地址準確。 Consent was given to the Registration and Electoral Office to carry out a matching procedure to compare the personal data collected by the Registration and Electoral Office from registered voters with the personal data collected by the Housing Department from the occupants of subsidized housing, so as to ensure accuracy of the address information in the voter register.