倡導循規守法

# Promoting Compliance


公署不時公佈重要的循規審查及視察行動結果，讓資料使用者引以為誡。

The PCPD warns data users to learn the lessons from the compliance check reports and inspection reports.

# 自律守法 追求卓越

## Meeting more than minimum legal improvements

**審查及政策部負責處理市民及機構就條例提出的查詢；對資料使用者涉嫌不符合條例規定的做法進行循規審查及調查；視察個人資料的處理系統，以及向資料使用者就循規方面提出忠告和建議。**

**機構的資料外洩事故通報，以及機構提出的個人資料自動化核對程序申請，均由這部門處理。**

The Compliance and Policy Division deals with enquiries from members of the public and organisations concerning the Ordinance, carries out compliance checks and investigations on data user practices that might be inconsistent with the requirements under the Ordinance, and conducts inspections of personal data systems. It gives advice and makes recommendations to the data users concerned for improved compliance.

The division also handles data breach notifications from data users and applications for approval of automated personal data matching procedures.

## 諮詢工作

### 提取強積金權益

強制性公積金計劃管理局（下稱「積金局」）建議修訂《強制性公積金計劃條例》，擬將「末期疾病」納入提早提取強積金權益的理由。

僱主可使用為僱員向強積金計劃繳付的僱主供款所產生的累算權益，抵銷根據《僱傭條例》須向僱員支付的遣散費或長期服務金。若僱員以罹患末期疾病為理由提早提取強積金權益，強積金計劃受託人可否通知其僱主有關金額，積金局因此徵詢公署的意見。

公署去信積金局表示，披露強積金計劃成員的個人資料，包括末期疾病，若目的是讓該成員的僱主計算員工可得的遣散費或長期服務金實際金額的話，在這情況下，強積金計劃受託人對個人資料的使用，與其處理提早提取權益的目的未必直接有關。因此，須先取得有關成員的訂明同意，以符合保障資料第3原則。

另外，公署亦關注強積金計劃受託人如此披露個人資料，時間可能過早和不恰當，因為有關成員在獲取強積金權益時，可能仍會繼續工作而未有資格領取遣散費或長期服務金。另一個可能的情況是，該成員有可能基於《僱傭條例》下的其他理由，而失去領取遣散費或長期服務金的權利。

公署指出，如果要方便僱主計算員工的遣散費或長期服務金，強積金計劃受託人只需提供該僱主供款所產生的累算權益金額便足夠，而不必透露僱員提取權益的理由。

## CONSULTATION

### Withdrawal of MPF benefits

The Mandatory Provident Fund Schemes Authority ("MPFA") proposed amending the Mandatory Provident Fund Schemes Ordinance to include "terminal illness" as one of the grounds for early withdrawal of Mandatory Provident Fund ("MPF") benefits.

According to the Employment Ordinance, an employer can use the accrued benefits in an employee's MPF account derived from the employer's contributions to offset severance payments/long service payments ("SP/ LSP"). The MPFA therefore sought the PCPD's views on whether the MPF trustee could notify the employer of the amount of MPF benefits derived from the employer's contributions paid to the employee who had withdrawn the benefits on the ground of terminal illness.

The PCPD wrote to the MPFA stating that the disclosure of the MPF scheme member's personal data, including information about his/her terminal illness, to the member's employer for the purpose of calculating the actual amount of SP/LSP, may not be considered directly related to the trustee's handling of the claim for early withdrawal. Hence, according to DPP3, the prescribed consent from the member would be required.

Furthermore, the PCPD expressed concern that it would be premature and inappropriate for the MPF trustee to so disclose the personal data because the member might continue his/her employment and would therefore not yet be entitled to the SP/LSP by the time payment of the MPF benefits was made. There was also the possibility that the member might subsequently be excluded from the right to the SP/LSP for any reasons under the Employment Ordinance.

The PCPD also pointed out that for the purpose of facilitating an employer to calculate SP/LSP, the MPF trustee should only be required to provide the amount of accrued benefits derived from the employer's contribution, not the ground of withdrawal.

## 處理查詢

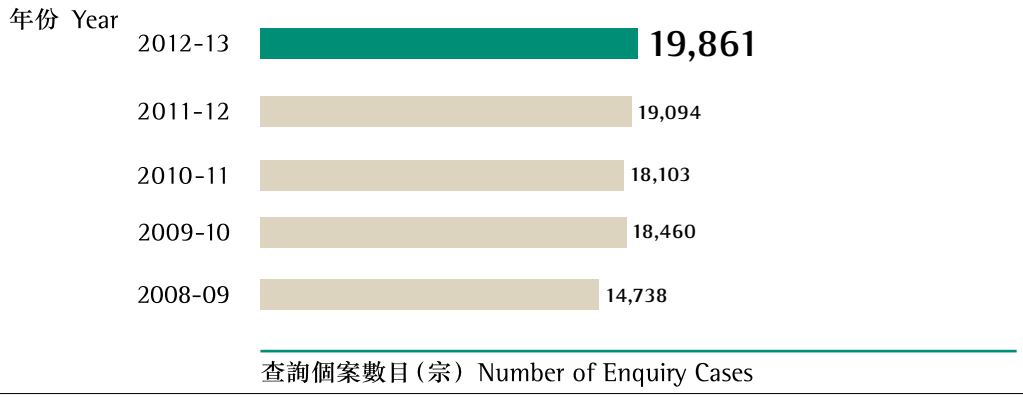
公署在本年度共處理19,861宗查詢個案，比上年度增加4%；平均每個工作天處理81宗查詢。(圖 4.1)

## HANDLING ENQUIRIES

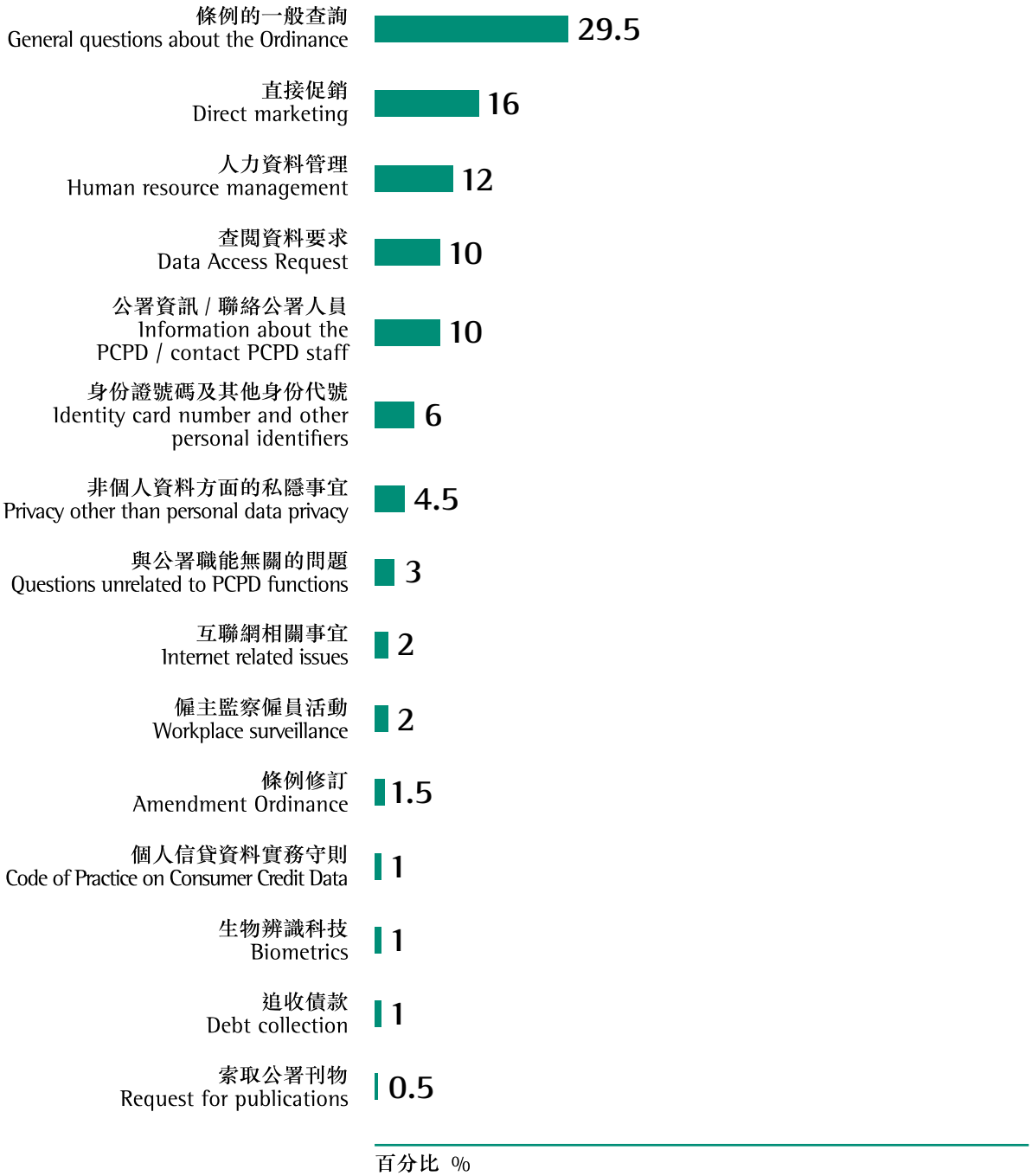
A total of 19,861 enquiry cases were handled during the year, 4 % up from the number of the previous year. On average, 81 enquiry cases were handled per working day. (Figure 4.1)

## 圖 4.1 – 全年查詢個案

## Figure 4.1 – Annual Enquiry Caseload




## 圖 4.2 – 查詢個案的性質　　Figure 4.2 - Nature of Enquiry Cases

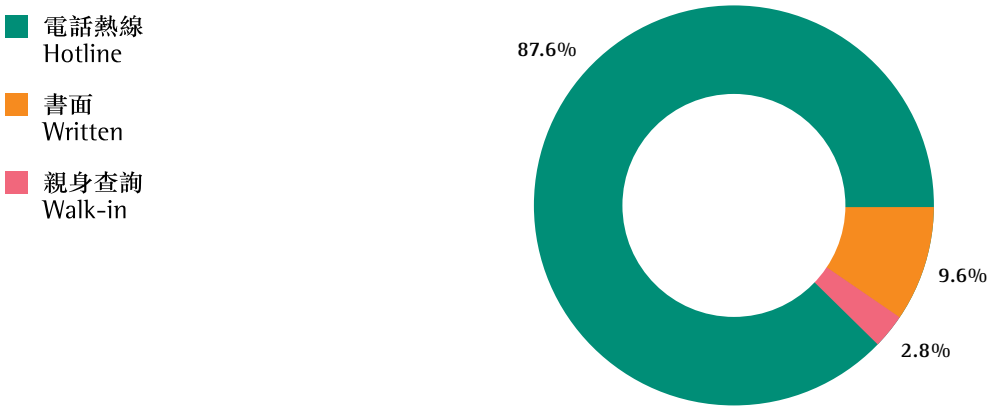


大部分(約88%)查詢經由公署的電話熱線(2827 2827)提出。(圖 4.3)

The majority of the enquiries (about 88%) were made via the PCPD hotline (2827 2827). (Figure 4.3)

## 圖 4.3 – 提出查詢的途徑

## Figure 4.3 – Means by which Enquiries were made




“我日常的工作是處理查詢。隨著社會對保護個人資料私隱的意識提高，不論是市民或是機構，都比以前更主動了解條例，以及就條例如何影響他們切身的事務諮詢公署。不同層面的人士對公署的工作越來越重視，我也感到欣慰。讓市民了解他們在條例下的權利；令資料使用者明白及切實履行他們在條例下的責任，是我努力不懈的動力。

My responsibility at the Office is handling enquiries. As overall awareness of data privacy soars, both members of the public and organisations are keener on finding out how the Ordinance can help and affect their interests and affairs. I am so pleased to see that the community has attached greater importance to what PCPD does in recent years – helping the public understand their rights and helping data users understand and fulfil their obligations under the Ordinance. That's the greatest motivation for me.”

**黃天賦** 個人資料主任
Michael WONG
Personal Data Officer

## 循規審查

當某機構的行事方式與條例規定看來有不相符時，私隱專員會展開循規審查。在完成循規審查行動後，私隱專員會書面告知有關機構，指出與條例規定不符或不足之處，促請有關機構採取適當的補救措施，糾正可能違規的情況，及防止類似情況再發生。

在本年度，私隱專員共進行了220次循規審查行動。

大部分(73%)的循規審查對象為私營機構，其餘則關乎政府部門和法定機構。

下文重點介紹在年內進行的部分循規審查行動。

### 院校網站管理失當　洩露學生私隱

公署跟進傳媒在2012年4月報道有學校網站洩露個人資料，向12間學校展開循規審查，證實其中9間學校的網站披露了2,115名學生的個人資料。

## COMPLIANCE CHECKS

The Commissioner conducts compliance checks into practices that appear to be inconsistent with the requirements under the Ordinance. Upon completion of a compliance check, the Commissioner alerts the organisation in writing, pointing out the apparent inconsistency or deficiency, and advising the organisation to take remedial action to correct the suspected breach and prevent further breaches.

During the year, the Commissioner carried out 220 compliance checks.

The majority (73%) of the compliance checks were conducted on private sector organisations, while the rest were on governmental departments and statutory bodies.

Below are highlights of some of the compliance checks conducted during the year.

### School website flaw exposing student privacy data

In the follow-up to a media report in April 2012, the PCPD commenced compliance checks on the practices of 12 schools which had allegedly leaked student data on their websites. The results confirmed that nine of the 12 schools had inadvertently exposed personal data on their websites, affecting 2,115 students.


專員指教育機構在保障個人資料方面欠缺警覺性和網上保安措施明顯不足。

The Commissioner remarked that the compliance check results reflect a serious lack of vigilance and adequate security measure on the part of educational institutions in safeguarding personal data.

披露的個人資料包括可識別資料當事人身份的姓名、學生編號(STRN)(在大部分情況下，該號碼與身份證號碼或出生證明書號碼相同)、學生及家長的電話號碼及學生電郵地址。個別個案更牽涉個人機密資料，如學生使用學校電腦設施的用戶名稱及登入密碼。

The personal data revealed included identifiable data, such as student name, Student Reference Number (STRN) (equivalent to Hong Kong identity card or birth certificate number in most cases), student and parent telephone numbers, and student email address. In several cases, confidential information such as user name and password for logon to the school IT system for online facilities was also exposed.

涉事的九間學校回應稱，資料外洩事件乃網站管理人員錯誤地將資料上載，或忘記將檔案從網站移除所致。其餘三間則表示網上的資料屬虛構以作教學用途。

The said nine schools explained that the data breaches were due to misplacement or prolonged retention of the information. The remaining three schools reported that the data concerned was fictitious and compiled for teaching purposes.

為了確定學校網站洩露個人資料的問題是否普遍，公署在互聯網上用關鍵詞進行搜尋，經過20小時的搜尋，找到來自21間教育機構(當中包括3間專上院校)、共39份包含個人資料的檔案。公署繼而對其中兩間專上院校展開循規審查，結果發現其中一間院校的個案影響範圍最大，涉及6,256名學生的資料。

To ascertain whether the problem of data leakage on the Internet was prevalent among local educational institutions, the PCPD conducted a 20 man-hour data search on the Internet based on certain keywords. It found 39 documents containing personal data from 21 educational institutions, of which three were tertiary institutions. The PCPD conducted compliance checks on two of these tertiary institutions, and subsequently concluded that the data breach at one institution involved the records of 6,256 students.

上述院校經公署知會循規審查結果後，已在網站刪除有關資料，以及要求搜尋器公司從伺服器刪除搜尋記錄的快取複本。

As a result of the compliance action, all the schools and tertiary institutions concerned have removed the leaked personal data from their websites and requested the relevant web search engine companies to remove cached copies from their servers.

公署已去信知會教育局是次循規審查的結果，以及建議當局就事件與其管轄範圍內的學校採取跟進行動。公署又特別安排了一次互聯網資料保安講座，受影響的學校都有指派職員出席。

The PCPD wrote to inform the Education Bureau of its findings and requested appropriate follow-up action in respect of all educational institutions under its general administrative purview. A follow-up talk on Internet information security was organised by the PCPD for the nominated staff of the affected schools.

## 某政府部門遺失存有個人資料的手提電腦

一個政府部門(下稱「部門」)向私隱專員呈報，遺失了三部筆記本型手提電腦，電腦儲存了5,161人的個人資料。涉及的個人資料源自該等人士的旅遊證件身份資料頁，包含個人的姓名、性別、出生地點、出生日期、國籍、證件相和旅遊證件號碼。

部門在回覆公署查詢時解釋，其中兩部電腦放置於一間房的架上充電，該房間只有獲授權人士可進入；另一部則放在當值人員的辦公桌上。部門懷疑牽涉偷竊，因此已向警方報案。

部門成立了專責小組，就電腦遺失事件展開內部調查，調查結果發現：

(1) 儲存在有關電腦上的個人資料已經加密處理，而流動影像掃描系統亦需要雙重認證才可登入；

(2) 電腦沒有受影響資料當事人的聯絡資料；

(3) 遺失電腦的部門單位並沒有就保安要求和監控措施制訂充足的執行指引。

事後，部門實施了一系列的糾正措施，以防同類事再發生，包括：

(1) 重設密碼和替換電子認證器；

(2) 更新系統伺服器的設定，以防止有人用遺失的電腦上載資料；及

(3) 提醒員工嚴格遵從部門指引所列出的規定。

部門亦採取了以下的預防措施，進一步減低遺失個人資料的風險：

(1) 加強內部監控程序；

(2) 應用流動裝置的資訊科技功能處理個人資料前，妥善評估收集、儲存、提取、保存和銷毀個人資料的程序的私隱風險；

(3) 整合各項針對使用流動裝置而制訂的指示和指引，以便員工參考；及

(4) 提供培訓，提升員工保護個人資料的意識。

## Loss of notebook computers containing personal data by a Government Department

A government department (the "Department") reported to the Commissioner that it had found missing three of its laptop computers, which contained the personal data of 5,161 individuals. The personal data involved the bio-data page of the individuals' travel documents, which had their name, gender, place of birth, date of birth, nationality, portrait and travel document number.

In response to our enquiry, the Department explained that two of the laptop computers had been placed on a rack for battery recharge in a room with restricted access, while the other had been placed on the Duty Officer's work desk. The Department considered the incident a case of suspected theft and therefore reported it to the Police for investigation.

The Department set up a Task Force to conduct an internal investigation into the incident. The investigation revealed that:-

(1) The personal data stored in the laptop computers had been encrypted, with two-factor authentication required to log in to the Mobile Imaging System;

(2) Contact information of the affected data subjects was not available; and

(3) The specific division of the Department responsible for the loss had not formulated adequate operation guidelines on security requirements and control measures.

After the incident, the Department implemented a series of remedial steps to prevent recurrence of similar incidents in the future, which included:

(1) Re-setting passwords and replacing e-tokens;

(2) Updating the settings of the system server to prevent uploading of information through the lost laptop computers; and

(3) Reminding staff to strictly adhere to the requirements stipulated in the departmental guidelines.

The Department also took the following preventive measures to further mitigate the risk of personal data loss in the future:

(1) Strengthening internal control procedures;

(2) Conducting proper risk assessment of the personal data being collected, stored, retrieved, retained and disposed of before implementing the IT functions for handling data through mobile devices;

(3) Consolidating instructions and guidelines specifically on the use of mobile devices for easy reference by staff; and

(4) Providing training to enhance staff awareness of personal data protection.

## 主動調查

### 零售商的顧客積分獎賞計劃過度收集個人資料，以及未能有效地與會員溝通

## PCPD-INITIATED INVESTIGATIONS

### Excessive collection of personal data and ineffective communication in retailers' customer loyalty programmes

**2010年發生八達通事件後，公眾對收集及使用個人資料作直接促銷活動的關注顯著提升。我期望香港的機構已汲取教訓，對資料保障規例更為關注。**

**After the Octopus incident in 2010, there was a significant increase in the public's awareness of the collection and use of personal data in direct marketing activities. I expect that corporations in Hong Kong would have learned a lesson and paid more attention to data privacy regulations.**

私隱專員於2012年10月11日發表四份調查報告，有關下述著名的顧客積分獎賞計劃在收集及使用會員個人資料的情況：

(1) 華潤萬家（香港）有限公司（下稱「華潤萬家」）營運的「積Fun咭」計劃；

(2) 牛奶有限公司（下稱「牛奶公司」）營運的「Mann Card計劃」；

(3) 屈臣氏集團（香港）有限公司（下稱「屈臣氏集團」）透過百佳及屈臣氏營運的「易賞錢計劃」。

On 11 October 2012, the Commissioner published four investigation reports on the collection and use of customers' personal data under the following prominent customer-loyalty schemes, namely:

(1) "Fun Fun Card", operated by China Resources Vanguard (Hong Kong) Company Limited ("CRV");

(2) the "Mann Card Program", operated by The Dairy Farm Company Limited ("DFC"); and

(3) the "MoneyBack Program", operated by A.S. Watson Group (HK) Limited ("ASW") through PARKnSHOP and Watsons.

這些在香港非常普遍的顧客積分獎賞計劃，任何18歲以上的消費者皆可登記。成功加入獎賞計劃的會員在指定的零售商店購物可累積獎賞積分，然後換取現金券作日後購物付款之用。會員亦可在指定的零售商店獲得特別折扣及計劃營運者的推廣優惠。

These customer loyalty programmes, which are very common in Hong Kong, are open for enrolment by consumers aged 18 or above. Members who have successfully enrolled in the programmes can accumulate reward points for purchases made at specified retail outlets. The reward points can be redeemed as cash vouchers for payment of further purchases. Members also receive special purchase discounts at the specified retail outlets and promotional offers from the programme operators.

私隱專員調查有關計劃，以確定收集申請人的個人資料及其後對有關資料的使用是否符合條例的保障資料第1及第3原則的規定。

The Commissioner investigated the programmes to ascertain whether the collection of the applicants' personal data and its subsequent use was in compliance with the DPP1 and DPP3 under the Ordinance.

私隱專員發現有關計劃營運者的違規行為有以下共通之處：

(1) 他們收集申請人的身份證號碼或護照號碼（全部或部分）（下稱「證件號碼」），以向申請人提供預設密碼，以使用計劃的網上服務，這構成不必要及超乎適度的收集，因此違反了第1(1)原則的規定，因為以任何字符已足夠達到預設密碼的同樣目的。

(2) 他們亦違反了第1(3)原則，沒有採取所有合理地切實可行的步驟，確保計劃申請人獲告知第1(3)原則所規定的事宜，例如資料的使用目的及有關資料可能轉移予甚麼類別的人。

The Commissioner found the following common contraventions among the programme operators:

(1) They had collected the applicants' Hong Kong Identity Card or passport number (complete or partial) ("ID number") for the purpose of providing them with a default log-in password to use the programme's online service. This amounted to unnecessary and excessive collection and thereby contravened DPP1(1), as any set of alpha-numerals would suffice for the same purpose.

(2) They also contravened DPP1(3) for having failed to take all reasonably practicable steps to ensure that programme applicants were notified of the matters required under DPP1(3), such as the purpose of use of the data and the classes of persons to whom the data might be transferred.

特別是，計劃營運者沒有界定或清楚界定資料的使用目的及/或資料承轉人的類別，令計劃申請人無法合理地確定其個人資料會被如何使用及誰可使用有關資料。雖然出現這些違規行為，但計劃營運者確認在實際上，資料的使用及轉移只限於與計劃目的直接有關的事宜。在沒有相反證據的情況下，私隱專員認為計劃營運者沒有違反第3原則的規定。

In particular, the programme operators had either failed to define or poorly defined the purpose of use of the data and/or class of data transferees, with the result that it would not be practicable for the applicants to ascertain with a reasonable degree of certainty how their personal data would be used and who would use the data. Despite these contraventions, the programme operators confirmed that in practice, the use and transfer of the data were restricted and directly related to the programme objectives. The Commissioner found no evidence to the contrary and hence there was no contravention of DPP3.

## 執法行動

就華潤萬家的「積Fun咭」計劃及牛奶公司的「Mann Card計劃」，私隱專員決定不送達執行通知，因為他信納該兩間公司已採取足夠步驟，對違規行為作出補救：

(1) 在調查過程中，他們已停止收集計劃申請人的證件號碼及出生年份(並非與計劃有關的必需資料)。

(2) 牛奶公司在調查期間已完全刪除之前在該計劃下所收集的證件號碼及出生年份資料，並修訂計劃申請表以符合資料保障第1(3)原則的要求。

(3) 華潤萬家已提供正式承諾書，承諾完全刪除之前在該計劃下所收集的證件號碼及出生年份資料，並修訂計劃申請表以符合資料保障第1(3)原則的要求。

私隱專員已向上述兩間公司發出警告，如它們日後在類似情況中沒有遵從條例的相關規定，專員會考慮對它們採取執法行動，包括送達執行通知。

至於「易賞錢計劃」，專員根據條例第50(1)條向屈臣氏集團送達執行通知，而該屈臣氏集團其後亦依從執行通知的指令，包括：

(1) 停止向計劃申請人收集部分證件號碼的做法；

(2) 完全刪除屈臣氏集團之前向計劃申請人及會員收集得的部分證件號碼；及

(3) 修訂計劃的條款及細則，以符合資料保障第1(3)原則。

網上閱覽調查報告：
www.pcpd.org.hk/chinese/publications/invest_report.html

## Enforcement Action

As for the investigations into the Fun Fun Card Scheme operated by CRV, and the Mann Card Program operated by DFC, the Commissioner decided not to serve an enforcement notice, as he was satisfied that both operators had taken adequate steps to remedy the contraventions:

(1) During the course of investigation, they had both ceased the collection of the programme applicants' ID numbers and years of birth (which was unnecessary for the purposes of both programmes);

(2) DFC had, during the course of the investigation, deleted all the ID numbers and years of birth previously collected, and revised the programme application documentation to meet the requirements under DPP1(3); and

(3) CRV had formally undertaken to the Commissioner to erase all the ID numbers and years of birth previously collected and redesign the programme application documentation to meet the requirements under DPP1(3).

Both operators were put on warning that enforcement action against them would be considered should they fail to comply with the Ordinance in similar situations in the future.

As regards the MoneyBack Program, the Commissioner served an enforcement notice pursuant to section 50(1) of the Ordinance on ASW in view of the continuing contraventions. The operator subsequently complied with the Commissioner's directives by:

(1) ceasing to collect partial ID numbers;

(2) deleting the partial ID numbers that it had previously collected; and

(3) revising programme terms and conditions to meet the requirements under DPP1(3).

Read the Investigation Reports online:
www.pcpd.org.hk/english/publications/invest_report.html

## 視察行動

### 視察港鐵閉路電視系統

公署根據條例第36條，於2012年6月至2013年2月期間視察港鐵車站公眾地方及列車車廂的閉路電視系統，包括實地視察11條路線的九個繁忙車站或轉車站及兩間車廠的閉路電視處理個人資料的系統，審閱相關的指引/政策以及訪問主要負責的職員。視察報告總結港鐵系統大致上遵從條例的規定，惟有可改進之處。

港鐵為本港最大的公共交通服務機構，每日載客量多達五百萬人次。港鐵在公眾地方安裝和使用的閉路電視攝錄機共有3,342部，在列車車廂內則有429部。港鐵347部列車當中有78部安裝閉路電視，平均每十架車廂有兩架有閉路電視；平均每日覆蓋逾一百萬名乘客。

裝有廿四小時攝錄鏡頭的位置包括港鐵路線車站的升降機、扶手電梯、樓梯、車站出入口、閘機位置及月台；及多個輕鐵車站的月台和路軌交接點。

從視察所得，根據《香港鐵路條例》、《香港鐵路規例》及《香港鐵路附例》，港鐵有責任調查鐵路事故和確保乘客安全，在運作上有合理理由安裝和使用閉路電視系統。整體來說，港鐵安裝的攝錄鏡頭都是可見和非隱蔽式的。

## INSPECTION

### Inspection of the MTR's CCTV system

The PCPD carried out an inspection of the Closed-Circuit Television System ("CCTV system") used by the MTR Corporation ("MTRC") in train stations and compartments, pursuant to section 36 of the Ordinance, between June 2012 and February 2013. It involved on-site inspection of the personal data system of the CCTV operating at nine interchanges or busy train stations with high traffic volume along the 11 rail lines and two train depots, a review of relevant manuals/guidelines, and interviews with key staff members involved in the operation of the CCTV system. The report concludes that the system complies with the requirements of the Ordinance but improvements are needed.

The MTRC is the largest public transport service provider in Hong Kong, carrying nearly five million passengers every weekday. It has installed and uses 3,342 CCTVs in the public areas of station premises and 429 CCTVs in train compartments. Of its 347 trains, 78 have CCTV installed. This means, on average, for every 10 compartments there are two CCTVs in operation, covering in excess of one million passengers every weekday.

Images are captured round the clock at various public locations, including lifts, escalators, staircases, entrances/exits, platforms and gate areas at MTR high-traffic rail stations, and a number of stations and junctions along Light Rail lines.

According to the inspection findings, the MTRC has statutory obligations under the Railways Ordinance, Railways Regulations and bylaws to monitor pre-incidents and investigate post-incidents, and to ensure safety of its service. The installation and use of the CCTV system for the purpose of performing such obligations were therefore justified. All MTRC CCTV cameras inspected by the Commissioner's officers were also overtly installed and visible.

惟視察過程發現幾項不足之處，有待改善：

- 港鐵在引入閉路電視系統前沒有進行私隱風險評估，因而未有仔細確立系統的資料流程和相關的私隱風險，以及採取措施減低風險。更重要的是，風險評估有助掌握更多數據，以消除公眾人士和持份者對私隱方面的憂慮。
- 在受視察的車站入口，「閉路電視攝錄進行中」告示普遍不夠顯眼；在屯門站和中環站的下車點沒有展示標準告示，內容亦過於簡單，例如告示未有顯示如何聯絡負責處理個人資料私隱事宜的港鐵職員。
- 在處理錄影片段方面，不同路線、類比和數碼攝錄系統所儲存錄影片段的保留時間不一；視察小組亦發現部分錄影片段的實際保留時間長於港鐵指引或其程序內所訂明的時間。
- 港鐵車務安全部職員共用查閱和儲存數碼錄映片段系統的密碼，個人資料外洩的風險因而增加。
- 視察小組發現港鐵人員使用未加密的USB記憶體複製、儲存及轉移由閉路電視系統所記錄的個人資料。

公署向港鐵提出多項建議，包括：

(1) 簡化及整合所有個人資料私隱政策及程序、指示及指引，令員工易於明白和遵行；

(2) 改善閉路電視通告的能見度及內容；

(3) 查閱電腦記錄及儲存閉路電視錄像的密碼不應共用以確保問責性及資料保安；及

(4) 港鐵應執行使用便提攜式儲存裝置(例如USB記憶體)的政策及程序，以防止閉路電視錄像在運送途中遺失或可能遭未經准許的查閱。

網上閱覽視察報告：
www.pcpd.org.hk/chinese/publications/files/R13_2768_c.pdf

However, some areas were found wanting:

- The MTRC had not conducted a Privacy Impact Assessment ("PIA") of the CCTV system. A PIA would have clearly identified the relevant data flow and associated privacy risks, and measures could have been taken to minimise or remove such risks. Importantly, it would have provided a credible source of information to allay any privacy concerns of the public and other stakeholders.
- The "CCTV in operation" notices at the entrances to the station premises inspected were not conspicuous or prominent, and non-standard notices were used at the drop off points at Tuen Mun Station and Central Station. All of the notices inspected did not contain sufficient information and did not include details of the officer to whom issues relating to personal data privacy should be addressed.
- On the handling of the MTRC's CCTV footage, retention periods vary for various lines and between the analogue and digital systems. Certain CCTV records were kept longer than the relevant retention period specified by the MTRC.
- The login account and password for access to and storage of footage in the Digital Video Recording System were shared among staff members of the Operations Safety Section. This arrangement is not conducive to user accountability and data security.
- USB thumb drives with no encryption facility were found to be used for copying, storage and transfer of personal data captured by the CCTV system.

The PCPD made a number of recommendations to the MTRC, including the following:

(1) All data privacy policies, procedures, instructions and guidelines should be consolidated and streamlined to promote compliance and user-friendliness;

(2) The visibility and content of the CCTV notices should be improved;

(3) Username and password access to computer recording and storage of CCTV footage should not be shared to ensure accountability and data security; and

(4) The policy and procedures on the use of portable storage devices (e.g. USB thumb drives) should be enforced to eliminate non-compliance.

Read the Inspection Report online:
www.pcpd.org.hk/english/publications/files/R13_2768_e.pdf

## 資料外洩通報

資料外洩事故一般是指資料使用者疑對其持有的個人資料保安不足，以致洩露資料，令資料可能被人未經授權或意外地查閱、處理、刪除、喪失或使用。資料外洩事故可能構成違反保障資料第4原則。公署敦請資料使用者一旦發生資料外洩事故，須通知受影響的資料當事人、私隱專員和其他相關人士。

接獲資料外洩事故通報（可用公署的指定表格呈報）後，公署會評估資料，以考慮是否有需要對有關機構展開循規審查。若私隱專員決定進行循規審查，會書面通知相關的資料使用者，並向機構指出明顯的不足之處，建議採取補救措施防止同類事故重演。

## DATA BREACH NOTIFICATION

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. The breach may amount to a contravention of Data Protection Principle 4. Data users are strongly advised to give formal data breach notification ("DBN") to the affected data subjects, the Commissioner and any other relevant parties after a data breach has occurred.

Upon receipt of a DBN from a data user (which can be submitted using the designated DBN form), the PCPD would assess the information provided in the DBN and consider whether a compliance check is warranted. For DBN cases which the Commissioner decides to conduct compliance checks, the Commissioner alerts the data users in writing, pointing out the apparent deficiency and inviting them, where appropriate, to take remedial action to prevent a recurrence of similar incidents.

在本年度，公署接獲 61 宗資料外洩事故通報
During the year, the PCPD received 61 Data Breach Notifications

（32 宗來自公營機構；29 宗來自私營機構
(32 from the public sector and 29 from the private sector)

牽涉 17,451 人的個人資料。公署對肇事機構展開 61 項循規審查行動。
affecting 17,451 individuals. In response, the PCPD conducted 61 compliance checks.

## 資料使用者申報計劃

根據條例第IV部，私隱專員有權指明某類別的資料使用者，要求他們提交申報表，呈報有關資料使用者持有的個人資料類別說明，以及使用該等資料的目的等。私隱專員使用該等申報表後，以備存資料使用者登記冊，列載有關資料使用者提供的訂明資料詳情。登記冊須供公眾查閱。條例賦予私隱專員酌情權，以決定此申報計劃的範圍和推行時間 。

公署於2011年7月發出諮詢文件，勾劃出「資料使用者申報計劃」的操作框架和實施規劃，並舉行簡佈會，收集公營機構、銀行、電訊和保險等在計劃實施第一階段受影響的行業團體的意見。

根據諮詢所收集的意見，公署了解有關行業團體對申報計劃旨在推動更高的保障個人資料私隱標準這目標並無異議，但有意見質疑申報計劃的形式不能達致上述目標。與此同時，公署留意到，本港「資料使用者申報計劃」借鑑經驗的歐盟資料保障制度正經歷改革，改革建議包括摒棄要求資料使用者申報的安排，取而代之是著重收集和使用個人資料須具問責性和透明度的改良制度。建議亦包括強制規定僱員人數達250人或以上的公、私營機構須設立資料保障主任的職位。

鑑於歐盟在這方面的動向，公署計劃暫緩推行申報計劃，直至歐盟改革完成為止，以便從中汲取經驗。

## DATA USER RETURNS SCHEME ("DURS")

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, such as descriptions of the kinds of personal data held by the data user concerned and the purposes for which they are used. The Commissioner uses the returns to maintain a register ("the Register") of data users containing particulars of the prescribed information supplied by the data users. The Register must 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 the scheme.

The PCPD issued a consultation document in July 2011 which sets out the operational framework and implementation plan of the DURS. The PCPD then conducted briefings and collected views from the industries to be regulated in the first phase of implementation of the DURS, namely, the public sector, banking, telecommunications and insurance.

The PCPD gathered from the consultation exercise that while there was no dispute over the objective of DURS to promote a higher standard in the protection of personal data privacy, there was scepticism about achieving the objective with this scheme. At the same time, the PCPD noted that the European Union ("EU") data protection system, upon which the proposed DURS was modelled, was undergoing reforms. Among other things, the EU was considering replacing the notification requirement with improved systems which emphasise accountability and transparency in the collection and use of personal data. That would include the mandatory designation of a data protection officer in public authorities and bodies, as well as private enterprises employing 250 persons or more.

In light of the EU developments, the PCPD planned to put the project on hold until the reforms in the EU have been finalised and useful lessons can be learnt from the exercise.

## 私隱管理系統

「資料使用者申報計劃」涵蓋的資料使用者在保障個人資料私隱方面，面對的公眾期望越來越高，公署提倡申報計劃實施最初階段所涉及的四個行業建立和採用「私隱管理系統」，以確保機構有適當的政策和程序，推動保障個人資料私隱的良好行事方式。推行「私隱管理系統」最起碼的效果，是反映機構具備遵從條例的能力。如果執行得宜，系統更可增強公眾對機構的信任和信心，提升機構的聲譽，最終達致的目標與「資料使用者申報計劃」一致。「資料使用者申報計劃」是基於嚴格遵行條例的規定，而「私隱管理系統」在保障個人資料的處理上更為靈活和整全，是替代「資料使用者申報計劃」的可取過渡方案。

## PRIVACY MANAGEMENT PROGRAMME ("PMP")

To meet the high public expectations for protection of personal data privacy among the data users covered by DURS, the PCPD has asked the four sectors involved in the initial phase of DURS implementation to develop and maintain a PMP which ensures appropriate policies and procedures promoting good privacy practices are in place. At the minimum, the outcome of a PMP would be a demonstrable capacity to comply with the Ordinance. If executed well, it would also promote trust and confidence among the public, enhance the organisation's reputation and thus serve the same purpose as the DURS. While the DURS operates on the basis of strict compliance with the requirements under the Ordinance, a PMP would be flexible and holistic in data protection, and serve as a good interim substitute for DURS.

## 個人資料的核對程序

在本年度，私隱專員共收到56宗個人資料核對程序申請，全部皆來自政府部門及公營機構。

經審閱後，私隱專員在有條件的情況下批准了52宗申請，否決了一宗申請。另外兩宗的申請人則撤回了申請。截至2013年3月31日，專員在考慮一宗申請。

## DATA MATCHING PROCEDURE

During the year, the Commissioner received 56 applications for approval to carry out matching procedures. All of the applications came from government departments and public sector organisations.

Upon examination, 52 applications were approved, subject to conditions imposed by the Commissioner. Two were subsequently withdrawn by the applicant and one was refused by the Commissioner. As at 31 March 2013, the remaining one application was under consideration by the Commissioner.

以下是私隱專員核准的部分個案：

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

| 提出要求者<br>Requesting Parties | 核准的資料核對程序詳情<br>Details of the Approved Data Matching Procedures |
|---|---|
| 選舉事務處<br>Registration and Electoral Office | 將選舉事務處從選民登記申請人收集的個人資料，與入境事務處收集的個人資料互相比較，藉以確定申請人的投票資格。<br>Comparing the personal data collected by the Registration and Electoral Office from voter registration applicants with the personal data collected by the Immigration Department, in order to determine the applicants' eligibility to vote. |
| 民政事務局<br>Home Affairs Bureau | 把關愛基金援助項目（為居住環境惡劣的低收入人士及其家庭成員提供津貼）的申請人資料，與土地註冊處收集的物業業主資料互相比較，從而確定申請人及其家庭成員是否符合受資助的資格。<br>Comparing the personal data collected from applicants of the Community Care Fund Assistance Programme, which provides a subsidy for low-income persons and their household members who are inadequately housed with the personal data collected by the Land Registry from property owners, in order to ascertain the eligibility of the applicants and their household members for the subsidy. |
| 香港警務處<br>Hong Kong Police Force | 把警務處收集的宿舍申請人/住戶及其配偶的資料，與房屋署的房屋住戶資料互相比較，以避免有申請人得到雙重房屋福利。<br>Comparing the personal data collected by the Hong Kong Police Force from the applicants/occupants of departmental quarters and their spouses with the personal data collected by the Housing Department from its tenants, in order to prevent the collection of double housing benefits. |
| 社會福利署<br>Social Welfare Department | 把綜合社會保障援助計劃受助人的個人資料，與勞工處收集的工作試驗計劃津貼申請人的資料互相比較，以避免向福利受助人提供雙重津貼。<br>Comparing the personal data collected from the beneficiaries of the Comprehensive Social Security Assistance Scheme with the personal data collected by Labour Department from applicants for the allowance under the Work Trial Scheme, in order to prevent double payments to welfare recipients. |

## 新的核對程序申請表

為資料核對程序申請而製備的新申請表，於2012年9月28日根據條例第31(1)條刊登於憲報，以作公佈。

新表格取締原有版本(於2010年3月刊憲)。由2012年9月30日起，資料使用者如要向私隱專員申請進行資料核對程序，須填妥新的申請表格。

## New Matching Procedure Form

On 28 September 2012, 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 superseded the form gazetted in March 2010. Data users are required to complete the new form when making a request for the Commissioner's consent to carry out a matching procedure after 30 September 2012.