

監察工作
Monitoring Compliance

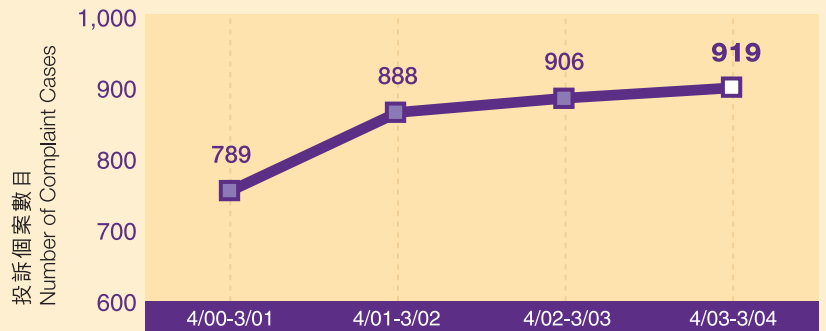


個人資料
(私隱)條例
PERSONAL DATA
(PRIVACY)
ORDINANCE

在二零零三至零四年度接獲的投訴個案

Complaints received during 2003-04

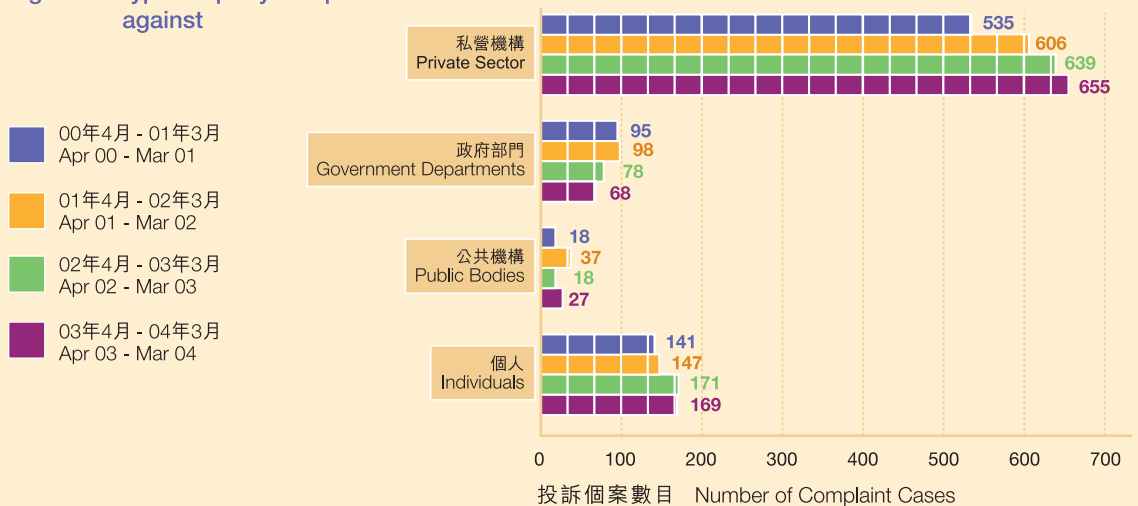
圖表1 — 每年的投訴個案
Figure 1 – Annual complaint caseload



■ 本年度公署共接獲919宗投訴個案(較去年度輕微上升了1.4%)。

■ A total number of 919 complaint cases were received in 2003-04 (a slight increase of 1.4% in comparison with the previous year).

圖表2 — 被投訴者的類別
Figure 2 – Types of party complained against



■ 本年度共接獲919宗投訴個案。

■ A total of 919 complaint cases were received in 2003-04.

■ 655宗(71%)個案投訴私營機構。

■ 655 (71%) complaint cases were against private sector organizations.


■ 169宗(19%)個案則投訴個人。


■ 169 (19%) complaint cases were against individuals.

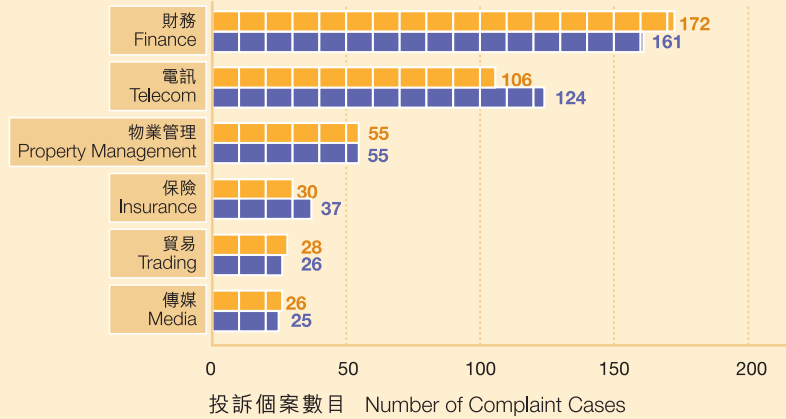
■ 95宗(10%)個案投訴公營機構(即政府部門及其他公共機構)。

■ 95 (10%) complaint cases were against public sector organizations (i.e. government departments and other public bodies).

圖表3 — 對私營機構的投訴
Figure 3 – Complaints against private sector organizations

 02年4月 - 03年3月
Apr 02 - Mar 03


 03年4月 - 04年3月
Apr 03 - Mar 04




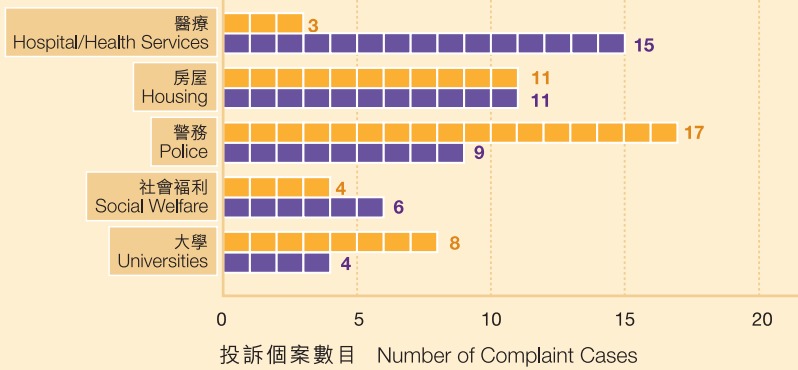
■ 在投訴財務機構或電訊業的個案中，大部份與在追收欠帳或服務費時被指使用個人資料有關。

■ The majority of the complaints against financial institutions or telecommunications industry concerned alleged use of personal data in recovery actions for overdue loans or service payments.

圖表4 — 對公營機構的投訴
Figure 4 – Complaints against public sector organizations

 02年4月 - 03年3月
Apr 02 - Mar 03

 03年4月 - 04年3月
Apr 03 - Mar 04



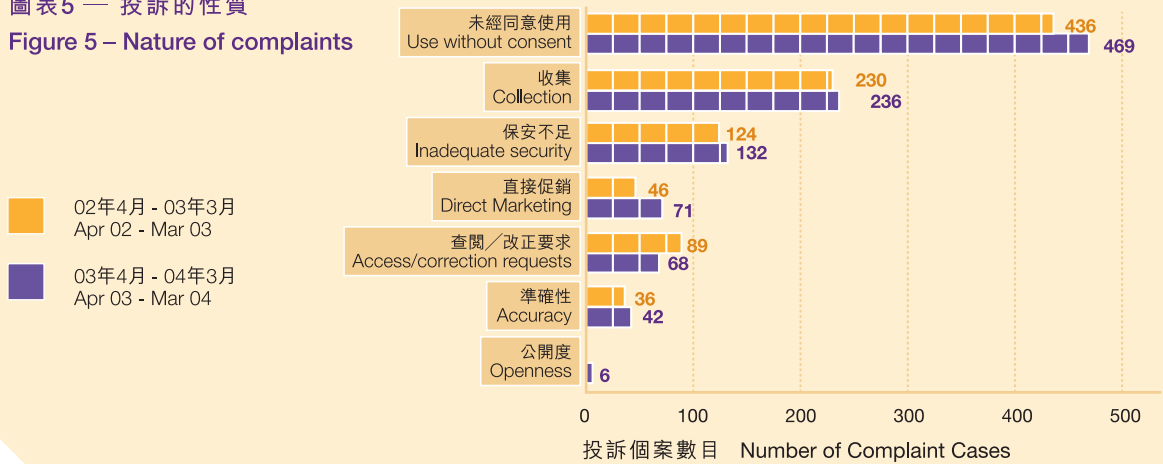
■ 在投訴公營機構的個案中，大部份被指與不符收集目的及未取得當事人同意而使用個人資料(36%)及未能遵守查閱資料要求(24%)有關。

■ The majority of the complaints against public sector organizations concerned alleged use of personal data outside collection purpose and without the consent of the individual (36%) and non-compliance with data access requests (24%).

個人資料 (私隱)條例 PERSONAL DATA (PRIVACY) ORDINANCE

圖表5 — 投訴的性質

Figure 5 – Nature of complaints



- 本年度接獲的919宗投訴個案共涉及1,024項被指違反私隱條例的規定。在這些投訴事項中，885項(86%)被指違反附表中的保障資料原則，餘下的139項(14%)則被指違反私隱條例的主體條文。
- 在885項被指違反保障資料原則的個案中，469項(53%)涉及在未獲投訴人同意前，涉嫌將個人資料使用於原有收集目的以外的目的。在這類個案中，106項(23%)涉及財務機構被指將客戶的個人資料，例如聯絡資料及欠帳額，轉交收數公司作追收欠債用途。

- The 919 complaints cases received in 2003-04 involved a total of 1,024 alleged breaches of the requirements of the PD(P)O. Of these, 885 (86%) were alleged breaches of the data protection principles scheduled to the PD(P)O while 139 (14%) were alleged contraventions of the provisions in the body of the PD(P)O.
- Of the 885 alleged breaches of the data protection principles, 469 (53%) concerned the alleged uses of personal data of complainants without their consent for purposes other than the purposes for which the data were collected. In this category, 106 (23%) involved debt collection, mostly allegations against financial institutions for passing customers' personal data, such as contact details and amounts of indebtedness, to debt collecting agencies for recovery of outstanding debts.

與上年度的情況相若，有些投訴人對私隱條例在收數活動方面的適用範圍仍然有所誤解。在一些個案中，投訴人似乎利用向公署作出投訴這個渠道來規避債權人(例如財務機構)向他們追收欠債。一般來說，債權人將欠債人的個人資料移轉給代理人追收欠債，此舉符合原有收集資料的目的。如只移轉收債目的所需的資料，並且在最初收集資料時給予債務人通知，如此使用資料不一定會構成違反私隱條例的問題。

Like the last reporting year, there has still been a misunderstanding on the part of some complainants about the ambit of the PD(P)O when applied to debt collection activities. There were again a number of cases where complainants seemingly tried to use the PCO's complaint channel to stall creditors such as financial institutions from collecting their debts. The transfer of personal data of a debtor from a creditor to its agent for collecting debt owed is normally within the original collection purpose of the data. Such use of the data may not raise any issue under the PD(P)O if only data that are necessary for the debt collecting purpose are transferred and prior notice has been given to the debtor at the time of collection of the data from the debtor.

投訴調查

在本年報期開始時，公署正處理上年度帶下來的203宗投訴，加上新收到的919宗投訴，公署在本年報期內共處理了1,122宗投訴。在這些個案中，367宗(33%)在作出初步審閱後不獲公署繼續受理，理由是其中的348宗的表面證據並不成立，無法支持有違私隱條例規定的指控，另外18宗不屬私隱專員的權力範圍，其餘1宗則為匿名投訴。餘下的755宗(67%)經審閱後獲進一步處理，其中598宗(79%)在本年報期內已得到解決，而餘下的157宗(21%)在二零零四年三月三十一日時仍在處理中(圖表6)。

Complaint Investigations

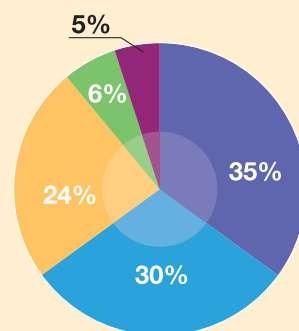
At the beginning of the reporting year, 203 complaints were being processed. Together with the 919 new complaints received, the PCO handled a total of 1,122 complaints during the reporting period. Of these, 367 cases (33%) were declined for further action after preliminary consideration on the basis that 348 of them were found to have no *prima facie* case to support allegations of breaches of the PD(P)O. A further 18 cases were outside the Privacy Commissioner's jurisdiction and the remaining one was anonymous complaint. The other 755 cases (67%) were screened-in for further consideration. Of these, 598 cases (79%) were resolved during the reporting year and the remaining 157 cases (21%) continued to be handled on 31 March 2004. (Figure 6)

圖表 6 — 二零零三至零四年度處理的投訴摘要
Figure 6 – Summary of complaints handled in 2003-04

	2000-01	2001-02	2002-03	2003-04
上年轉來的投訴 Complaints carried forward	94	146	157	203
接獲的投訴 Complaints received	789	888	906	919
經處理的投訴的總數 Total complaints processed	883	1,034	1,063	1,122
經審閱後不再處理的投訴 Complaints screened-out	352	394	359	367
經審閱後繼續處理的投訴 Complaints screened-in	531	640	704	755
完結 Completed	385	483	501	598
處理中 In process	146	157	203	157

圖表 7 — 調查結果

Figure 7 – Outcome of investigations

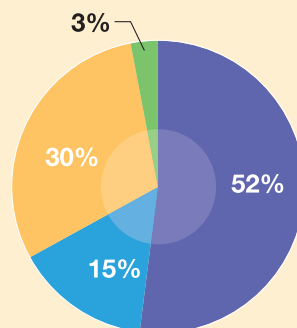
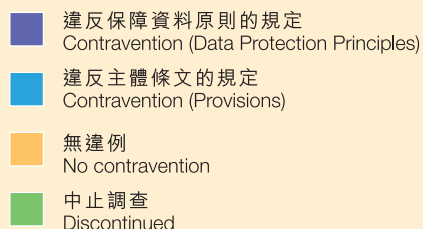


在本年報期內完結的598宗個案中，178宗(30%)透過調解得到解決，27宗(5%)在進行正式調查後得到解決，209宗(35%)在進行初步查詢後發現證據不足，146宗(24%)在初步查詢期間由投訴人撤回。餘下的38宗(6%)投訴個案，投訴人亦同時將有關個案交其他規管機構跟進。

Of the 598 cases completed during the reporting period, 178 (30%) cases were resolved through mediation, 27 (5%) cases were resolved after formal investigations, 209 (35%) cases were found to be unsubstantiated as a result of preliminary enquiries and 146 (24%) cases were withdrawn by the complainants during preliminary enquiries. The remaining 38 (6%) cases involved complaints where the complainants had also reported the matters to other authorities to follow up.

圖表 8 — 正式調查

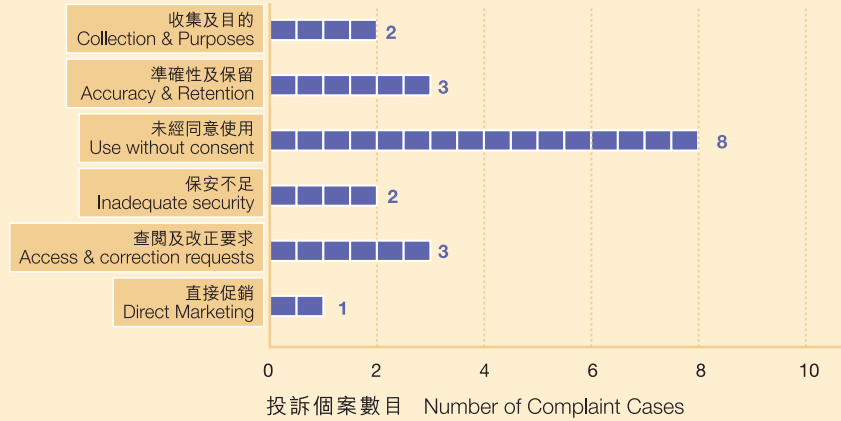
Figure 8 – Results of formal investigations



在本年報期內完成正式調查的27宗個案中，公署發現其中18宗(67%)違反了條例的規定，8宗(30%)並無違例或因缺乏充份證據而無法證明有違例情況。至於餘下一宗(3%)則應投訴人的要求中止調查。

Of the 27 formal investigations completed during the reporting period, the PCO found contravention of the requirements of the PD(P)O in 18 (67%) cases. In 8 (30%) cases, there was no contravention found or contravention was not established due to lack of sufficient evidence. The one remaining case (3%) was discontinued by request of the complainant.

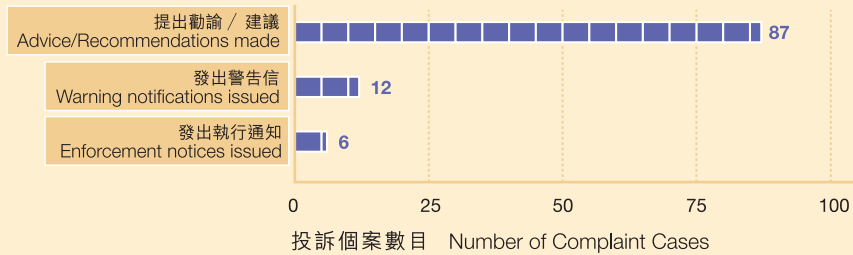
圖表9 — 違例事項
Figure 9 – Issues of contravention



在違反條例規定的18宗個案中，14宗違反一項或以上在附表中的保障資料原則，其餘4宗違反了條例的主體條文的規定，當中所涉及的違例事項與依從查閱資料要求及直接促銷有關。

Of the 18 cases where the requirements of the PD(P)O were found to have been contravened, 14 cases involved contravention of one or more of the data protection principles. The remaining 4 cases involved contravention of the provisions in the body of the PD(P)O relating to compliance with data access requests and direct marketing.

圖表10 — 根據調查結果採取的行動
Figure 10 – Actions taken as a result of investigation



在178宗透過調解得到解決的個案中，公署向87間機構提出勸諭及建議，以協助它們在行事方式及程序上遵守保障資料的規定。

In the 178 cases resolved through mediation, the PCO provided advice and recommendations to 87 organizations on their practices and procedures in order to assist them in complying with the data protection requirements.

在違反條例規定的18宗個案中，公署共向有關機構發出12封警告信，其中亦有要求該等機構作出書面承諾，答應採取措施糾正有關違例情況。在所有要求承諾的個案中，有關機構均按照公署的要求作出承諾，公署因而毋須採取強制性行動，即不須向有關機構發出執行通知。

In the 18 cases in which requirements of the PD(P)O were found to have been contravened, the PCO issued 12 warning notices to the organizations concerned, some of them were required to give written undertakings to implement measures to remedy the contraventions. In all these cases, the organizations gave the undertakings sought, and given such undertakings, enforcement action through the issue of an enforcement notice was not deemed to be necessary.

在其餘6宗個案中，公署向被投訴者發出執行通知，指令他們採取糾正措施，以防止他們繼續或重複違反條例的規定。

In the other 6 cases, enforcement notices were served on the parties complained against to direct them to take remedial actions to prevent their continued or repeated contravention of the PD(P)O.

循規查察行動

當發現某一機構的行事方式，看來有違私隱條例規定時，公署便會展開循規查察行動。在該等情況下，公署會以書面知會有關機構，指出看來與條例規定不符的事宜，並請有關機構採取適當的補救措施。在大多數情況下，有關機構會自動採取即時措施糾正涉嫌違例事項。在其他情況下，有關機構會就如何採取改善措施，以免重複涉嫌違例事項，向公署尋求意見。

在本年報期間，公署共進行了10次循規查察行動，對資料使用者被指可能違反條例規定的行事方式進行循規查察行動。下表列示年內進行的一些循規查察行動：

Compliance Checks

A compliance check is undertaken when the PCO identifies a practice in an organization that appears to be inconsistent with the requirements of the PD(P)O. In such circumstances, the PCO raises the matter in writing with the organization concerned pointing out the apparent inconsistency and inviting it, where appropriate, to take remedial action. In many cases, the organization concerned takes the initiative and responds by undertaking immediate action to remedy the suspected breach. In other cases, organizations seek advice from the PCO on the improvement measures that should be taken to avoid repetition of suspected breaches.

During the reporting year, the PCO conducted 10 compliance checks in relation to alleged practices of data users that might be inconsistent with the requirements of the PD(P)O. The following are some of the compliance checks undertaken in the year.

問題 Issues

一間職業介紹所在發給所有之前曾提供個人資料的求職者的電郵中，在收件人一欄列示了所持有的電郵「地址簿」中的收件人的資料。每位接獲電郵的收件人因而可得知其他收件人的姓名和電郵地址。

In an email sent by an employment agency to all job seekers who have previously provided their personal data, the agency addressed recipients of the email by using information about them held in its email “address book”. A recipient of the email can read the names and email addresses of others.

建議採取的改善措施 Improvement Measures Recommended

求職者許多時以密件方式向職業介紹所提供個人資料，並且期望介紹所亦用密件的方式與他們聯絡。有關的職業介紹所採用的方法雖然方便，但卻可能不必要地披露了有關個人的姓名及電郵地址。如電郵「地址簿」的設定將個人的姓名及電郵地址連結起來，則在使用「地址簿」同時向多人發送電郵時必須小心行事。在此個案的情況下，有關職業介紹所應考慮使用「隱藏副本收件者」(blind carbon copy (“bcc”))的方法向各收件人發送電郵。

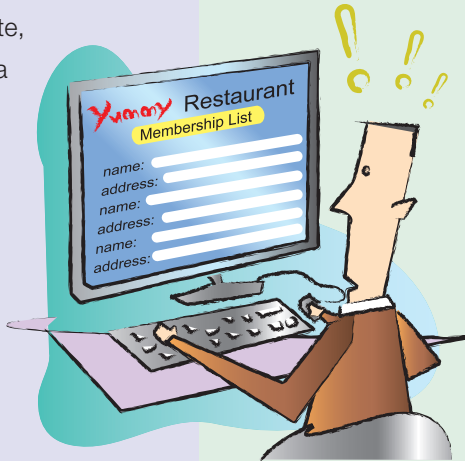
Very often, job seekers provide their personal data under confidence to an employment agency and would expect the agency to communicate with them on a confidential basis. Although the way that the agency sends the email can bring convenience, it may lead to an unnecessary disclosure of the names and email addresses of individuals. Where an email “address book” is configured to link an individual’s name with his email address, care should be taken when using the “address book” to send emails to multiple recipients. In the circumstances, the alternative of addressing recipients using the “blind carbon copy” (“bcc”) function should be considered.



問題 Issues

當網頁瀏覽者瀏覽一間食肆的網站時，按下其中一頁的超連結，可閱覽載有食肆顧客個人資料的資料庫。

When visiting a page on a restaurant's website, visitors are provided a hyperlink that directs them to a database that contains personal data of customers of the restaurant.



建議採取的改善措施 Improvement Measures Recommended

在維修或重新設計網頁時，機構應小心確保公眾人士不能隨意查閱不擬披露的個人資料。如網站尚未準備妥當待用，良好的行事方式是提示瀏覽者網站「尚在編寫／發展中」，並且告知他們暫時不能使用超連結。

When performing website maintenance or re-design of web pages, care should be taken to ensure that control on public access to information not intended for disclosure can still be maintained. When a website is not ready for use, it would be a good practice to alert visitors that the site is “under construction/development” and to inform them of the temporary suspension of any hyperlink access.

個人信貸報告中在列示來自公眾法院文件的令狀資料時，有關資料可能有誤導成份。

Information contained in an individual's credit report may be misleading when it shows the writ information obtained from public court documents.

信貸報告可能載有資料當事人的令狀資料。在缺乏獨一無二的個人身份代號以作正確核對的情況下（法院文件屬此等情況），將該等資料與有關個人聯繫起來時必須小心行事。該等資料可能將姓名類似但不相同的其他人士的令狀資料與有關人士聯繫起來，導致出現錯配的情況。為免誤導，信貸報告應載有一項明確訊息，例如將此類公眾記錄資料載於信貸報告的另一頁，標題為「可能相關的公眾記錄資料」。

A credit report may display writ information concerning an individual who is the data subject. In the absence of any unique personal identifier (as in the case of court documents) that may facilitate correct matching, care should be taken when relating such information to the individual concerned. A mis-match may occur that results in writ information of another person with similar but not identical name being associated with the individual. To avoid any misleading effect, a clear message should be displayed in the credit report, e.g. to put this kind of public information under a heading that reads “Public Record of Potential Relevance” on a separate page of the report.

問題 Issues

乘搭來往香港與澳門渡輪的乘客須填寫旅客資料表格，填報姓名、電話號碼、地址及座位編號等個人資料。

Passengers traveling on ferries between Hong Kong and Macau are asked to complete a passenger information form that requires personal data such as the name, telephone number, address and seat number.



建議採取的改善措施 Improvement Measures Recommended

在「沙士」這種傳染病爆發期間，各方面有需要採取預防措施以確保公眾衛生及安全，這是可以理解的。利用衛生當局發出的「健康申報表」收集乘客的個人資料是偵測及控制「沙士」擴散至社區的其中一種方法。不過，衛生當局並無制訂政策，亦無規定渡輪營辦者必須收集乘客的個人資料，以防止「沙士」重臨。故此，有關渡輪公司被勸喻停止採用有關手法。

It is understandable that precautionary measures need to be taken to ensure public health and safety during the outbreak of SARS, which is a communicable disease that occurred worldwide. The collection of passengers' personal data by means of a "Health Declaration Form" issued by the Health Authority is one of the means that serve to detect and control the spread of SARS in the community. However, it is neither the policy of the Health Authority nor a requirement imposed on ferry operators to collect personal data of passengers for the prevention of resurgence of SARS. The ferry operator was advised to cease the practice.

核對程序

在本年報期間，公署共收到5宗新的核對程序申請，以及28宗對繼續進行過去數年已獲准的核對程序的重新申請。5宗新申請全部均來自公營機構。公署審閱後發現其中一宗申請與去年已核准的核對程序有關，因而毋須另行給予核准。另外一宗申請不屬私隱條例釋義所指的核對程序。其餘3宗申請則在有條件的情況下獲得批准。

Matching Procedures

During the reporting year, the PCO received 5 new applications for approval to carry out matching procedures and 28 requests for re-approval to continue matching procedures approved in previous years. All these five new applications were requested by public sector organizations. Upon examination, one application was found to pertain to a matching procedure which has already been approved and therefore a separate consent is not required whereas another one was found not to be a matching procedure as defined under the PD(P)O. In respect of the other 3 applications, they were approved subject to certain conditions.

提出要求者

Requested party

獲准的有關核對程序

Related matching procedures that were approved

香港房屋協會
Hong Kong Housing Society

將受市區重建計劃影響的業主／租客的個人資料與香港房屋委員會收集的資料 — 其他公共房屋福利的房屋管理綜合系統的資料庫作出比較，以防止他們享用雙重福利。
To prevent double housing benefits from being granted to those landlords and / or tenants affected by the Urban Renewal Projects by comparing their personal data with data collected by the Hong Kong Housing Authority - the Integrated System for Housing Management database in respect of other public housing benefits.

學生資助辦事處
Student Financial Assistance Agency

將幼稚園學費減免計劃下的經濟資助申請人的個人資料與幼兒中心繳費資助計劃所收集的資料互相比較，以防止有關申請人享用雙重福利。
To prevent double benefits from being granted to applicants for financial assistance under the Kindergarten Fee Remission Scheme by comparing their personal data with data collected under the Fee Assistance Scheme for Child Care Centre.

社會福利署
Social Welfare Department

將綜合社會保障援助受助人的個人資料與入境處的出入境記錄互相比較，以找出未有申報及未能符合居留規定的綜援受助人。
To identify applicants of Comprehensive Social Security Assistance who failed to report and meet the residence requirement by comparing their personal data with data with the Immigration Department in respect of their travel movement records.

關於違反《個人資料(私隱)條例》的作為或行為的概述

下文簡述公署在二零零三至二零零四年度調查投訴個案時發現的一些違反私隱條例規定的作為或行為。公署是基於有關事件的實況作出挑選，旨在述明受私隱條例(包括保障資料原則)管限的各種行為的多样化情況。

Highlights of acts or practices found in contravention of the PD(P)O

Provided below are brief illustrations of some of the acts or practices that were found to have contravened the requirements of the PD(P)O in the complaint investigations completed in 2003-2004. They are selected on the basis of subject matter and demonstrate the wide variety of conduct that are subject to the requirements of the PD(P)O, including those of the data protection principles (“DPPs”).

銀行謹防：依賴中介人轉介未經核實的信貸申請而查閱信貸資料 — 保障資料第1原則

Bankers beware: when accessing credit data in reliance of unverified credit application referred by an intermediary — DPP1

1/04

投訴內容

一名獨資經營者投訴一間銀行在未獲他的授權及無理由的情況下，查閱信貸資料服務機構持有關於他的信貸資料，以及取得一份有關他的信貸報告。

有關銀行聲稱在收到中介人轉介的信貸申請後，為了核對信貸申請人的信貸狀況，於是向信貸資料服務機構查閱該獨資經營者的信貸資料，並且取得一份信貸資料副本。銀行並無聯絡該名被號稱為信貸申請人的個人，亦無在查閱他的信貸資料前先取得他的書面授權。

調查結果

私隱專員發出的《個人信貸資料實務守則》容許信貸提供者在向個別人士批出新的信貸時，可透過信貸報告查閱信貸資料服務機構所持有關於該人的信貸資料。本個案的獨資經營者實際上有否申請信貸實在成疑。銀行在未核實申請的真確性前查閱有關人士的信貸報告，在本個案中的情況下屬不公平地收集個人資料，有違保障資料第1(2)原則的規定。

公署向有關銀行發出執行通知。銀行其後改變處理由中介人轉介的信貸申請的做法及程序，規定必須直接向申請人核實信貸申請。

The Complaint

An individual who is the sole proprietor of a business, complained that a bank, without his authority and without cause, accessed and obtained his credit data held by a credit reference agency through a credit report.

The bank alleged that it received a credit application referred by an intermediary and in order to check the credit status of the purported credit applicant, i.e. the sole-proprietorship, the bank accessed and obtained the sole-proprietor's credit data held by the credit reference agency. The bank did not contact the purported credit applicant nor had it obtained any written authorization from the sole proprietor prior to accessing his credit data.

Outcome of Investigation

The Code of Practice on Consumer Credit Data issued by the Privacy Commissioner allows a credit provider, through a credit report, to access consumer credit data held by a credit reference agency on an individual in the course of the consideration of any grant of new consumer credit to the individual. It was doubtful as to whether the sole proprietor had actually made the credit application. The bank's access to the credit report without first verifying the truthfulness of the application was considered unfair collection of personal data in the circumstances of the case amounting to a contravention to the requirement of DPP1(2).

An enforcement notice was issued and the bank subsequently changed its practice and procedure in relation to credit application referred by an intermediary, requiring direct verification of the application with the applicant.

控方證人的個人資料：避免披露與審理案件無關的個人資料 — 保障資料第3原則

2/04

Prosecution witness' personal data: avoid disclosing personal data unrelated to the purpose of the proceedings — DPP3**投訴內容**

一名證人向某個政府部門提供一份口供記錄，作檢控違例者之用。證人須在有關部門使用的標準口供表格填寫她的個人資料，包括姓名、年齡、性別、身份證號碼、出生地點、國籍及所操方言、地址、住宅電話號碼、職業及辦事處電話號碼。有關部門在證人不知情及未取得她的同意前，將一份未刪裁，當中載有證人上述的所有個人資料的口供記錄副本給予被告人。證人對該部門向被告披露該等屬其私人及個人的資料表示憂慮，因而向公署投訴。

調查結果

毫無疑問，口供記錄中的資料是為檢控目的而收集，故將口供記錄中的資料移轉給辯方作答辯之用與收集個人資料的目的是直接有關的。不過，據理解，檢控當局長久以來的做法是將口供記錄中與審理案件無關的證人個人資料刪除，例如證人的地址、電話號碼及工作地點(如適用)。在本個案中，證人的身份證號碼、地址(即工作地點)、聯絡電話號碼及出生地點與審理案件無關。故此，向被告披露這些資料不屬原有收集作為審理案件的目的或直接有關的目的。故此，在未取得證人的訂明同意前，不得將這些資料披露或移轉給被告人。有關部門由於未向證人取得所需的同意，因而違反了保障資料第3原則的規定。

公署向有關部門發出執行通知。為糾正上述事宜，該部門其後修訂了工作指南，特別是規定各職員在向辯方發出口供記錄副本前，必須檢視及刪裁有關副本，以免披露與審理案件無關的證人個人資料。

The Complaint

A witness provided a statement to a government department for the purpose of prosecuting an offender. The department's standard statement form was used which required the witness to fill in her personal particulars including name, age, sex, identity card number, place of birth, nationality & dialect, address, residential telephone number, occupation and office telephone number. An unedited copy of the witness statement, containing all the witness' personal particulars, was released to the defendant by the department without the prior knowledge or consent of the witness. The witness was concerned about the disclosure of such private and personal information to the offender and made a complaint to the PCO.

Outcome of Investigation

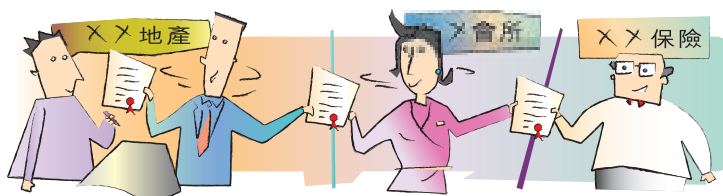
It was not disputed that the information collected in the witness statement was for the purpose of prosecuting the subject case and hence the transfer of the statement to the defence to answer the charge was for a directly related purpose. However, it was understood to be the long standing practice of the prosecuting authority to edit out witness' personal information from a witness statement, such as the address, telephone numbers and, where applicable, the place of employment of a witness which are irrelevant to the proceedings in question. In the instant case, the identity card number, address (i.e. place of employment), contact telephone numbers and place of birth bore no relevancy to the proceedings. The disclosure of these data to the defendant was therefore not accepted to be for the original purpose of collection or for a directly related purpose for the proceedings. These data should not therefore be disclosed without the prescribed consent of the witness. Without obtaining the requisite consent from the witness, the department had acted contrary to the requirement of DPP3.

An enforcement notice was issued and as a result the department revised its working manual to remedy the matters by, *inter alia*, requiring staff to review and edit copy witness statements before releasing to the defence so as not to disclose personal particulars of witnesses that were irrelevant to the proceedings in question.

移轉顧客的個人資料：不是明示及自願給予的同意並非「訂明同意」，不得據此而將顧客的個人資料送交第三者促銷無關的產品 — 保障資料第3原則
Transfer of customers' personal data: consent not expressly and voluntarily given is not "prescribed consent" to justify transfer of customers' data to third parties for promotion of unrelated products — DPP3

投訴內容

一名顧客透過地產代理租賃一個樓宇單位。有關地產代理將他的個人資料轉交其經營會籍的附屬公司。該經營會籍的公司以書面指出如顧客不反對，他會自動擁有該會籍。該經營會籍的公司並無收到顧客提出的反對。其後，經營會籍的公司與一間保險公司進行聯合促銷活動，並且將該顧客的姓名、聯絡資料及身份證號碼送交保險公司。保險公司其後致電該名顧客促銷人壽保險產品。該名顧客投訴地產代理不當地使用他的個人資料。



The Complaint

A customer rented a flat through the service of a property agency. The agency transferred his data to a club operated by its subsidiary. The club sent a letter to the customer notifying him that he would automatically become a member of the club if he failed to object. The club did not receive any objection from the customer. The club later engaged in a joint marketing scheme with an insurance company and passed the customer's name, contact details and identity card number to the insurance company. The insurance company then called the customer to promote its life insurance products. The customer complained about improper use of his personal data by the agency.

調查結果

保障資料第3原則禁止將顧客的個人資料使用(包括移轉)於原本收集目的以外的目的，或不是與原本目的直接有關的目的，除非事前已取得有關個人的「訂明同意」。明顯地，此個案中的地產代理是為了提供樓宇單位的租賃服務的目的而收集有關顧客的個人資料，而在收集資料時，地產代理並無述明會將有關資料使用於其他目的。有關會籍提供各種地產代理服務以外的服務，加入會籍故此不能視為與租賃樓宇的原本目的直接有關，尤其是經營會籍的公司會向第三者披露會員的資料，藉以促銷與物業交易無關的產品。就私隱條例而言，向顧客發出通知信及有關顧客並無提出反對，並不同他已給予「訂明同意」讓對方可使用他的個人資料使其加入成為會員。

故此，將有關顧客的個人資料移轉給經營會籍的公司，使他成為會員，以及其後向保險公司披露他的個人資料，藉以促銷人壽保險產品，均有違保障資料第3原則的規定。在公署發出執行通知後，有關物業代理及經營會籍的公司已停止上述使用顧客的個人資料的做法。

Outcome of Investigation

DPP3 prohibits the use (including transfer) of the individual customer's personal data for any purpose other than the original purpose for which the data were collected or a directly related purpose, unless his "prescribed consent" has been obtained beforehand. It was clear that the original collection purpose of the customer's data was for the provision of property-agency service for renting a flat. The agency had not informed the customer of any other purpose of use of his data at the time of collection of the data. Joining the club, which provided multifarious services other than property-agency service, could not be said to be related to the original collection purpose for renting a flat, in particular when the club would disclose members' data to third parties for promotion of products unrelated to property transaction. "Prescribed consent" means voluntary and express consent. For the purpose of the PD(P)O, the sending of the notification letter and the customer's failure to object could not amount to "prescribed consent" for using his data to make him a member of the club.

Accordingly, the transfer of the customer's data to the club for making him a member and the subsequent disclosure to the insurance company for marketing life insurance products were found to be in contravention of DPP3. Consequently, the agency and the club ceased such uses of customers' data after the issuance of enforcement notices to them.

業主當心：向租戶的僱主披露租務糾紛的詳情可能視為不當 — 保障資料第3原則

4/04

Landlords beware: disclosing to tenant's employer details of rental dispute may be wrongful — DPP3

投訴

個案涉及由欠租引起的租務糾紛。在採取行動追收欠租的過程中，業主的律師向租客發出追收信件，並將副本送交租客的僱主，因而披露了糾紛及所拖欠的租金詳情。

調查結果

公署認為，涉及租務糾紛的租客個人資料，其收集目的是為處理或解決雙方的糾紛。在本案中，租客的僱主與有關租務或當中的糾紛無關，業主亦未能提出任何理由為何將糾紛通知租客的僱主。業主或許希望藉此向租客施加壓力，迫使租客付款，但如此使用資料的目的不屬原有的收集目的。由於無證據證明租客已給予「訂明同意」容許業主向他的僱主披露租務糾紛中有關他的個人資料，業主因此違反了保障資料第3原則的規定。公署遂向該業主（是一間從事地產業務的公司）發出執行通知，規定他們在類似情況下不得將租務糾紛告知租客的僱主。

The Complaint

A tenancy dispute over rental payment arose. In the course of taking action for recovery of rent, the landlord's solicitors issued a demand letter to the tenant and had it copied to his employer disclosing details of the dispute and the rent in arrears.

Outcome of Investigation

Personal data of the tenant relating to the tenancy dispute are considered to be collected for the purpose of dealing with or resolving the dispute between the parties. The employer of the tenant had no prior involvement in the tenancy nor the dispute. The landlord failed to justify why it was necessary to write to the employer about the dispute. The landlord might wish to put pressure on the tenant to submit to their demand but such use of the data was considered not within the original collection purpose. In the absence of evidence showing that the tenant had given his "prescribed consent" to the disclosure of his personal data in relation to the tenancy dispute to his employer, the landlord was found in contravention of DPP3. Enforcement notice was issued requiring the landlord (which is in the real estate business) to cease such practice of informing tenants' employers in similar situations.

網上保安：重新啟動已封鎖戶口時應採用隨機密碼而非固定的重設密碼 — 保障資料第4原則

5/04

Internet security: randomly assigned instead of fixed reset password preferred when reactivating a locked account — DPP4

投訴內容

一間流動電話服務公司在其網頁為客戶提供網上帳單服務。載有客戶個人資料（包括通話記錄）的電子帳單是受密碼保護的。此外，為防止黑客入侵，當有關戶口在五次登入失敗後，便不能進行網上查閱。然而，當公司應客戶要求重新啟動已封鎖的戶口時，戶口的密碼會自動重設為一串固定數字（例

The Complaint

A mobile phone service company provided an internet billing service to its customers through its website. The electronic bills, which contained customers' data including calling records, were password protected. In addition, a mechanism to deactivate internet access to an account after five unsuccessful logins was built in to preclude hacking. However, upon reactivation of the locked account by request of the customer, the password would be automatically reset to a fixed number (e.g. 123456),

(續下頁)

(to be continued on next page)

如123456)，此做法適用於所有客戶的戶口。這使黑客有機會入侵戶口資料，因為他可先作出五次失效登入，令有關戶口不能啟動，而有關客戶隨後便會通知流動電話公司他不能登入戶口，黑客然後便在客戶未更改密碼前，乘機利用固定數字的重設密碼登入口口。流動電話服務公司的一名客戶就此保安漏洞向公署投訴。

調查結果

保障資料第4原則規定有關電話公司必須採取所有合理地切實可行的步驟，以免客戶的資料受到未獲准許的查閱。鑑於個別人士的通話資料的敏感性質，有關公司將已封鎖戶口的密碼重設為一串固定數字的一成不變做法，並不足以保障客戶的個人資料，雖然有關公司已提示客戶須透過系統定期更改戶口密碼，但看來無法避免黑客以上述方法入侵戶口。案件中沒有資料顯示有關公司在客戶重新啟動封鎖的戶口時，設定不同而非固定的密碼是不切實可行的。最後，有關公司對系統作出改善，將密碼設定為隨機密碼，以及透過客戶的流動電話以短訊形式將重設的密碼通知客戶。

which was applicable to all customers. This allowed a hacker to gain access to the account information by first deactivating an account with five unsuccessful login attempts to prompt the customer to make a lockout report to the mobile phone company and then logging in to the account with the fixed reset password before the customer ever changed the password. A complaint on the security pitfall on password control was lodged with the PCO by a customer.

Outcome of Investigation

DPP4 requires the phone company to take all reasonably practicable steps to guard against unauthorized access to its customers' data. Taking into account the sensitivity of an individual's calling records, the phone company's unvaried practice of resetting the password of a lockout account to a fixed number was considered insufficient to protect customers' data against possible intrusion as suggested above, despite the phone company's effort to remind customers via their system to change passwords periodically. There was nothing suggesting that it was not reasonably practicable for the phone company to allot a varied, rather than a fixed, password to customer when reactivating a lockout account. Eventually, the mobile service provider improved its system to have the password reset to a random number and the customer informed of the reset password via short message sent to his mobile telephone.

網上保安：堵塞系統上的漏洞，以防止受密碼保護的客戶個人資料受到未經准許或意外的查閱 — 保障資料第4原則

Internet security: system loopholes mended to prevent unauthorized or accidental access to password protected personal data of customers — DPP4

6/04

投訴內容

這是另一宗有關流動電話公司提供的網上帳單服務的投訴。該流動電話公司提供的網上帳單服務系統要求客戶輸入密碼，才可查閱本身的帳戶資料。一名客戶透過此項服務查閱本身的帳戶資料時，赫然發現即使他已登出該系統及離線，只要按「上一頁」的鍵掣或透過瀏覽器的「記錄」功能，便可返回一些先前所瀏覽的受密碼保護的網頁。

(續下頁)

The Complaint

Another case of internet billing service provided to customers by a mobile phone service company. The system was secured by password feature where a customer had to enter his password to gain access to his account information. In an attempt to access the account information via the service, a customer was alarmed to find out that it was possible to return to the same secured pages which he had previously visited by simply striking the "Back" button or via the "History" function of the browser, even after he had logged out from the system and gone offline.

(to be continued on next page)

調查結果

鑑於上述系統的保安漏洞，該公司客戶的個人資料可能會有被其他人士查閱的危險，尤其是當客戶使用設於公眾地方的電腦來查閱帳單資料。該公司由於未有採取足夠的保安措施以保障客戶的個人資料，此舉有違保障資料第4原則的規定。該公司對公署的調查結果作出回應，立即修正有關係統以堵塞該漏洞，以及在網頁中加上警告字句，建議客戶在網上閱覽帳戶資料後，應登出有關係統及關閉瀏覽視窗。

Outcome of Investigation

By allowing such security loopholes, the company exposed its customers' personal data to the risk of being accessed by unintended or unauthorized third parties, particularly so when the customers used computer terminals available in public places. This was considered a contravention of DPP4 in failing to provide sufficient safeguards to protect customer data held. In response to the PCO's findings and in order to remedy the situations, the company immediately carried out rectifications to eliminate the loopholes and added security alert statements on the website, advising customers to log out from the system and close the browser window after finished viewing the password controlled personal information on the website.

進行外展促銷活動收集個人資料時：須採取保安措施避免意外遺失申請表上的個人資料 — 保障資料第4原則

Personal data collected through outdoor marketing campaigns : organizers to take safety steps to prevent accidental loss of application data collected — DPP4

7/04

投訴內容

一間銀行在週末於某書店推銷信用卡。在推銷活動結束後，銀行職員將所有申請表及申請人的身份證副本放進公事包帶回家，然後打算在下一個工作天將有關資料帶回銀行處理。不幸地，有關職員將公事包遺留在公共小巴上，因而遺失了所有文件。



The Complaint

A bank conducted a marketing campaign in a bookshop to solicit credit card applications on a Saturday. At the end of the campaign, the bank staff put all the application forms together with applicants' identity card copies in a briefcase and carried them home before returning to office the next working day. Unfortunately, the bank staff left the briefcase in a public light bus and lost all the documents.

調查結果

公署在調查投訴時，發現銀行並無就如何處理在外展促銷活動中所收集到的個人資料，向職員發出充份指引。在考慮過有關資料的敏感性，以及意外遺失該等資料可能對當事人造成的損害後，公署認為銀行沒有採取切實可行步驟保障所收集的個人資料，因而違反保障資料第4原則的規定，遂向銀行發出執行通知。銀行按照執行通知的指示制訂相應保障措施，包括規定在外展促銷活動結束時將信用卡申請表及其他有關文件送回附近的分行，而非讓職員將有關資料攜帶回家。

Outcome of Investigation

Upon investigation of the complaint, it was discovered that the bank did not have adequate guidelines issued and given to staff in relation to handling of personal data collected during outside-office marketing campaigns. Taking into account the sensitivity of the data collected and the harm that is likely to be inflicted upon the data subject on accidental loss of the data, the bank was found in breach of the requirements of DPP4 in failing to take practicable steps to protect the security of the personal data collected. Enforcement notice was issued, and in compliance therewith the bank implemented corresponding safeguard measures, including the transmission of those credit card applications and supporting documents to a nearby branch of the bank at the end of the marketing campaign instead of allowing staff to bring them home.

向行政上訴委員會提出的上訴個案的簡述

根據私隱條例的規定，投訴人或被投訴的資料使用者均可就私隱專員的決定提出上訴。根據私隱條例第39(4)條，投訴人可就私隱專員拒絕行使對投訴進行調查或繼續調查的權力而向行政上訴委員會上訴。此外，投訴人亦可根據第47(4)條，就私隱專員在完成調查後，拒絕向被投訴的資料使用者發出執行通知的決定提出上訴。另外，被調查的資料使用者亦有權根據第50(7)條，就私隱專員向他發出執行通知一事，向行政上訴委員會提出上訴。

行政上訴委員會在本年報期內共處理了兩宗上訴個案。其中一宗個案的簡述如下：

Notes on Appeal Cases lodged with the Administrative Appeals Board

Under the PD(P)O, an appeal may be lodged by a complainant or the relevant data user complained of against the decisions made by the Privacy Commissioner. Pursuant to section 39(4), an appeal may be made by a complainant to the Administrative Appeals Board (“AAB”) against the decision of the Privacy Commissioner in refusing to exercise his power to investigate or to continue to investigate a complaint. An appeal may also be lodged by a complainant pursuant to section 47(4) against the decision of the Privacy Commissioner in refusing to issue an enforcement notice against the data user complained of after completion of an investigation. Alternatively, a data user investigated has the right to appeal to the AAB pursuant to section 50(7) against the decision made by the Privacy Commissioner in issuing an enforcement notice against it.

There were 2 AAB appeal cases disposed of in the reporting period. The case note on one of them is given below.

銀行接獲僱主終止聘用員工的通知而取消有關員工的信用咭 — 咭主向銀行作出查閱資料要求 — 銀行不依從該要求，及未經許可下向咭主的前僱主披露該項查閱要求：條例第19(1)條及保障資料第3原則(1/04)

Cancellation of credit card by bank upon notification of cessation of employment by card holder's employer — data access request by card holder to bank — non compliance with the request — unauthorized disclosure of the request to card holder's ex-employer — section 19(1) and DPP3 (1/04)

事件起因

一名投訴人向銀行申請並獲發一張由該投訴人的僱主參與的員工信用咭計劃的信用咭。根據計劃的條款，當持有信用咭的僱員停止受僱時，僱主須通知銀行。一天，該投訴人接獲銀行通知會取消他的信用咭，理由是他不再受僱於有關僱主。投訴人於是向銀行提出查閱資料要求，藉以查閱僱主就其終止受聘一事向銀行發出的通知的複本。銀行拒絕依從他的查閱要求，理由是因為其僱主擁有及控制該文件的用途。在處理他的查閱要求時，銀行向投訴人的僱主透露他曾提出該項查閱要求。

(續下頁)

Facts

The complainant applied and was issued credit card by the bank pursuant to a scheme participated by his employer who under the terms of arrangement was required to notify the bank should its employee who was holder of the credit card cease to be employed. One day, the bank informed the complainant that his credit card would be cancelled, as he was no longer employed by his employer. The complainant then lodged a data access request with the bank requesting access to a copy of the employer's notice to the bank on the cessation of his employment. The bank refused to comply with the request claiming that it was unable to do so as the employer possessed and controlled the use of the document. In the course of handling the request, the bank disclosed to the employer that the complainant had made such a request.

(to be continued on next page)

投訴內容及私隱專員的調查結果

投訴人指稱銀行錯誤地拒絕他的查閱資料要求。他更指稱銀行在未經他同意下，向他的僱主披露了他的個人資料(即他提出了查閱資料要求)。

私隱專員進行調查，發覺所要求查閱的通知文件，包含一份名單及隨名單附上的信件，名單中列述了幾名前僱員(包括投訴人)的姓名。銀行聲稱當收到投訴人的查閱資料要求時，銀行只持有名單，卻無隨附的信件。銀行進一步聲稱它必須先得僱主同意，才能將有關名單發放；而為了尋求僱主的同意，銀行遂將投訴人的查閱要求向僱主披露。

私隱專員在調查後及從所得的證據發現，僱主並無禁止銀行發放有關的名單，而銀行亦毋須先得僱主同意，才可向投訴人發放名單，有關銀行因而違反了私隱條例第19(1)條的規定。至於未經許可向僱主披露投訴人的查閱要求的指稱，私隱專員發現披露有關資料的目的，與收集投訴人的個人資料的原本目的直接有關，亦即是處理他的查閱要求。私隱專員認為有關披露並無違反保障資料第3原則的規定。

銀行按照私隱專員的指示，承諾在將名單中第三者的姓名刪除後，向投訴人提供有關名單的副本，並且向投訴人確認在收到他的查閱要求時，銀行並無持有他所要求的其他文件。鑑於銀行已實踐承諾，私隱專員認為銀行不大可能在日後重複違反條例的有關規定，因而酌情不向該銀行發出執行通知。

(續下頁)

Complaint and findings by Privacy Commissioner

The complainant alleged that the bank had wrongfully refused to comply with his data access request. He further alleged that the bank had disclosed his personal data (that he had made a data access request) to the employer without his consent.

The Privacy Commissioner carried out an investigation and found that the notice requested consisted of a covering letter and a list with the names of several ex-employees including the complainant. The bank claimed that at the time when the request was received, they were in possession of the list but not the covering letter. The bank further claimed that consent from the employer was required before it could release the list and for the purpose of seeking consent, it disclosed the complainant's data access request to the employer.

Upon investigation and from evidence gathered, the employer did not prohibit the disclosure of the list requested and no consent was needed before the bank could release the list to the complainant. The Privacy Commissioner found that the bank had contravened section 19(1) of the PD(P)O. As to the allegation on unauthorized disclosure of the complainant's request to the employer, the Privacy Commissioner found that the purpose of disclosure by the bank was directly related to its original purpose of collecting the complainant's personal data, namely, to handle his request. He opined that such disclosure had not contravened DPP3.

Pursuant to the undertakings imposed by the Privacy Commissioner, the bank provided to the complainant a copy of the list with names of third parties deleted and confirmed to the complainant that at the time of the request, it did not hold any other requested document. In view of the compliance with the undertakings by the bank, the Privacy Commissioner opined that the contravention by the bank was not likely to be repeated and therefore exercised his discretion not to issue an enforcement notice to the bank.

(to be continued on next page)

上訴

就私隱專員不向銀行發出執行通知的決定，投訴人向行政上訴委員會提出上訴。委員會同意私隱專員在決定是否發出執行通知時有很大的酌情權。委員會認為私隱專員已考慮到這是銀行的首次違例，以及銀行願意作出及履行承諾，因而得出一個合理的結論，即銀行在此事上不大可能會重複違反條例的規定。至於未經許可向僱主披露個人資料的指稱，委員會認為雖然銀行錯誤地認為該等資料是由投訴人的僱主持有及管控，銀行披露有關查閱要求是為了讓投訴人得以查閱該等資料，委員會裁定銀行在此情況下披露投訴人的個人資料，與收到該查閱資料要求的目的一致，或無論如何有關的披露是與該目的直接有關，銀行的做法故此並無違反保障資料第3原則的規定。

行政上訴委員會的決定

委員會支持私隱專員的決定並駁回上訴。

The appeal

The complainant appealed to the AAB on the Privacy Commissioner's decision not to issue an enforcement notice to the bank. The AAB agreed that the Privacy Commissioner had a wide discretion in deciding whether to issue an enforcement notice. The AAB found that the Privacy Commissioner had reasonably concluded that a repeated contravention by the bank was not likely having regard to the fact that this was the first contravention by the bank and to the cooperation of the bank in giving and performing the required undertakings. As to the alleged unauthorized disclosure of personal data to the employer, the AAB took the view that the disclosure of the request by the bank was to enable the complainant to gain access to the data which the bank thought, though erroneously, was in the employer's possession and control and without whose permission could not be released to the complainant. The AAB decided that the disclosure in the circumstances was for a purpose for which the request had been received by the bank or at least for a purpose directly related thereto and thus not contravened DPP3.

AAB's decision

The AAB upheld the Privacy Commissioner's decision and dismissed the appeal.

向高等法院提出的司法覆核

根據行政法，受屈一方可就私隱專員拒絕對他的投訴進行調查的決定提出司法覆核。在本年報期間，有一名投訴人就私隱專員根據私隱條例第39(2)(c)條(即該項投訴屬瑣屑無聊或無理取鬧或不是真誠作出)為理由拒絕進行調查的決定，向高等法院申請司法覆核。在本年報期結束時，此個案已進行部份聆訊。

Judicial Review lodged with the High Court

Under administrative law, an aggrieved party may make an application for Judicial Review to the Court against the decision made by the Privacy Commissioner in refusing to carry out an investigation of his complaint. During the reporting period, there was an application for Judicial Review made to the Court by a complainant against the Privacy Commissioner's decision made under section 39(2)(c) of the PD(P)O in refusing to carry out an investigation of his complaint on the ground that the complaint was frivolous or vexatious or was not made in good faith. At the end of the reporting period, the case was part heard.