

Serving
竭誠服務

Seven

million 七百萬
people



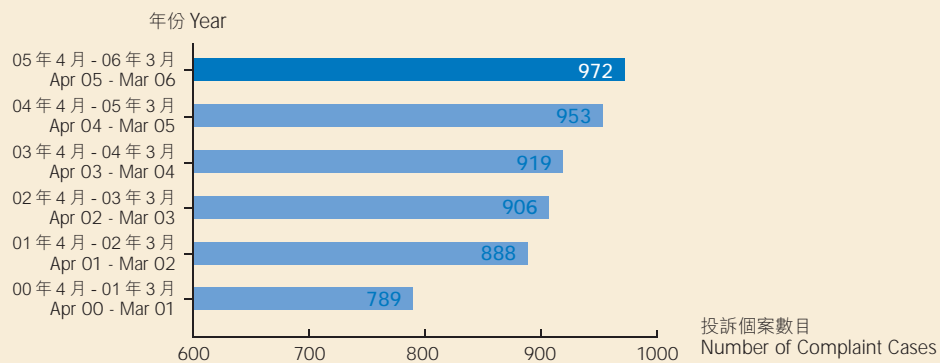
投訴工作 Complaint Investigations



在二零零五至零六年度接獲的投訴個案

Complaints Received 2005-2006

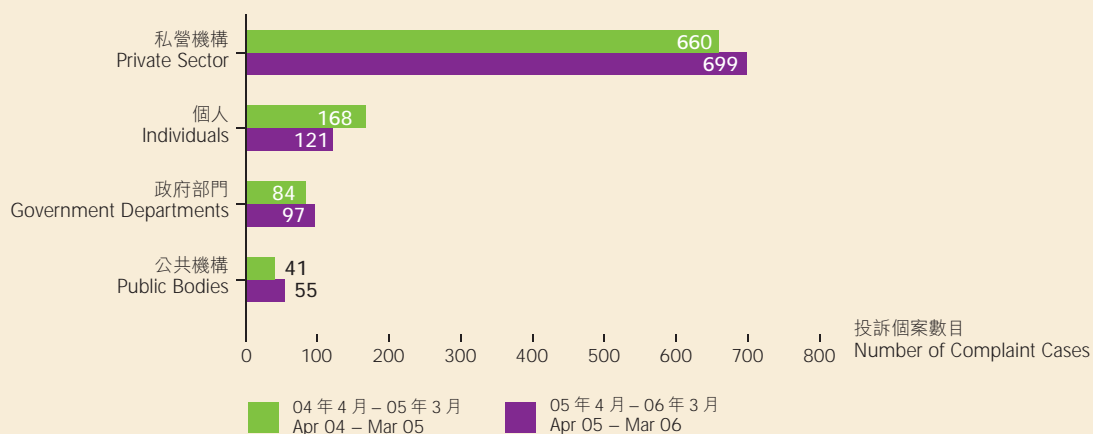
圖表 1 — 每年的投訴個案
Figure 1 – Annual Complaint Caseload



在二零零五至零六年度公署共接獲972宗投訴個案（較去年上升2%）。

A total of 972 complaint cases were received in 2005-2006 (an increase of 2% on the previous year).

圖表 2 — 被投訴者的類別
Figure 2 – Types of Party Complained Against

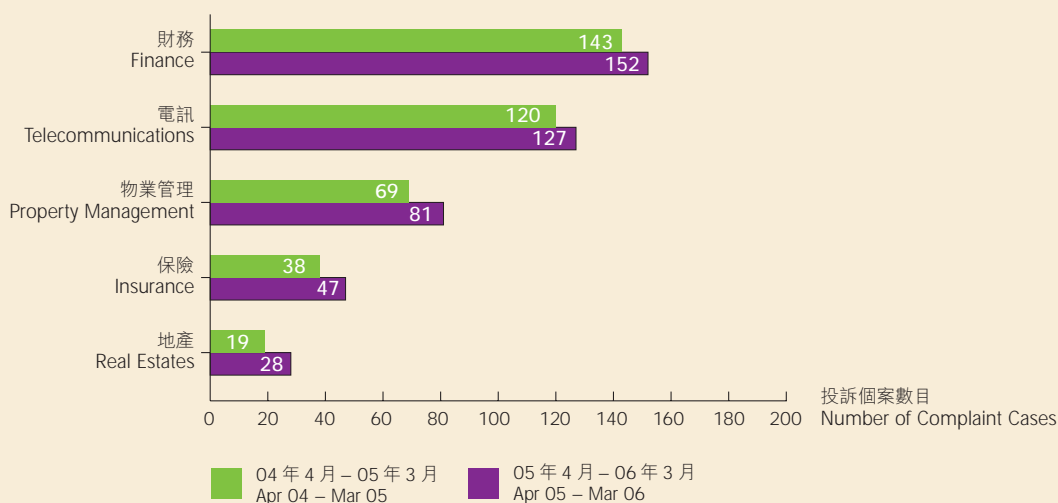


- ◆ 699宗(72%)個案投訴私營機構。
- ◆ 121宗(12%)個案投訴個人。
- ◆ 152宗(16%)個案投訴公營機構（即政府部門及其他公共機構）。

- ◆ 699 (72%) complaint cases were against private sector organizations.
- ◆ 121 (12%) complaint cases were against individuals.
- ◆ 152 (16%) 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

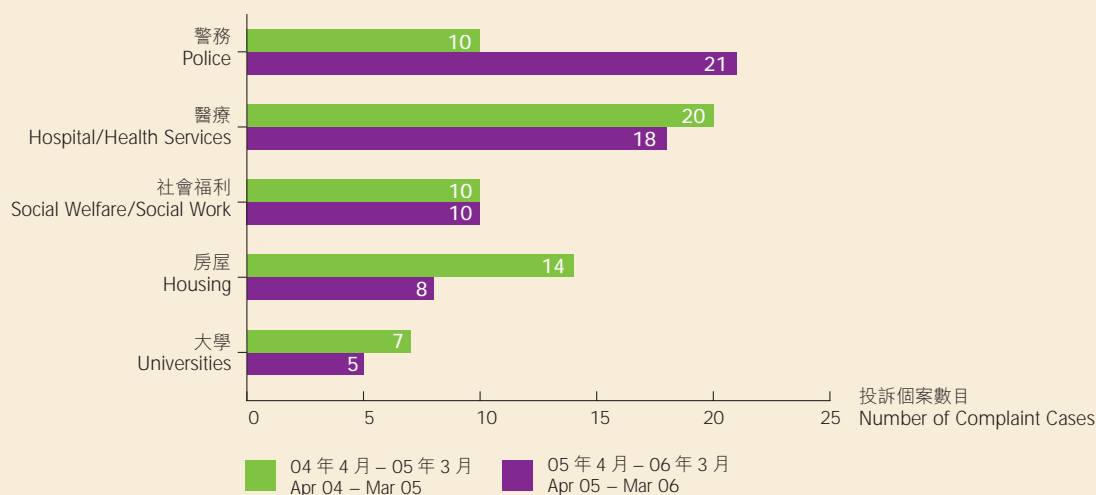


在投訴財務機構及電訊業的個案中，大部分被指非法使用客戶的個人資料，許多投訴與追收欠債 / 服務費有關。

The majority of complaints against the financial and telecommunications sectors alleged the unlawful use of customers' personal data. Most of the complaints involved recovery actions for overdue loan/service payments.

圖表 4 — 對公營機構的投訴

Figure 4 – Complaints Against Public Sector Organizations



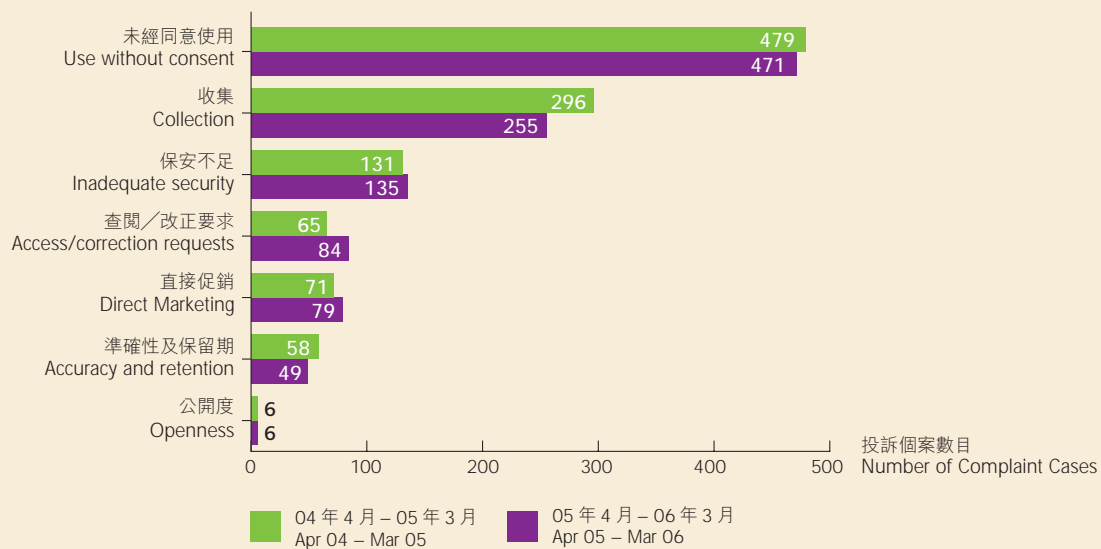
在投訴公營機構的個案中，大部分涉及：

- ◆ 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%)；
- ◆ 過量或不公平收集個人資料 (22%)；
- ◆ 未能遵守查閱資料要求或改正資料要求 (20%)；及
- ◆ 欠缺保障個人資料的保安措施 (19%)。

The majority of complaints against public sector organizations involved:

- ◆ the alleged use of personal data beyond the scope of collection purpose and without the consent of the individual (36%);
- ◆ excessive or unfair collection of personal data (22%);
- ◆ non-compliance with data access or correction requests (20%);
- ◆ and lack of security measures to protect personal data (19%).

圖表 5 — 投訴的性質
Figure 5 – Nature of Complaints



二零零五至零六年度接獲的 972 宗投訴個案共涉及 1,079 項被指違反私隱條例的規定。在這些事項中，916 項（85%）被指違反保障資料原則的規定，以及 163 項（15%）被指違反私隱條例的主體條文。

在 916 項被指違反保障資料原則的事項中，471 項（51%）涉及在未獲投訴人同意前，使用他們的個人資料。在這類個案中，84 項（18%）涉及收債活動，大部分是財務機構及電訊公司被指將客戶的個人資料，例如聯絡資料及欠帳額，轉交追討欠款公司作追收欠債用途。

有些投訴人對私隱條例在個人資料的使用及披露方面的適用範圍有所誤解。一個常見的例子是，有些投訴人認為只可在取得他們的特定同意後才可使用或向他人披露他們的個人資料。私隱條例限制個人資料只可使用或披露於原有收集目的或直接有關目的，其他的使用或披露必須經資料當事人的明示同意。換句話說，假如個人資料的使用或披露是在原有收集目的的範圍內，或為了直接有關的目的，則資料使用者便無須在使用或披露前先取得資料當事人的同意。

The 972 complaint cases received in 2005-2006 involved a total of 1079 alleged breaches of the requirements of the Ordinance. Of these, 916 (85%) were alleged breaches of the data protection principles and 163 (15%) were alleged contraventions of the provisions in the body of the Ordinance.

Of the 916 alleged breaches of the data protection principles, 471 (51%) concerned the alleged use of personal data of complainants without their consent. In this category, 84 (18%) involved debt collection, mostly allegations against financial institutions and telecommunications companies for passing customers' personal data, such as contact details and amount of indebtedness, to debt collecting agencies for the recovery of outstanding debts.

There is a misunderstanding among some complainants regarding the ambit of the Ordinance when applied to use or disclosure of personal data. A common example is that some complainants believe their personal data can only be used or disclosed to others after prior consent concerning a particular act has been obtained from them. The Ordinance restricts the purpose of use or disclosure of personal data to their original collection purpose or a directly related purpose. Any other use or disclosure of personal data requires the express consent of the data subject concerned. In other words, if the use or disclosure of personal data is within an original collection purpose, or a directly related purpose, it is not necessary for the data user to obtain the consent of the data subject prior to use or disclosure.

調查投訴

Complaint Investigations

在本年報期開始時，公署正處理上年度帶下來的 195 宗投訴，加上新收到的 972 宗投訴，私隱專員在本年報期內共須處理 1,167 宗投訴。在這些個案中，400 宗 (34%) 經初步審閱後不獲受理，理由是其中的 363 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 37 宗不屬專員的權力範圍。餘下 767 宗 (66%) 正在審閱中或經審閱後獲進一步處理，其中 579 宗 (75%) 在本年報期內已得到解決，而餘下的 188 宗 (25%) 在二零零六年三月三十一日時仍在處理中 (圖表 6)。

At the beginning of the reporting year, 195 complaints were being processed. With the 972 new complaints received, the Privacy Commissioner handled a total of 1,167 complaints during the reporting period. Of these, 400 (34%) cases were declined for further action after preliminary consideration because 363 of them were found to have no *prima facie* case to support allegations of breaches of the Ordinance, and the remaining 37 cases were outside the jurisdiction of the Commissioner. The remaining 767 (66%) cases were either in the preliminary screening process or screened-in for further consideration. Of these, 579 (75%) cases were resolved during the reporting year while the balance of 188 (25%) were still being processed on 31 March 2006 (Figure 6).

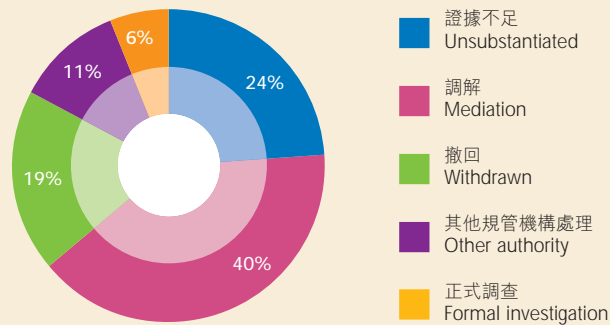


圖表 6 — 二零零五至零六年度處理的投訴摘要
Figure 6 – Summary of Complaints Handled in 2005-2006

	2002-03	2003-04	2004-05	2005-06
上年轉來的投訴 Complaints carried forward	157	203	157	195
接獲的投訴 Complaints received	906	919	953	972
須處理的投訴的總數 Total complaints processed	1063	1122	1110	1167
經審閱後不受理的的投訴 Complaints screened-out	359	367	220	400
正在審閱或經審閱後獲處理的投訴 Complaints being screened or screened-in	704	755	890	767
完結 Completed	501	598	695	579
處理中 In process	203	157	195	188

圖表 7 — 調查結果

Figure 7 – Outcome of Investigations



在本年報期內完結的 579 宗個案：

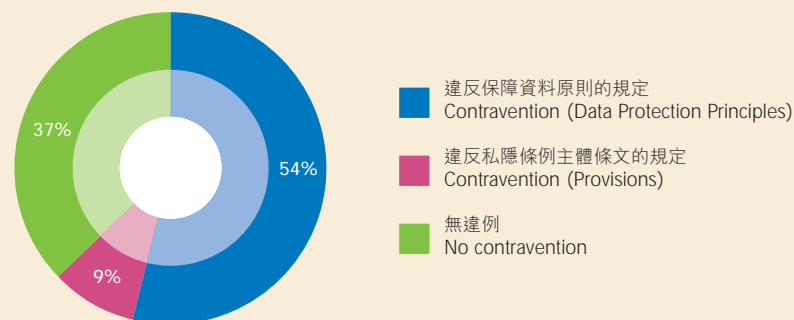
- ◆ 232宗(40%)透過調解得到解決；
- ◆ 35宗(6%)在進行正式調查後得到解決；
- ◆ 140宗(24%)在進行初步查詢後發現證據不足；
- ◆ 109宗(19%)在初步查詢期間由投訴人撤回；及
- ◆ 餘下的 63 宗(11%)投訴個案，大多涉及投訴人不回應私隱專員的查詢或個案已被或交由其他規管機構，例如警方跟進。

Of the 579 cases completed during the reporting period:

- ◆ 232 (40%) cases were resolved through mediation;
- ◆ 35 (6%) cases were resolved after formal investigations;
- ◆ 140 (24%) cases were found to be unsubstantiated after preliminary enquiries;
- ◆ 109 (19%) cases were withdrawn by complainants during preliminary enquiries; and
- ◆ the remaining 63 (11%) cases involved mostly complaints where the complainants did not respond to the Privacy Commissioner's inquiries or where the matter had been transferred or reported to other authorities, e.g. the Hong Kong Police.

圖表 8 — 正式調查結果

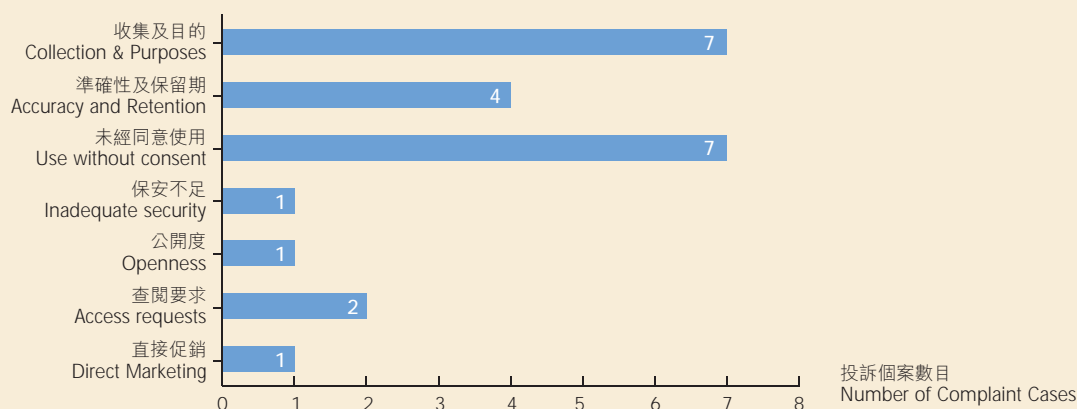
Figure 8 – Results of Formal Investigations



在本年報期內完成正式調查的 35 宗個案中，私隱專員發現其中 22 宗(63%)違反了條例的規定，餘下 13 宗(37%)並無違例或因缺乏證據而無法證明有違例情況。

Of the 35 formal investigations completed during the reporting period, the Privacy Commissioner found contravention of the requirements of the Ordinance in 22 (63%) cases. In the remaining 13 (37%) cases, either no contravention was found or contravention was not established due to insufficient evidence.

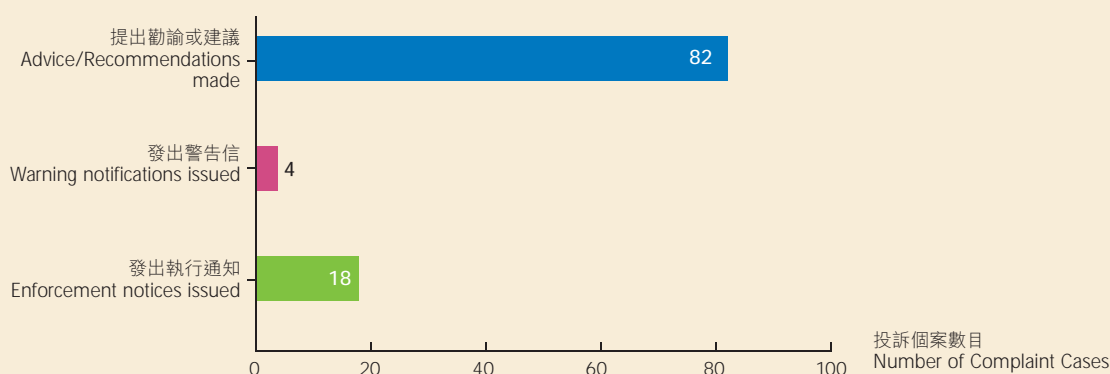
圖表 9 — 違例事項的性質
Figure 9 – Nature of Contravention



在被確定違反條例規定的 22 宗個案中，19 宗違反一項或以上保障資料原則，其餘 3 宗違反了條例主體條文的規定，當中涉及的違例事項與依從查閱資料要求或直接促銷有關（圖表 9）。

Of the 22 cases where the requirements of the Ordinance were found to have been contravened, 19 cases involved contravention of one or more of the data protection principles. The remaining 3 cases involved contravention of the requirements in the main body of the Ordinance relating to compliance with data access requests or direct marketing (Figure 9).

圖表 10 — 根據調查結果採取的行動
Figure 10 – Actions Taken as a Result of Investigation



在 232 宗透過調解得到解決的個案中，私隱專員向 82 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原則及私隱條例的其他規定。

In the 232 cases resolved through mediation, the Privacy Commissioner provided advice and recommendations to 82 organizations on their practices and procedures in order to assist them in complying with the data protection principles and other requirements of the Ordinance.

在被確定違反條例規定的 22 宗個案中，私隱專員共向被投訴的資料使用者發出 18 份執行通知，以防止他們繼續或重複違反規定。至於餘下的四宗個案，被投訴者已採取或書面承諾採取糾正措施，私隱專員因而無須作出強制性行動，發出執行通知，而只是向有關資料使用者發出警告信。

In the 22 cases in which requirements of the Ordinance were found to have been contravened, the Privacy Commissioner issued 18 enforcement notices on the parties complained against to prevent continuation or repetition of the contraventions. In the remaining four cases, the parties complained against had either taken measures to remedy the contraventions, or given a written undertaking to implement them. As a result, enforcement action through the issuance of an enforcement notice was not deemed to be necessary, and warning notices were issued.

重要的調查結果

Significant Investigation Results

下述投訴個案是本年報期內一些資料使用者被確定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。

The following complaint cases illustrate some data user acts or practices that were found to have contravened the requirements of the Ordinance during the reporting period. They are selected on the basis of subject content and demonstrate the wide variety of conduct subject to the provisions of the Ordinance, including those of the Data Protection Principles (“DPP”).

沖曬店：顧客沒有出示收據而提取相片時，不應收集顧客的身分證號碼 — 保障資料第 1(1)原則及《身分證號碼及其他身分代號實務守則》

PHOTO SHOP : SHOULD NOT COLLECT IDENTITY CARD NUMBER OF CUSTOMER WHEN COLLECTING PHOTOGRAPHS WITHOUT PRODUCING THE RECEIPT—DPP1(1) AND THE CODE OF PRACTICE ON THE IDENTITY CARD NUMBER AND OTHER PERSONAL IDENTIFIERS

投訴內容

一名顧客要求一間沖曬店沖曬一些相片。該店在記錄顧客的姓氏及流動電話號碼後，向顧客發出收據。可惜顧客遺失收據，在提取相片時不能出示收據。該店要求顧客在「申索表格」上登記身分證號碼，作為把相片及底片交還給他的必要條件。顧客認為收集他的身分證號碼是不必要的，因為他的流動電話號碼及他在相片上的容貌足以證明他正是要求沖曬相片的人。他於是向專員作出投訴。



The Complaint

A customer placed an order for printing some photographs with a photo shop. The shop issued a receipt to the customer after recording the customer's surname and mobile telephone number. The customer unfortunately lost the receipt and was unable to present it when attempting to collect the photographs. The shop asked for the customer's Hong Kong identity card number for recording in

an “Order Claim Form” as a prerequisite to releasing the photographs and negatives to him. The customer took the view that the collection of his identity card number was unnecessary as his mobile telephone number as well as his images appearing in the printed photographs were sufficient to show that he was the rightful person placing the order. He thus made a complaint to the Commissioner.

該店解釋，收集身分證號碼是必需的，作用是識辨提取相片的人，避免相片錯交他人。該店認為請顧客描述相片中的圖像並不可行，因為這並不表示他就是要求沖曬相片的人。該店亦表示，曾經有顧客控告他們遺失相片、底片、膠卷等，更有一次，他們要向一名顧客賠償超過五千港元。因此，該店認為根據《身分證號碼及其他身分代號實務守則》（下稱「實務守則」）第2.3.3.3段，收集身分證號碼是獲准的。第2.3.3.3段准許資料使用者為正確識辨身分證持證人的身分而收集身分證號碼，以避免對資料使用者造成損害或損失，而該損害或損失在有關情況下是超過輕微程度的。不過，該店承認他們從未收過底片、膠卷或相片被他人錯取的顧客投訴。

私隱專員的調查結果

私隱專員認為要援引實務守則第2.3.3.3段，資料使用者預期的損失的發生及程度應該在實際上是有充分理由支持的。在未有資料顯示會招致超過輕微程度損失或損害的真正風險下（正如本個案），容許收集身分證號碼等同於容許一般性的收集，這是違反實務守則的目的。在本個案，由於顧客在要求沖曬相片時已留下流動電話號碼，只要在顧客前來提取相片時，在他面前致電該號碼，便可以核對身分。此外，該店亦可以為識別目的而登記該顧客的全名（可核對出示的身分識別文件），以核對其記錄，及／或查看相片上的容貌。在有關情況下，私隱專員認為該店如此收集身分證號碼是不必要的措施，而且是侵犯私隱的。

私隱專員所採取的行動

私隱專員向該沖曬店發出執行通知，該店按指示終止有關做法，並銷毀所收集的身分證號碼記錄。

The shop explained that the identity card number was necessary for identifying the person who actually collected the photographs to avoid giving the photographs to the wrong person. The shop did not consider asking the person to describe the images on the photographs feasible because it did not necessarily mean that he was the one placing the order. The shop also stated that there had been cases where customers sued them for loss of photographs, negatives, films, etc., and on one occasion, they had paid a compensation of more than HK\$5,000 to a customer. The shop therefore argued that the collection was permitted under paragraph 2.3.3.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers ("the PI Code"). Paragraph 2.3.3.3 allows the collection of identity card number by a data user if it is necessary for the correct identification of the holder so as to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances. The shop however admitted that they had not received any complaints from customers who had their negatives, films or photographs wrongfully collected by others.

Findings of the Privacy Commissioner

The Privacy Commissioner holds the view that the existence and extent of loss that a data user contemplated should be something realistically justified for paragraph 2.3.3.3 of the PI Code to be invoked. To allow for the collection of identity card number where a real risk of more than trivial loss or damage is not shown (as in the present case) is tantamount to allowing collection in general cases which would be contrary to the objectives of the PI Code. In this particular case, since the mobile telephone number was given by the customer when placing the order, verification could simply be done by calling the number in his presence when he came to collect the photographs. Alternatively or additionally, the shop could record the full name of the customer (checked against the identification document presented) for identification purpose and to match with the records of the surname kept by them, and/or examine the images on the photographs. In the circumstances, the Privacy Commissioner considered such practice of the shop of collecting identity card number not a necessary measure, while it was privacy intrusive, to take.

Action by the Privacy Commissioner

An enforcement notice was served on the photo shop and, as directed, the practice was ceased and the records of identity cards numbers so collected were destroyed.

物業管理機構：收集駛離停車場的人士的身分證號碼屬過度收集—保障資料第 1(1)原則及《身分證號碼及其他身分代號實務守則》

PROPERTY MANAGEMENT BODY : COLLECTION OF IDENTITY CARD NUMBERS OF PERSONS DRIVING OUT FROM A CAR PARK VIEWED AS EXCESSIVE COLLECTION – DPP1(1) AND THE CODE OF PRACTICE ON THE IDENTITY CARD NUMBER AND OTHER PERSONAL IDENTIFIERS



投訴內容

為了防止汽車盜竊事件，一間商場停車場的管理公司在晚上 11 時至早上 7 時登記駛離停車場的司機的身分證號碼。兩名司機反對該公司收集他們的身分證號碼，於是向專員作出投訴。

管理公司解釋，鑑於停車場的盜竊數字上升，他們在徵詢某政府部門的意見後，實施這項措施。該部門確認，在回應該公司有關停車場盜竊問題的查詢時，他們曾建議該公司加強停車場的保安措施，例如增加巡邏人手及攝錄監察、與警方合作巡邏，以及張貼通告，提醒司機保護汽車的方法。但該部門並無建議該公司收集停車場使用者的身分證號碼。

The Complaint

For the purpose of preventing car theft, the company managing a car park in a shopping mall sought to record Hong Kong identity card numbers of drivers who

drove their vehicles leaving the car park between 11:00 p.m. and 7:00 a.m. Two drivers objected to the collection of their identity card numbers and made complaints to the Commissioner.

The management company explained that the measure was taken in view of the rising figures of thefts in car parks and after consulting a government department. The department confirmed that in response to the company's enquiries about car park theft, they had advised the company to step up car park security measures such as enhancing patrolling manpower and video monitoring, cooperation with the police in patrol exercise and display of notices reminding drivers of tips to protect their cars. The department however did not suggest the company to collect identity card numbers of car park users.

私隱專員的調查結果

該停車場是供公眾使用的。收集司機的身分證號碼這個措施會導致管理公司收集及儲存大量敏感的個人資料。在採取這個措施之前，該公司必須考慮對個人資料私隱的負面影響，以及是否還有其他侵犯私隱程度較低的方法。

其中一個可行的方法是採取「雙證」制度，在車輛駛進停車場時，司機獲發一張註有車牌號碼的「出閘證」，當車輛離開停車場時，在出口的保安職員便可收集並核對資料。另一個方法是安裝電子器材，在車輛駛進停車場時拍下車牌號碼，並在車輛離開停車場時核對號碼，確保車輛使用同一張泊車票。

實務守則第 2.3.2.2 段容許資料使用者為防止或偵測罪行的目的而收集身分證號碼。雖然管理公司聲稱停車場在過去兩年曾發生三宗汽車盜竊事件，但該公司無法證明採取該政府部門建議的保安措施和上述的方法不能圓滿地解決汽車盜竊問題。在有關情況下，並根據行政上訴委員會在行政上訴案件第 41/2004 號的裁決，管理公司不能依賴第 2.3.2.2 段的豁免條文，收集司機的身分證號碼。

如果本個案容許收集身分證號碼，那麼百貨公司亦可以因為高買問題而收集每一名進出百貨公司的顧客的身分證號碼。這顯然不是實務守則的原意。因此，專員認為在本個案的情況下，管理公司收集司機的身分證號碼是不必要及超乎適度的。

私隱專員所採取的行動

私隱專員向該管理公司發出執行通知，該公司按指示終止收集司機的身分證號碼的措施，並銷毀所有已收集的身分證號碼記錄。

Findings of the Privacy Commissioner

The car park was opened to public use. The practice of collecting identity card numbers of drivers would result in large amount of sensitive personal data of individuals being collected and held by the management company. Before adopting such practice, it is imperative for the company to consider the adverse impact on individuals' personal data privacy and if there are any less privacy-intrusive alternatives.

One practical alternative is to adopt a "double permit" system whereby the vehicle registration number is marked on an "exit pass" given to the driver when he drives into the car park, so that security staff at the exit may then collect and check the same when the vehicle leaves the car park. Another alternative is to install electronic devices designed to capture the image of the number plate when the vehicle enters the car park and have it checked against the registration number of the vehicle leaving the car park to ensure that the same car park ticket is used for the same vehicle.

Paragraph 2.3.2.2 of the PI Code allows the collection of identity card number where the use of the number by the data user is necessary for the prevention or detection of crime. Although the management company claimed that there had been three car thefts happening in the car park in the past two years, the company was unable to show that adoption of the above security measures recommended by the government department as well as the aforesaid alternatives could not satisfactorily solve the car theft problem. In the circumstances and according to a previous ruling of the Administrative Appeals Board in Administrative Appeals No. 41/2004, the management company may not rely on the exemption provision in paragraph 2.3.2.2 to collect identity card numbers of the drivers.

If collection of identity card numbers is allowed in this particular case, so will be the collection of identity card numbers of everyone entering and exiting a department store because of its shoplifting problem. This apparently is not the intention of introducing the PI Code. The Commissioner therefore considered it unnecessary and excessive in collecting the identity card numbers of the drivers by the management company in the circumstances of the case.

Action by the Privacy Commissioner

An enforcement notice was served on the management company and, as directed, the company ceased such practice of collecting drivers' identity card numbers and destroyed all records of identity card numbers so collected.

僱主：在使用隱蔽方式監察僱員工作活動前，應小心考慮清楚—保障資料第1(1)、1(2)及5原則

EMPLOYERS : THINK CAREFULLY BEFORE USING COVERT MEANS TO MONITOR EMPLOYEES' ACTIVITIES AT WORK – DPP1(1), 1(2) AND 5

投訴內容

本地報章報導一個政府部門的分區辦事處在工作地點（洗手間及更衣室附近）安裝針孔攝錄機。該部門的回應是，由於辦事處發生連串的失竊事件，所以安裝針孔攝錄機偵測罪行。該部門相信，使用針孔攝錄機是找出罪犯及收集罪證的有效方法。



The Complaint

It was reported in local newspapers that pinhole cameras were found installed by a government department in the working areas, near the toilets and changing rooms of its regional office. The department's response was that pinhole cameras were installed for the purpose of detecting

crime as a result of a series of theft cases occurring in the office. The department believed that the use of pinhole cameras was an effective way for them to identify the culprit(s) and gather evidence.

私隱專員的調查結果

公署的人員實地視察後發現辦事處的不同地點共安裝了六個針孔攝錄機。攝錄機是安裝在類似插座的盒子內，人們是很難察覺到的。

根據私隱專員發出的《保障個人資料私隱指引：僱主監察僱員工作活動須知》，除非有充分理由證明使用隱蔽式監察是最後的辦法，並且絕對需要用作偵測或收集非法活動的證據，否則隱蔽式監察是不可以使用的，而在進行監察時，監察的範圍及持續時間都應受到限制。此外，僱主應制定清晰的僱員監察政策，令僱員知悉監察

Findings of the Privacy Commissioner

Site investigation conducted by the Privacy Commissioner's officers revealed that six pinhole cameras were installed at different working locations of the office. The cameras were discreetly concealed inside a socket-like box and it was difficult for anyone to notice their existence.

Under the "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" issued by the Privacy Commissioner, covert monitoring is not to be used unless justified as last resort measures and being absolutely necessary in detecting or gathering evidence of unlawful activities, and the monitoring should be limited in scope and duration. Further, the employer should formulate a clear employee monitoring policy by making known and communicating to the employees the purposes of monitoring, the circumstances

的目的、監察會在何種情況下進行，以及會收集的個人資料類別。

雖然該部門有合理的原因要保障自己及顧客的財物免受盜竊，但證據顯示損失的風險程度，不致於可以合理地大規模使用高度侵犯私隱的針孔攝錄機進行監察活動。是次監察活動的規模及範圍超越了收集資料的目的，而且該部門打算長期及全面進行防範性的監察。鑑於大量的個人資料可以在僱員不知情的情況下被收集，因此專員認為該部門為收集犯罪證據而以如此規模及範圍進行僱員監察活動是屬於過度，因而違反保障資料第 1 (1) 原則的規定。

沒有證據顯示該部門曾適當考慮採用其他侵犯私隱程度較低的方法，或者採用公開的方式會破壞收集的目的。全面及長期使用隱蔽式監察，而在使用期限方面沒有明確的計劃或政策，屬高度侵犯私隱，會加重對無辜人士的傷害(如有的話)。專員認為是次隱蔽式監察是不合理及不公平的，違反了保障資料第 1 (2) 原則的規定。

在監察僱員前，應採取合理可行的步驟，制定清晰的私隱政策聲明，並讓受監察活動影響的人士知悉。由於(在使用針孔攝錄機之前)該部門已為保安理由而安裝公開的閉路電視攝錄系統，個人資料可能已被收集，該部門確實有需要實施有效的監察政策，而有關政策應讓受影響的僱員知悉。基於該部門沒有就使用攝錄機進行僱員監察活動而制定任何私隱政策，私隱專員認為該部門違反了保障資料第 5 原則的規定。

私隱專員所採取的行動

私隱專員向該部門發出執行通知，該部門按指示終止有關的隱蔽式監察、拆除所有針孔攝錄機、銷毀所有有關記錄，以及制定有關錄影監察活動的私隱政策。

under which monitoring will take place and the kind of personal data that will be collected.

Though the department do have a legitimate purpose to protect its and its customers' property from theft, the evidence available did not show the existence of a risk of loss to such extent as to justify the engaging in vast scale video monitoring activities using pinhole cameras which was highly privacy intrusive. The dimension and extensiveness of the monitoring activity carried out was out of proportion to attaining the purpose of collection, and the department was intent upon engaging in continuous and universal preventive monitoring. The Commissioner was therefore of the view that the engaging in employee monitoring activities in such dimension and scale by the department to collect evidence of crime, given the vast amount of personal data that could be captured without the knowledge of the employees, was excessive and thus in breach of DPP1(1).

There was no evidence showing that the department had given due consideration to the use of other less privacy intrusive alternatives or that the use of overt means would necessarily frustrate the purpose of collection. The universal and continuous covert monitoring without a definite plan or policy for its duration is highly privacy intrusive, aggravating the harm, if any, that may be inflicted upon innocent parties. The Commissioner found that the covert monitoring was carried out in an unreasonable and unfair manner, contravening the requirement of DPP1(2).

Where employee monitoring is to be undertaken, reasonable practical steps should be taken to formulate and communicate a clear privacy policy statement to persons affected by the monitoring activity. Since (before using the pinhole cameras) the department had already installed overt CCTV cameras for security reason through which personal data might be collected, there was a real need to implement an effective monitoring policy which should be brought to the attention of the employees affected. On the basis that the department did not have any privacy policy to address employee monitoring activity by using video recording system, the Privacy Commissioner found that the department had contravened the requirement of DPP5.

Action by the Privacy Commissioner

An enforcement notice was served on the department and, as directed, the department ceased the practice of covert monitoring, dismantled all the pinhole cameras, destroyed all relevant recordings and formulated a privacy policy in relation to video monitoring activities undertaken by it.

服務提供者：必須確保記錄中的顧客通訊地址準確，避免洩漏顧客的資料 — 保障資料第 2 (1) 原則

SERVICE PROVIDERS : MUST ENSURE ACCURACY OF CUSTOMERS' CORRESPONDENCE ADDRESSES IN THEIR RECORDS TO AVOID LEAKAGE OF CUSTOMERS' INFORMATION – DPP2(1)

投訴內容

一間電訊公司的兩名前顧客分別以其新地址再次登記使用固網電話服務。該公司其後按記錄中的舊帳單地址，向顧客發出信件及帳單。顧客獲悉後，向私隱專員投訴他們的個人資料被洩漏予他人。

The Complaint

Two ex-customers re-subscribed to the fixed line telephone services of a telecommunications company at their new addresses respectively. The company subsequently sent letters and bills to the customers' old billing addresses as shown in their records. The customers later learnt about this and filed complaints to the Privacy Commissioner for leakage of their personal data to others.

私隱專員的調查結果

該公司表示造成錯誤是由於職員沒有適當地更新記錄中的顧客帳單地址。如果該公司的自動化系統能夠發現帳單地址與安裝地址不符，應該可提示職員核對地址是否準確，從而避免錯誤的郵遞。不過，該公司的客戶資料庫系統並無這項偵測功能。此外，該公司並沒有標準的核對程序，檢查資料輸入員輸入系統中的顧客資料是否正確。專員亦發現該公司並沒有為職員提供任何指引或程序，確保顧客的個人資料準確。因此，該公司因沒有採取一切合理可行的步驟，確保顧客的個人資料準確而違反了保障資料第 2(1)原則的規定。

Findings of the Privacy Commissioner

The company attributed the mistakes to the failure of their staff to properly update the customers' billing addresses in their records. The wrong mails could have been avoided if the automated system of the company was able to detect the discrepancy between the billing address and the installation address, which should be a sign for verification of the accuracy of the inputted addresses. The company, however, did not provide such detection tool in their customer database system. In addition, the company did not have any standard procedure for counter-checking the correctness of the customer data that the operators inputted into the system. The Commissioner also discovered that the company did not have in place any guidelines or procedures for their staff for ensuring accuracy of customers' personal data. The company was therefore found to have contravened DPP2(1) for failing to take all reasonable practicable steps to ensure accuracy of customers' personal data.

私隱專員所採取的行動

私隱專員向該公司發出執行通知，該公司同意在其系統加上上述的偵測功能，並修訂及實施有關措施及程序，以確保顧客的資料準確，包括加入檢查程序，以及為職員提供培訓及定期講解。

Action by the Privacy Commissioner

The Privacy Commissioner issued an enforcement notice against the company and consequently, the company agreed to develop the said detection tool in their system and also revised and implemented its practice and procedure for ensuring accuracy of customer data, including a counter-checking procedure and providing training and regular briefings to staff.

服務提供者：在使用顧客的資料作推廣活動前，應小心考慮清楚—保障資料第3原則

SERVICE PROVIDERS : THINK CAREFULLY BEFORE USING CUSTOMERS' DATA FOR PROMOTION PROGRAM – DPP3

投訴內容

一間電訊公司的國際直撥電話顧客收到該公司的信件，通知他已獲贈兩個月免費的意外保險。該信附有保險公司發出的保險證書，顧客為受保人。顧客不滿該公司未經他同意，便將他的個人資料交給保險公司，於是向私隱專員提出投訴。

該電訊公司解釋，他們把顧客的個人資料轉移給保險公司，是為了進行聯合推廣活動，向顧客推銷保險產品。該公司聲稱此舉是符合原本收集顧客的個人資料的目的。

私隱專員的調查結果

私隱專員特別考慮到該公司的業務性質是提供電訊服務，與保險無關，而且該公司的顧客並無合理地預期他的資料會被如此利用，所以專員認為利用顧客的資料投保並非收集資料的原本目的。該公司在有關情況下使用顧客的個人資料是違反保障資料第3原則的規定。

私隱專員所採取的行動

公署向該公司發出執行通知，指示它糾正情況。其後，該公司終止了該聯合推廣活動，並制定政策，防止類似的違反事件重演。

The Complaint

A customer of the IDD service of a telecommunications company received a letter from the company informing him that as a gift they gave him a 2 months' free insurance plan against accidents. The letter enclosed an insurance certificate issued by an insurance company, with the customer named as the insured. The customer was dissatisfied that his personal data were passed to the insurer without his consent and thus made a complaint to the Privacy Commissioner.

The telecommunications company explained that they had transferred their customers' personal data to the insurer for a joint marketing program to sell insurance products to their customers, and asserted that this was within the original collection purpose of the customers' personal data.

Findings of the Privacy Commissioner

The Privacy Commissioner was of the opinion that the use of the customer's data for the purpose of taking out an insurance policy was not within the original purpose of collection of the data, taking into account, in particular, the business nature of the company in providing telecommunications services which was unrelated to insurance, and that it would not be within the reasonable expectation of a customer of the company to have his data being used in such manner. The use of customers' personal data by the company in the circumstances was therefore found to be in contravention of DPP3.

Action by the Privacy Commissioner

An enforcement notice was served on the company directing it remedy the situation. Subsequently, the joint marketing program was ceased and the company established a policy to prevent recurrence of similar contravention.

進行戶外推廣活動的公司：必須確保推廣部職員適當地處理顧客的個人資料 — 保障資料第 4 原則

COMPANIES CARRYING OUT OUTDOOR MARKETING ACTIVITIES : MUST ENSURE PROPER HANDLING OF CUSTOMERS' PERSONAL DATA BY MARKETING STAFF –DPP4

投訴內容

一間收費電視公司的營業員到一幢私人住宅大廈進行逐戶推廣活動。營業員向一名男子推銷，他是該公司的前顧客。該男子稍後向專員投訴營業員拿著的電腦打印紙張載有他的姓名及地址，但卻沒有採取任何措施遮蓋資料，以致附近的人很輕易可以看到資料。不過，該公司否認曾派職員到該大廈進行推廣活動。

私隱專員的調查結果

根據所得證據，私隱專員信納該營業員是該公司的僱員，並曾在該大廈進行推廣活動。該營業員在到訪該男子的單位時，確是拿著一疊紙張，內裏載有該男子的個人資料。調查發現，該公司並無向推廣部的職員提供任何關於在戶外推廣時處理個人資料的指引。在有關情況下，該公司因沒有採取合理可行的步驟，確保在戶外進行推廣活動時妥善處理顧客的個人資料，所以違反了保障資料第 4 原則的保安規定。

私隱專員所採取的行動

公署向該公司發出執行通知，要求它就戶外推廣活動中的個人資料保安，制定政策、措施及程序。

The Complaint

A salesman of a pay television company visited a private residential building for a door-to-door promotion campaign. The salesman approached a man who was an ex-customer of the company. The man later complained to the Commissioner that the salesman had carried a computer printout recording the man's name and address but failed to take any steps to conceal the data so that anyone in the vicinity could easily read the data. The company however denied having sent any staff to conduct promotional activities in the building.

Findings of the Privacy Commissioner

Based on evidence available, the Privacy Commissioner satisfied that the salesman was an employee of the company and had carried out the promotional activities at the building. The salesman did hold a pile of paper containing the man's personal data when he visited the man's premises. It was also discovered that the company had not provided any guidelines to their marketing staff regarding the handling of personal data during outdoor marketing exercises. In the circumstances, the company was found to have contravened the security requirements of DPP4 in failing to take any reasonable practicable steps to ensure the proper handling of customers' personal data during outdoor marketing activities.

Action by the Privacy Commissioner

An enforcement notice was issued and the company was required it to devise a policy, practice and procedure regarding personal data security during the conduct of outdoor marketing campaigns.

向行政上訴委員會提出的上訴個案的簡述

Notes on Appeal Cases Lodged with the Administrative Appeals Board

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。同樣，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審結了15宗上訴個案。以下選取一些上訴個案作出簡述：

Under the Ordinance, 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 ("the AAB") against the decision of the Privacy Commissioner in refusing to exercise his powers 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. Similarly, a data user that is the subject of an investigation 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.

A total of 15 AAB appeal cases were heard during the reporting period. Case notes on selected appeal cases are presented below.



仲裁機構在一宗訴訟中向答辯人披露申請人的病假證明書 — 《個人資料（私隱）條例》不適用於司法行為

(行政上訴委員會上訴案件第 39/2004 號)

Disclosure by a Tribunal of an applicant's medical certificate to the respondent in a court action – Personal Data (Privacy) Ordinance has no application to judicial acts

(AAB APPEAL NO.39/2004)

投訴內容

投訴人投訴一仲裁機構於一宗訴訟中在未獲授權下，向答辯人披露司法文件內有關他的個人資料。有關的個人資料是他為申請覆核該仲裁機構的裁決而提交的病假證明書。投訴人指稱該仲裁機構未得到他的同意前不應這樣做，遂向私隱專員投訴此舉違反條例的規定。

The Complaint

The complainant complained against a Tribunal for unauthorized disclosure to the respondent in a court action of his personal data contained in court documents. The personal data in question being his medical certificate submitted in support of his application for a review of the Tribunal's decision. The complainant alleged that the Tribunal should not have done so without his consent and complained to the Privacy Commissioner for contravention of the Ordinance.

私隱專員的調查結果

私隱專員向該仲裁機構進行初步查問。該仲裁機構承認曾就聆訊投訴人申請覆核裁決一事，向答辯人披露投訴人的病假證明書。該仲裁機構認為該病假證明書屬司法文件，而披露行為是司法程序的一部分。該仲裁機構認為司法文件及司法程序兩者均不在條例的監管範圍內。

Findings by the Privacy Commissioner

The Privacy Commissioner conducted preliminary enquiry with the Tribunal. The Tribunal admitted disclosure of the complainant's medical certificate to the respondent for hearing the complainant's application for a review of the Tribunal's decision. The Tribunal considered that the medical certificate constituted court documents and that the act of disclosure was part of the judicial process. It was the view of the Tribunal that both court documents and judicial process were not within the jurisdiction of the Ordinance.

私隱專員同意，該仲裁機構在處理投訴人的申請過程中披露病假證明書屬司法行為，不受條例規限。私隱專員亦認為即使條例適用，有關披露也符合保障資料第 3 原則的規定，因為有關披露是與該仲裁機構當初收集投訴人的個人資料的目的直接有關，就是處理他的覆核申請。因此，私隱專員依據條例第 39(2)(d) 條，拒絕對投訴進行調查。投訴人不滿意有關決定，向行政上訴委員會提出上訴。

The Privacy Commissioner agreed that the disclosure by the Tribunal of the medical certificate in the course of handling the complainant's application was a judicial act which was not within the scope of the Ordinance. The Privacy Commissioner was of the further view that even if the Ordinance was applicable, the disclosure was consistent with the requirement of DPP3 for being directly related to the original purpose of collecting the complainant's personal data by the Tribunal, namely, to handle his judicial application. As such, pursuant to section 39(2)(d), the Privacy Commissioner refused to carry out an investigation of the complaint. Dissatisfied with the decision, the complainant appealed to the AAB.

上訴

委員會同意私隱專員的調查結果。披露投訴人的病假證明書，目的是為了確保公平審訊，答辯人在當時情況下有權知道投訴人申請覆核的理據。該仲裁機構在司法申請中向答辯人披露有關資料屬司法行為，不在條例的監管範圍內。委員會亦同意，即使條例適用，有關披露也符合保障資料第3原則，因為有關披露是與當初收集資料的目的直接有關，就是處理投訴人的覆核申請。

行政上訴委員會的決定

上訴被駁回。

The Appeal

The Board agreed with the Privacy Commissioner's findings. The purpose of disclosing the complainant's medical certificate was to ensure a fair trial and that the respondent was entitled in the circumstances to know the complainant's reasons to support his application for review. The disclosure by the Tribunal to the respondent in a judicial application was a judicial act which was not within the jurisdiction of the Ordinance. The Board also agreed that, should the Ordinance have application, the disclosure would have been consistent with DPP3 for being a purpose directly related to the original purpose of data collection, namely to handle the complainant's court application.

The AAB's decision

The appeal was dismissed.

有關檢控依靠賣淫的收入為生之刑事法律程序 — 控方向與訟中的被告人披露從行動中檢獲的數碼相機記憶卡下載的相片 — 被界定為未用於檢控的資料 (“unused materials”) 展示親密行為及其中一名投訴人的私處 — 普通法中為公平審訊而披露資料 — 直接相關的目的及豁免 — 保障資料第 3 原則及第 58(1)(a) 及 (b) 條及第 58(2) 條

(行政上訴委員會上訴案件第 40/2004 號)

Criminal proceedings for prosecution of offences relating to living on the earnings of prostitution – photographs downloaded from a memory card of digital camera seized during the operation were disclosed to co-defendants of the action by prosecution – photographs classified as “unused materials” showed intimate acts and sex organ of one of the complainants – common law on disclosure for fair trial – directly related purpose and exemptions – DPP3 and section 58(1)(a) and (b) and section 58(2)

(AAB APPEAL NO.40/2004)

投訴內容

兩名投訴人共同投訴一個執法機構向被告控依靠賣淫的收入為生罪名的被告人披露某些相片。有關相片是從一項行動中檢獲的數碼相機記憶卡下載的。相片展示投訴人之間的親密行為及其中一名投訴人的私處。投訴人聲稱披露這些相片令他們感到尷尬，並且違反了保障資料第 3 原則的規定。

The Complaint

The complainants jointly complained about the disclosure of certain photographs by a law enforcement agency to the defendants charged with offences relating to living on the earnings of prostitution. The photographs were downloaded from a memory card of digital camera seized during an operation. They showed intimate acts of the complainants and the sex organ of one of the complainants. The complainants claimed that such disclosure caused them embarrassment and infringed DPP3.

私隱專員的調查結果

經向執法機構查問後，證實有關相片是下載得來的，並且被界定為 “unused materials”，即不會用作支持控方案情的證據。不過，根據普通法的披露資料責任（有關這點，案例 *HKSAR v Lee Ming Tee, FACC1/2003* 被引用為典據），控方有責任向訴訟中的被告人披露這些資料。控方亦援引條例第 58(2) 條有關為罪行的防止或偵測及犯罪者的拘捕、檢控或拘留而持有的個人資料的豁免條文，豁免保障資料第 3 原則的規定適用於有關的個人資料的使用。

Findings by the Privacy Commissioner

Upon enquiry raised with the law enforcement agency, it was confirmed that the photographs in question were downloaded and were categorized as “unused materials”, i.e. not being used as evidence to support the prosecution's case. However, in accordance with the common law duty on disclosure (the case of *HKSAR v Lee Ming Tee, FACC1/2003* was quoted as judicial authority on this point), the prosecution has a duty to disclose these materials to the defendants of the action. The prosecution also relied upon the exemption provisions in section 58(2) of the Ordinance in relation to personal data held for the prevention or detection of crime and the apprehension, prosecution or detention of offenders as applicable to exempt from compliance with DPP3 in respect of the use of the personal data in question.

私隱專員認為，依從普通法規定披露個人資料是與當初收集的目的直接有關，而且無證據顯示那些相片已向無關的人士披露。此外，在本個案的情況下，第 58(1)(b) 及 (2) 條是被適當援用，以豁免受保障資料第 3 原則的管限。依據

The Privacy Commissioner found that compliance with the common law requirements on disclosure of personal data was for a directly related purpose and there was no evidence showing that the photographs were being disclosed to unrelated parties. Moreover, it was found that section 58(1)(b) and (2) were properly invoked in the circumstances

第 39(2)(d) 條，私隱專員並沒有對投訴展開調查。投訴人不滿意有關決定，向行政上訴委員會提出上訴。

上訴

委員會要考慮的問題是：私隱專員不進行調查的決定是否恰當。委員會細閱 *Lee Ming Tee* 案中有關控方披露資料的普通法責任。在普通法中，為求公平審訊，控方有責任將其持有的資料或訊息向辯方披露，公平審訊包括讓辯方對控方案情有足夠知悉的權利。如果控方對辯方隱瞞可能削弱控方案情或可能對辯方案情有利的資料，便會違反這個普通法原則。本身不獲法庭接納為證據的資料，通過一連串的調查，也可能導致找出一些法庭接受的證據，而一些不獲法庭接納的資料亦可能與辯方針對控方證人的可信性而提出的盤問有關，或對此有幫助。

鑑於控罪的性質及考慮到有關相片並無向與控罪無關的人士披露，委員會認為披露相片的目的與收集的目的相符，即為檢控犯罪者。此外，委員會亦同意第 58(1) 及 (2) 條的豁免條文適用於這次個人資料的披露。

行政上訴委員會的決定

上訴被駁回。

of the case to exempt from application of DPP3. Pursuant to section 39(2)(d), no investigation was commenced on the complaint lodged. Dissatisfied with the decision, the complainant appealed to the AAB.

The Appeal

The question to decide by the Board was whether the decision not to investigate by the Privacy Commissioner was properly made. The Board examined the common law duty of disclosure by prosecution as expounded in *Lee Ming Tee's* case. The prosecution is under a common law duty to disclose to the defence material or information in its possession in the interest of a fair trial and the right to a fair trial includes adequate knowledge of the case to be made by the prosecution. It would be contrary to this common law principle if the prosecution were to withhold from the defence materials which might undermine the case against the defendant or which might assist the defence case. Information not itself admissible might lead by a train of inquiry to evidence which is admissible and materials which is not admissible may be relevant and useful for cross examining of a prosecution witness on credit.

In view of the nature of the offence charged and having also considered that the photographs were not disclosed to parties unrelated to the offence charged, the Board found the disclosure to be for a purpose consistent with the purpose of collection, i.e. for prosecution of the offence. Besides, the Board also agreed that the exemption provisions under section 58(1) and (2) applied to such disclosure of the personal data.

The AAB's decision

The appeal was dismissed.

收集停車場訪客的身分證號碼以防止及偵測罪案 — 真正有需要方可收集 — 保存所收集的身分證號碼 — 《身分證號碼及其他身分代號實務守則》(下稱「實務守則」) 第 2.3 條 — 保障資料第 1(1)及 2(2)原則

(行政上訴委員會上訴案件第 41/2004 號)

Collection of identity card numbers of visitors of car park for deterring and detecting crimes – collection is only allowed when there is a real need – retention of collected identity card numbers – clause 2.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers – DPP1(1) and 2(2)

(AAB APPEAL NO.41/2004)

投訴內容

一名司機投訴一座商業大廈停車場的管理公司(下稱「該公司」)在他進出停車場時記錄他的身分證號碼。

The Complaint

A driver lodged a complaint against the management company (“the company”) of a car park in a commercial building for recording his identity card number when he entered and exited the car park.

私隱專員的調查結果

該公司聲稱停車場及商業大廈內曾發生多宗盜竊事件，因此他們採取這政策，以防止罪案及協助警方偵測罪行。他們亦指稱這措施是依從警務處發出的指引。該公司亦援引實務守則第 2.3.2.2 條的規定，該規定容許資料使用者可為條例第 58(1) 條所述的目的(即罪行的防止或偵測；犯罪者的拘捕、檢控或拘留等)而收集身分證號碼。

私隱專員認為，實務守則第 2.3.2.2 條的規定只適用於當時已有收集資料的確切及實際需要，而不應為將來可能有罪案發生這假設而收集。至於該公司所援引的警務處指引，專員認為該指引只適用於進入大廈的訪客，而非用於停車場。由於沒有證據證明收集身分證號碼是有真正需要，該公司的行為違反了實務守則第 2.3 條的規定，因此違反了保障資料第 1(1)原則。由於該公司不應收集及保存身分證號碼，故此該公司亦因無需要保存有關號碼而違反保障資料第 2(2)原則。專員於是發出執行通知，其中要求該公司立即停止收集身分證號碼，並立即銷毀所有已收集的號碼。該公司不滿意專員的決定，向行政上訴委員會提出上訴。

Findings by the Privacy Commissioner

The company claimed that there had been many theft incidents happened in the car park and the commercial building, so they adopted the policy for the purpose of prevention of crime and for assisting the police in detecting crime. They also alleged that the practice was in compliance with the guidelines issued by the police. Reliance was further made by the company on clause 2.3.2.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers (“the Code”) which permits collection of identity card number for the purposes listed under section 58(1) of the Ordinance (i.e. prevention or detection of crime, apprehension, prosecution and detention of offenders, etc.)

The Privacy Commissioner took the view that clause 2.3.2.2 of the Code applied only when there had been a real and practical need for the collection but not for presumption of the possible commission of a crime in the future. In relation to the guidelines issued by the police relied upon by the company, the Commissioner found that it applied only to visitors to a building but not to a car park. In the absence of evidence that manifested the real need for collecting identity card numbers, the company acted contrary to clause 2.3 of the Code, and therefore was in breach of DPP1(1). As the identity card number should not have been collected and retained, the company had breached also DPP2(2) for unnecessarily retaining the number. An enforcement notice was then issued to demand, amongst others, immediate cessation of the collection of identity card numbers and destruction of all collected numbers. Dissatisfied with the Commissioner’s decision, the company lodged an appeal to the AAB.

上訴

委員會裁定，雖然警方曾五次要求該公司提供進出停車場車輛的閉路電視錄影帶，但無證據支持這些錄影帶與指稱的盜竊事件有關。此外，該公司並無提供證據，支持指稱在停車場發生的盜竊數字，以及收集身分證號碼的措施令罪案數字下降。另外，該公司從來沒有採取警方建議的較不侵犯私隱的措施，以防止罪案，例如無需收集身分證號碼的雙證制。至於警務處發出的指引，只適用於到訪大廈，而非開放予公眾使用的停車場。無論如何，該指引並無法律約束力，依從指引並不一定是符合條例的規定。

該公司聲稱他們把收集的身分證號碼保存一個月是為了防止及偵測罪案。同樣地，沒有證據證明如此保存身分證號碼能有助偵測罪犯。事實上，根據該公司記錄，警方從來沒有要求該公司提供所保存的身分證號碼。

行政上訴委員會的決定

上訴被駁回。

The Appeal

The Board ruled that while there were 5 incidents whereby the police required the company to provide the CCTV recordings of vehicles entering and leaving the car park, there was no evidence to support these recordings related to the alleged theft incidents. In addition, the company had not provided evidence to support the alleged numbers of theft incidents happened in the car park and that the practice of collecting identity card numbers had caused a drop of the number of crimes. Moreover, the company never adopted a less privacy intrusive means suggested by the police to deter crimes, i.e. using the two-card system which required no collection of identity card numbers. As far as the guidelines issued by the police was concerned, they were merely directed to visiting building but not car parks that were open to public. In any event, the guidelines were not legally binding and its compliance did not necessarily satisfy the requirements in the Ordinance.

The company claimed that they retained the collected identity card numbers for one month for the purpose of deterring and detecting crimes. Again, there was no evidence to prove that such retention could assist detecting criminals. In fact, according to the company, the police never required the company to produce the retained identity card numbers.

The AAB's decision

Appeal dismissed.



在大廈大堂張貼投訴信件而披露個人資料 — 沒有刪除無關的資料並不違反保障資料第3原則 — 收集不一定是主動地收集 — 調查展開前被投訴的行為已終止 — 未能合理地預計取得更滿意的結果 — 根據第39(2)(d)條行使酌情權 — 委員會不會干預合理、合法及按訂明程序行使的酌情權

(行政上訴委員會上訴案件第47/2004號)

Disclosure of personal data by posting letter of complaint in lobby of a building - failure to delete irrelevant data did not amount to breach of DPP3 — collection unnecessarily meant active collection — cessation of complained act before investigation — a more satisfactory result could not be reasonably expected — discretion under section 39(2)(d) — the Board would not intervene discretion exercised reasonably, legally and in accordance with prescribed procedures

(AAB APPEAL NO.47/2004)

投訴內容

投訴人是一個住宅物業的業主。由於公眾地方的維修欠妥善，導致她的單位滲水。她向大廈的業主立案法團發信投訴此事，信中表示業主立案法團應負擔其單位的維修費用。業主立案法團在收到該封載有投訴人的姓名、地址及電話號碼的信件後，把它張貼於大廈大堂。投訴人向私隱專員公署投訴，業主立案法團在張貼該信前，沒有刪去她的資料，尤其是她的電話號碼。

私隱專員的調查結果

私隱專員認為，張貼該信的目的與收集投訴人的個人資料的目的直接有關，因此並無違反保障資料第3原則的規定。此外，由於業主立案法團其後已把該信除下，繼續調查亦不能合理地預計可帶來更滿意的結果。因此，專員依據條例第39(2)(d)條拒絕進行調查。

上訴

投訴人的部分論點是：

- (i) 業主立案法團公開她的電話號碼，並無理據；
- (ii) 保障資料第3原則不適用於這情況，因為業主立案法團並不是收集資料，它只是收到載有她的個人資料的信件；以及

The Complaint

The complainant, who was the landlord of a residential property, sent a letter to the Owners Incorporation of the building to complain against the water seepage problem caused to her flat because of the improper maintenance of common area. It was said in the letter that the Owners Incorporation should bear the costs of repairing her flat. Upon receiving the letter which contained the complainant's name, address and telephone number, the Owners Incorporation posted the letter in the lobby of the building. The complainant complained to the PCPD that the Owners Incorporation failed to obliterate her data, in particular her telephone number, from the letter before posting it.

Findings by the Privacy Commissioner

The Privacy Commissioner came to the view that the purpose of posting the letter was directly related to the purpose of collecting the complainant's personal data hence, there was no breach of DPP3. Moreover, for the letter had been taken down subsequently by the Owners Incorporation, a more satisfactory result could not be reasonably expected from any further investigation. The Commissioner therefore refused to carry out an investigation pursuant to section 39(2)(d) of the Ordinance.

The Appeal

The complainant sought to argue amongst others, that:

- (i) the Owners Incorporation had no ground to publicize her telephone number;
- (ii) DPP3 had no application in the situation, for the Owners Incorporation did not collect but was only given the letter containing her personal data; and

(iii) 專員不能以調查不會帶來更滿意的結果為理由而拒絕調查，因為該信在大堂張貼時，她的私隱已被侵犯。

委員會裁定，業主立案法團被動地獲得投訴人的投訴信，也是收集她的個人資料，因為「收集」的意思不一定是指主動地收集。張貼該信的目的是通知大廈的所有業主有關滲水的投訴，讓他們有機會表達意見及作出決定。如果滲水問題正如投訴人所述，大廈的所有業主便要負擔維修費用。因此，委員會認為披露該投訴信的目的是與原來收集該信的目的直接有關。

披露附有投訴人的姓名和地址的投訴信內容是必須的，否則業主會懷疑投訴的真實性，對業主立案法團處理問題造成困難。雖然披露電話號碼對張貼該信的目的沒有幫助，但是此舉並無違反保障資料第3原則的規定。

按照第39(2)(d)條，專員可以基於任何理由，拒絕進行調查，只要他的酌情權是合理、合法及按訂明程序行使即可。在這情況下，委員會不會干預他的決定。委員會同意，在本上訴個案的情況下，對投訴人的投訴進行調查是沒有實際的效果，因為要業主立案法團除下信件的目的已經達到。因此，委員會認為專員已合理地行使酌情權，拒絕進行調查。

行政上訴委員會的決定

上訴被駁回。

(iii) The Commissioner could not refuse investigation by stating that investigation could not bring a more satisfactory result, for her privacy had been intruded when the letter was posted in the lobby.

The Board ruled that the Owners Incorporation did collect the complainant's personal data by passively receiving her letter of complaint, for the meaning of "collection" did not necessarily mean active collection. The purpose of posting the letter was to inform all owners of the building, to give them opportunity to express opinion, and to make decision in respect of the water seepage complaint. It was noted that if the water seepage was as stated by the complainant, all owners of the building would have to bear the repair cost. Accordingly, the Board decided that the purpose of disclosure of the complaint letter was directly related to the original purpose of collection of the letter.

It was necessary to disclose the content of the letter together with the complainant's name and address. Otherwise, the owners would doubt the truthfulness of the complaint, thus causing difficulties to the Owners Incorporation in handling the problem. Although disclosure of telephone number was of no assistance to the purpose of posting the letter, DPP3 was not breached.

In accordance with section 39(2)(d), the Commissioner could base on whatever grounds to refuse investigation, provided that he exercised his discretion reasonably, legally and in accordance with prescribed procedures. In this circumstance, the Board would not intervene his decision. The Board agreed that in the circumstances of the appeal case, to carry out an investigation of the complainant's complaint has no practical effect since the purpose of requiring the Owners Incorporation to take down the letter had been fulfilled. The Board therefore decided that the Commissioner had reasonably exercised his discretion to refuse to carry out an investigation.

The AAB's decision

Appeal dismissed.

顧客的信用卡資料轉移到聯營公司 — 聯營公司從信用卡帳戶扣除欠款 — 退回已收款項及承諾日後不再使用有關信用卡的資料，作為補救措施 — 無表面證據證明違反保障資料第3原則 — 專員依據第39(2)(d)條具有廣泛酌情權，可以決定進行或繼續進行調查

(行政上訴委員會上訴案件第52/2004號)

Transfer of customer's credit card data to an associated company – the associated company debited the unsettled amount from the credit card account – remedial actions taken by returning the charged sum and undertaking not to use the credit card data in future – no prima facie case of DPP3 contravention – the Commissioner had a wide discretion whether to carry out or continue investigation pursuant to section 39(2)(d)

(AAB APPEAL NO.52/2004)

投訴內容

投訴人於1999年與一間電訊公司（下稱「甲公司」）登記使用電話及撥號上網服務。她選擇以信用卡自動轉帳方式繳付服務費用。2000年，甲公司把撥號上網服務交由一間聯營公司（下稱「乙公司」）經營，乙公司向投訴人的信用卡繼續收取了五個月的服務費。2003年，投訴人向乙公司申請家居電話服務，並選擇以現金付款。2004年，投訴人沒有以現金繳交費用，乙公司於是從她的信用卡帳戶扣除165元的服務費。投訴人聲稱她從來沒有把信用卡帳戶資料交給乙公司，乙公司無權從她的帳戶扣款，收取她選擇以現金繳付的服務費。投訴人向私隱專員公署投訴乙公司濫用她的個人資料。

私隱專員的調查結果

初步調查展開後，乙公司自願作出補救措施，交回已收取的款項，並承諾日後在未得到明確授權之前，不會使用信用卡資料收取費用。私隱專員認為並無表面證據證明乙公司違反保障資料第3原則，而且該公司已作出補救措施，調查或進一步調查不能帶來更滿意的結果。因此，專員決定不進行或繼續進行調查。投訴人不滿意專員的決定，向行政上訴委員會提出上訴。

The Complaint

In 1999, the complainant registered with a telecommunication company (company A) for telephone service and dial-up internet services. She elected to pay for the use of those services by means of autopay through her credit card account, and for that purpose provided her credit card account number to the company. In 2000, company A spun off its business of dial-up internet services to an associated company (company B) which charged the complainant through her credit card for her continued use of the services for 5 months. In 2003, the complainant applied to company B for home telephone services and chose to pay for the services by cash. In 2004, company B charged the complainant a sum of \$165 for the services and debited the amount from the complainant's credit card account after her failure in settling the same by cash. The complainant claimed that she had never given her credit card account details to company B and they had no authority to debit her account for the services that she had chosen to pay by cash. The complainant lodged with the Commissioner's Office a complaint against company B for the misuse of her personal data.

Findings of the Privacy Commissioner

After the commencement of the preliminary investigation, company B took voluntary remedial steps to return the charged amount and undertook not to use the credit card information for collecting payment in the future without express authorization. The Privacy Commissioner came to the view that there was no *prima facie* case of breaching DPP3 and that, in view of company B's remedial actions taken, investigation or further investigation could not bring a more satisfactory results. Therefore, the Commissioner decided not to carry out or continue investigation. The complainant was dissatisfied with the Commissioner's decision and appealed to the AAB.

上訴

投訴人重申，乙公司濫用她交給甲公司的個人資料，挪用她的金錢。行政上訴委員會認為，根據第39條，尤其是第39(2)(d)條，專員具有廣泛酌情權，可以決定進行或繼續進行調查。在本個案，由於乙公司已自願作出補救措施，專員很合理地認為進一步調查是不必要的。

The Appeal

The complainant reiterated that company B had appropriated her money by misusing her personal data given to company A. The AAB decided that under section 39, the Commissioner had a wide discretion whether to carry out or continue an investigation, in particular, pursuant to section 39(2)(d). In this case, it was reasonably open to the Commissioner to come to the view that any further investigation was unnecessary in view of the voluntary remedial action taken by company B.

行政上訴委員會的決定

行政上訴委員會支持私隱專員的決定，駁回上訴。

The AAB's Decision

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



執法機構完成對一名公務員的調查 — 指控不成立 — 向政府部門發出調查報告，供考慮是否採取行政或紀律行動 — 要求查閱調查報告 — 按執法機構建議，根據第58(1)條拒絕查閱要求 — 豁免不能與持有資料的目的分開 — 該部門不能純粹採取另一資料使用者的觀點而聲稱可獲豁免

(行政上訴委員會上訴案件第 30/2005 號)

A law enforcement body completed investigation against a civil servant – allegations unsubstantiated – an investigation report sent to the government department for consideration of administrative or disciplinary action – sought access to the investigation report – access request refused under section 58(1) as advised by the law enforcement body – exemption was inseparable from the purpose for which the data was held – the department could not simply adopt the view of another data user and claimed the exemption

(AAB APPEAL NO.30/2005)

投訴內容

投訴人是一名公務員，曾被執法機構調查。調查完成後，執法機構的一個委員會收到調查報告（下稱「該報告」）。委員會於是將該報告連同一封信轉交投訴人的上司，信中表示對投訴人的指控不成立，不會採取進一步調查行動。投訴人的上司收到報告後曾與投訴人會面，並向他展示該報告，但拒絕給他一份副本。該報告其後被送交管理組的職員，以供考慮是否需要對投訴人採取行政或紀律行動。個案最後完結，沒有採取有關行動。

投訴人向其服務的部門（下稱「該部門」）要求索取該報告的副本。該部門聲稱不能背離執法機構的反對而披露該報告，因此拒絕要求。投訴人於是根據條例第18條向該部門提出查閱該報告的要求。他的要求再次被拒，理由是執法機構反對披露該報告，而且憑藉條例第58(1)條，該報告可獲豁免披露。投訴人於是向公署作出投訴。

私隱專員的調查結果

私隱專員裁定該部門違反條例第19(1)條，因為他們沒有提出適當的豁免依從查閱資料要求的理由。該部門與執法機構相比，是另一個資料使用者，不能純粹依賴

The Complaint

The complainant, a civil servant, was once under investigation by a law enforcement body. Upon completion of the investigation, a committee of the law enforcement body was presented with an investigation report (“the Report”). The committee then diverted the Report to the supervisor of the complainant together with a letter stating that the allegation against the complainant was not substantiated and that no further investigative action was warranted. After receiving the Report, the supervisor met the complainant and showed him the Report, but refused to give him a copy of it. The Report was then passed to staff of the management unit to consider if it was necessary to take administrative or disciplinary action against the complainant. The case was eventually closed without any such action being taken.

The complainant asked for a copy of the Report from the Department for which he worked (“the Department”). The Department, claiming to have no reason to depart from the law enforcement body’s objection to the disclosure, declined the request. The complainant then lodged a data access request (“the DAR”) under section 18 of the Ordinance with the Department seeking access to the Report. Again, his request was turned down on the ground that the law enforcement body advised against the disclosure and that the Report was exempted from disclosure by virtue of section 58(1) of the Ordinance. The complainant then made a complaint to the PCPD.

Findings of the Privacy Commissioner

The Privacy Commissioner found that the Department had contravened section 19(1) of the Ordinance, for they had failed to put forward any grounds or justifications for claiming exemption to complying with the DAR. The Department, being

執法機構的觀點而聲稱可獲豁免。由於有關的違規行為很可能會繼續或重複，公署向該部門發出執行通知，要求他們採取補救措施。該部門向行政上訴委員會提出上訴。

上訴

該部門辯稱他們具充分理由根據第 58(1) 條拒絕依從查閱資料要求，並認為專員決定各政府部門是不同的資料使用者的看法是錯的，因而以同一份文件來說，對該執法機構可能適用的豁免亦應該同樣對他們適用。

行政上訴委員會表示，當執法機構為了防止或偵測罪行而持有個人資料，資料當事人便不能查閱其他機構為無害的目的而持有的相同個人資料，這說法是不對的。不同人士可能會同一時間為不同目的而持有相同的個人資料。執法機構可能為防止或偵測罪行而持有個人資料，例如個人身分識別資料，但同一時間，某一間公司、醫院或其他機構都會分別為商業目的、醫療目的或特定目的而持有有關資料。

行政上訴委員會亦表示，根據第 58(1) 條聲稱獲得的豁免是與第 18(1) 條及保障資料第 6 原則相連的。資料使用者必須證明他持有資料的目的是其中一個或多個的指定目的，而讓資料當事人查閱該等資料相當可能會損害當時持有資料的目的。豁免是不能與當時持有資料的目的分開的。只有資料使用者持有個人資料的目的符合第 58 條所列的其中一個理由，他才有權根據該條文聲稱獲得豁免。執法機構根據該條文的目的而持有該報告，但該部門卻無權援引相同的豁免。

行政上訴委員會找不到任何資料顯示，依從查閱資料要求相當可能會損害執法機構調查、防止或偵測罪行，或該部門依從查閱資料要求會有實在及重大的風險，導致損害性的影響。該部門收到該報告作參閱，並為行政目的而進行研究。他們的結

different data user from the law enforcement body, could not simply follow the views of that law enforcement body and claimed exemption. As it was likely that the contravention would continue or to be repeated, an enforcement notice was issued against the Department demanding remedial steps to be taken. The Department lodged an appeal to the AAB.

The Appeal

The Department argued that they had established a case which justified refusal to comply with the DAR under section 58(1), and that it was wrong to hold that each government department was different data user and thus the exemption which might apply to the law enforcement body should have been equally applicable to them in respect of the same document.

The AAB stated that it was not right to say that once the personal data were held by a law enforcement agency for the prevention or detection of crime, the data subject could not have access to the same personal data held by the other institutions for innocuous purposes. Different persons might hold the same personal data at the same time for different purposes. Personal data such as personal identification might be held for prevention of crime or detection of crime by a law enforcement agency but at the same time held by a company for commercial purposes or by a hospital for medical purposes or other institutions for their particular purposes.

The AAB further stated that claim of the exemption under section 58(1) was linked to section 18(1) and DPP6. The data user had to show the purposes for which he held the data was one or more of the specified purposes and allowing the data subjects to have access to them would likely prejudice the purposes for which the data were being held. The exemption was inseparable from the purpose for which the data were being held. A data user was only entitled to claim exemption under section 58 if the purposes of that user in holding the personal data matched one of the grounds listed therein. That the law enforcement body might hold the Report for the purposes under that section did not entitle the Department to invoke the same exemption.

The AAB did not find any information that would indicate that compliance with the DAR would be likely to prejudice the investigation, prevention or detection of crime by the law enforcement agency or there would be a real and substantial risk that compliance with the DAR by the Department would have such prejudicial effect. The Department received the

論是，該報告內並無執法機構運作上的敏感資料，而且沒有甚麼是投訴人不知道的。

行政上訴委員會不明白為何該部門要依賴執法機構的反對，拒絕投訴人向他們（作為資料使用者）提出的查閱資料要求。如果他們根據第58(1)條拒絕查閱資料要求，他們應該提供自己的理由，而不是另一資料使用者（並非被查閱資料的對象）的理由。當一個機構為了另一目的把為防止或偵測罪行而持有的資料向另一人（下稱「該另一人」）公開，該另一人所持有資料的目的是與該執法機構不同的，在這情況下，該執法機構必須認為公開資料是安全的，否則他們一開始便不應這樣做，尤其是當他們不能控制得到資料的人會如何使用該等資料。因此，行政上訴委員會並不認為第58條的立法意圖包含了當有關的資料當事人向該另一人查閱持有的資料時，該另一人可以同樣基於公開資料相當可能會損害防止或偵測罪行等理由而拒絕有關的查閱資料要求。

行政上訴委員會的決定

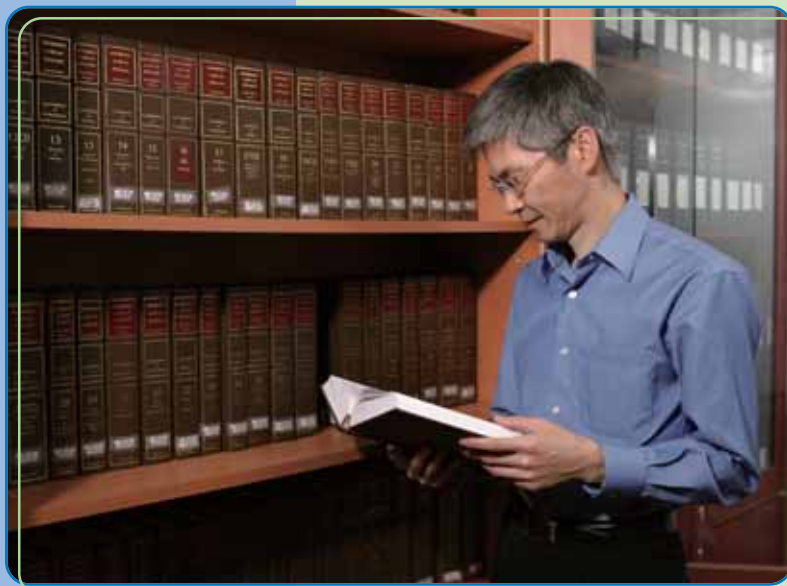
行政上訴委員會支持私隱專員的決定，駁回上訴。

Report for information, and had studied it for administrative purposes. Their conclusion was that nothing in the Report was sensitive to the operation of the law enforcement body and there was nothing in the Report not known to the complainant.

The AAB did not see why the Department had to rely on the law enforcement body's objection to refuse the DAR made to themselves as a data user. If they relied on section 58(1) to decline the DAR, they should provide their own justifications for so doing and not the justifications of another data user who was not a party to the DAR. Where data held by a body for the purpose of prevention or detection of crime were released to another person for a different purpose, the latter did not hold the data for the same purpose as the former. In that case, the body responsible for prevention or detection of crime had to have regarded it safe to release the data, otherwise, they would not have done so in the first place, particularly when they did not retain control of the use of the data by the person to whom the data had been released. That being so, the AAB did not think that section 58 intended that access to the data held by the latter by the data subject should be denied on the ground that the release would be likely to prejudice the prevention or detection of crime, etc.

The AAB's Decision

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



僱主拒絕僱員兼職的申請 — 僱員向法定機構投訴 — 僱主向法定機構提供僱員的病假證明書，以支持其決定 — 為人力資源的目的而收集病假記錄 — 向法定機構披露資料符合收集目的 — 保障資料第3原則

(行政上訴委員會上訴案件第 32/2005 號)

Employee's application of outside work refused by employer – employee complained to a statutory body – employer supplied the employee's sick leave certificates to the statutory body in support of the decision made – sick leave records collected for human resources purposes – disclosure to the statutory body consistent with the purpose of collection – DPP3

(AAB APPEAL NO.32/2005)

投訴內容

投訴人在受聘期間曾經受傷。他向僱主申請准許從事兩份兼職。僱主考慮他的病假記錄及得知他還未完全康復後，拒絕他的申請。投訴人不滿被拒絕，向相關的法定機構（下稱「法定機構」）提出投訴。法定機構向僱主查詢，僱主回應時，提供了投訴人的病假記錄（包括指稱受傷之前的時期）。投訴人指控僱主提供的個人資料多於法定機構所要求的，而且有關披露是違反原本的收集目的，於是向私隱專員提出投訴。

私隱專員的調查結果

私隱專員認為僱主是為了人力資源管理而收集投訴人病假記錄的個人資料。使用該等資料以考慮其兼職申請，是與收集目的直接有關，符合保障資料第3原則。由於投訴人向法定機構投訴其僱主對其申請所作的決定，專員認為僱主有權向法定機構披露促使他作出決定的資料，因此依據第39(2)(d)條拒絕對投訴進行調查。投訴人不滿意私隱專員的決定，向行政上訴委員會提出上訴。

上訴

投訴人在上訴中進一步指稱，由於病假記錄亦載有他的藥方，有關披露是不必要的。委員會強調他們只關心有沒有違反保障資料第3原則。委員會考慮到僱主收集

The Complaint

The complainant suffered past injuries in the course of his employment. He applied to his employer for permission to engage in two part-time jobs. His application was refused by the employer after considering his sick leave records and found that he had not fully recovered from his injuries. Dissatisfied with the refusal, the complainant lodged a complaint with a relevant statutory body ("the statutory body"). Enquiries were raised by the statutory body with the employer who in response furnished it with the sick leave records of the complainant covering periods prior to the alleged injuries. The complainant accused the employer of supplying more personal data than requested by the statutory body and that disclosure was contrary to the original purpose of collection. A complaint was filed with the Privacy Commissioner.

Findings of the Privacy Commissioner

The Privacy Commissioner found that personal data of the sick leave records of the complainant were collected by his employer for the purpose of human resources management. The use of such data in considering his application for part-time employment was for a purpose directly related to the purpose of collection in compliance with DPP3. Since the complainant lodged a complaint against his employer to the statutory body, the Commissioner decided that his employer was entitled to disclose the data considered by it in coming to the decision to the statutory body and refused to investigate this complaint pursuant to section 39(2)(d). Dissatisfied with the decision of the Privacy Commissioner, the complainant lodged an appeal to the AAB.

The Appeal

In his appeal, the complainant further alleged that since the sick leave records also contained the medication prescribed to him, the disclosure was not necessary. The Board emphasized that it was only concerned whether there was

投訴人病假證明書的個人資料很明顯是為了人力資源管理，僱主使用醫療記錄以決定兼職申請，以及其後為回應投訴人對其決定作出的投訴而向法定機構披露該等資料，都沒有違反保障資料第3原則。由於投訴人並無投訴他的藥方被披露，亦沒有向私隱專員提供病假證明書副本，以支持其投訴，私隱專員在作出決定前沒有索取病假證明書副本並無犯錯。

行政上訴委員會的決定

上訴被駁回。

any contravention of DPP3. Having considered the purpose of collection of the personal data of the complainant contained in the sick leave certificates by his employer which was clearly for human resources management, the Board found no contravention of DPP3 in the using of his medical records in determining the application for part-time jobs and the subsequent disclosure to the statutory body in response to the complainant's complaint on the decision made by the employer. The Privacy Commissioner was found not to have erred in not asking for copies of the sick leave certificates before coming to his decision as the complainant did not complain about the disclosure of medication prescribed to him in his complaint nor did he supply the Privacy Commissioner with copies of the sick leave certificates in support of his complaint.

AAB's Decision

The appeal was dismissed.

幼稚園校長披露教師的個人資料(已離婚的狀況) — 未經教師同意而披露資料 — 校長在給私隱專員的信中作出道歉 — 校長承諾日後遵從保障資料第3原則 — 專員根據第39(2)(d)條具有酌情權

(行政上訴委員會上訴案件第 38/2005 號)

The disclosure of a teacher's personal data (her divorce status) by the Headmistress of a kindergarten – disclosure without the teacher's consent – Headmistress apologized letter to the Privacy Commissioner – undertaking by the Headmistress to comply with DPP3 in future – discretion of the Commissioner under section 39(2)(d)

(AAB APPEAL NO.38/2005)

投訴內容

投訴人投訴她任職教師的幼稚園的校長未經她同意，向她的同事披露她已離婚這項個人資料。校長承認在投訴人請病假時，曾向一名代課老師披露她的個人資料。投訴人不同意有關資料是向代課老師披露，認為是向其他校工披露。

The Complaint

The complainant complained against the Headmistress of the kindergarten in which she was working as teacher for disclosure without consent of her personal data, namely her divorce status to her colleagues. The Headmistress admitted having disclosed the personal data to a substitute teacher at the time when the complainant requested for sick leave. The complainant did not agree that the disclosure was made to a substitute teacher but to other workmen of the kindergarten.

私隱專員的調查結果

私隱專員對投訴進行初步查問。校長承認曾向一名代課老師披露資料，但投訴人堅稱有關資料是向其他校工披露。私隱專員認為無論第三者的身分是誰，條例的保障資料第3原則適用於決定有關披露是否合法。

Findings of the Privacy Commissioner

The Privacy Commissioner conducted preliminary inquiry into the complaint. The Headmistress admitted disclosure to a substitute teacher. The complainant however insisted that the disclosure was made to other workmen of the kindergarten. No matter the identity of the third party to whom the disclosure was made, the Privacy Commissioner was of the view that DPP3 of the Ordinance was applicable to determine the legitimacy of the disclosure.

私隱專員認為，校長是為了與聘用投訴人有關的人力資源目的而收集她的個人資料。其後向他人的披露，不論是校長所承認的代課老師，抑或是投訴人指稱的其他校工，都與原本的收集目的沒有直接關係，因此與保障資料第3原則不符。

The Privacy Commissioner found that the personal data of the complainant had been collected by the Headmistress for human resources purposes related to her employment. The subsequent disclosure thereof, whether to a substitute teacher as alleged by the Headmistress or to other workmen as alleged by the complainant, was not directly related to the original collection purpose, hence not consistent with DPP3.

校長知道公署的初步意見後，在致私隱專員的信件中向投訴人致歉，並承諾日後不再披露投訴人的個人資料。根據該承諾及考慮到進一步調查不會達致更佳的结果，私隱專員依據條例第39(2)(d)條拒絕進一步調查。投訴人不滿意有關決定，向行政上訴委員會提出上訴。

Being informed of such preliminary view, the Headmistress apologized to the complainant in her letter to the Privacy Commissioner and undertook not to further disclose the complainant's personal data in the future. On the basis of the undertaking and of the view that further investigation would not yield to better result, the Privacy Commissioner refused to carry out further investigation pursuant to section 39(2)(d) of the Ordinance. Dissatisfied with the decision, the complainant appealed to the AAB.

上訴

投訴人在聆訊中放棄上訴。委員會認為，調查投訴是為了查出校長究竟有沒有違反條例的規定，如果有的話，便考慮採取適當措施，防止違規情況再次發生。專員的初步查問已確定校長有違反規定，而她承諾遵守規則，因此調查的目的已經達到。條例的目的是減低私隱被侵犯的可能性，以保障個人資料。條例的目的不是要懲罰違反條例的資料使用者，亦不是賦予私隱專員懲罰的權力。即使投訴人因其離婚狀況被披露而蒙受損失，專員亦無權處理有關申索，或要求校長向任何人道歉。不過，校長確在其承諾書中致歉，並願意親自向投訴人道歉。這都顯示她日後會小心處理員工的個人資料，避免違反條例的規定。

行政上訴委員會同意，私隱專員具有酌情權，可以根據第 39(2) 條拒絕進行調查，而只要決定是合理、合法及按訂明程序作出，委員會是不會干預的。委員會認為專員已合理地行使酌情權，因此應該駁回上訴。

行政上訴委員會的決定

投訴人放棄上訴，而行政上訴委員會認為不管怎樣，該上訴是應該被駁回的。

The Appeal

The complainant abandoned her appeal at the hearing. The Board considered that the purpose of carrying out an investigation of the complainant's complaint was to find out whether the Headmistress had contravened the requirement of the Ordinance and if so, to consider taking appropriate measures to prevent repetition of the breach. The Commissioner's preliminary inquiry confirmed the Headmistress' contravention and she had undertaken to abide by the rules, hence the purpose of investigation completed. The purpose of the Ordinance was to reduce the possibility of infringement of privacy in order to protect personal data. The purpose of the Ordinance was not to punish the data user who infringed the Ordinance nor did the Ordinance confer such power of punishment to the Privacy Commissioner. Even if the complainant had suffered any damages as a result of disclosure of her divorce status, the Commissioner had no power to handle any such claim, or to require the Headmistress to apologize to anybody. However, the Headmistress did in her letter of undertaking expressed her apology and her willingness to apologize to the complainant in person. All these revealed that she would be careful in her future handling of staff personal data to avoid any contravention of the Ordinance.

The AAB agreed that the Privacy Commissioner had the discretion to refuse investigation under section 39(2) and the Board would not intervene as long as the decision was reasonable, legal and in accordance with prescribed procedures. The discretion of the Commissioner was found by the Board to have been reasonably exercised, the appeal should hence be dismissed.

The AAB's Decision

The complainant abandoned the appeal and the AAB found that the appeal should in any event be dismissed.