聆聽分析市民的申訴

The art of listening and analysis

執行部員工感言
Message from Staff of Operations Division

在公署的執行部工作，我的職責包括就涉嫌違反條例規定的事宜進行調查，及採取適當的跟進行動，以促使違例者遵從條例的規定，從而改善整體社會在保障個人資料私隱方面的情況。

從接獲投訴個案開始，到個案最後得以完滿解決，實在是步步為營，重重挑戰。投訴個案中，有些性質看似相近，但實不相同；有些有案例可循，卻不可一概而論。在處理過程中所獲得的經驗及體會，可教我一生受用。

在我處理過的投訴個案中，有很多機構已就保障個人資料私隱制定政策，可惜部分機構未能確保員工遵從有關政策，因而引致投訴的產生。不過，大部分被投訴的機構對公署的調查一般都會作出相當積極的回應，並採取有效的補救措施及作出承諾，確保日後遵守條例的有關規定，使個案得以迅速解決。

至於投訴的一方，在我接觸過的投訴人當中，大多數都知道自己的個人資料私隱權利，但部分投訴人未能清楚領會條例的立法原意並不是以懲罰性的手段來達到保障個人資料私隱的目的，他們認為違反保障資料原則即等同犯罪，應立即予以檢控並處以重罰。然而，經過公署不斷作出溝通及調解，絕大部分的投訴人都能理解條例的規定，並滿意被投訴者的補救措施，個案亦得以完滿解決。

有機會參予公署的調查工作，著實帶給我不少的滿足感，還令我感受到工作背後那份使命感。我會繼續認真執行保障個人資料私隱的工作，希望透過這份工作，讓投訴人與被投訴者明白雙方都應該小心處理個人資料，以避免不必要的爭執或損失。

程燕芳
助理個人資料主任

In the PCPD's Operations Division, my duties include investigation of suspected breaches of the Ordinance and taking appropriate follow up actions to ensure that offenders comply with the Ordinance so as to enhance personal data privacy protection in the community at large.

From receipt of a complaint to full settlement of the case, I have to act cautiously as challenges are abundant. Though some of the complaint cases seemed to be similar, in fact they were not the same. There were precedents for some cases, but they were not definitely applicable. The experience I got from the handling of these cases is invaluable for the rest of my life.

Among the complaint cases that I handled, many organizations had put in place policies on protection of personal data privacy. Unfortunately, some of them could not ensure compliance with the policies by their staff, which gave rise to complaints. However, most of the parties complained against gave active response to the PCPD's investigation, adopted effective remedial actions and undertook to comply with the requirements of the Ordinance in future. Complaint cases could then be resolved quickly.

Although most of the complainants knew their rights of personal data privacy, some of them were not aware that the legislative intent of the Ordinance was to protect personal data privacy by taking remedial rather than punitive measures. They thought that contravention of data protection principles was an offence, which required immediate prosecution and heavy penalty. However, after continuous communication and mediation of the PCPD, most of the complainants understood the requirements of the Ordinance and were satisfied with the remedial actions taken by the parties complained against. As a result, cases were resolved to the satisfaction of the parties.

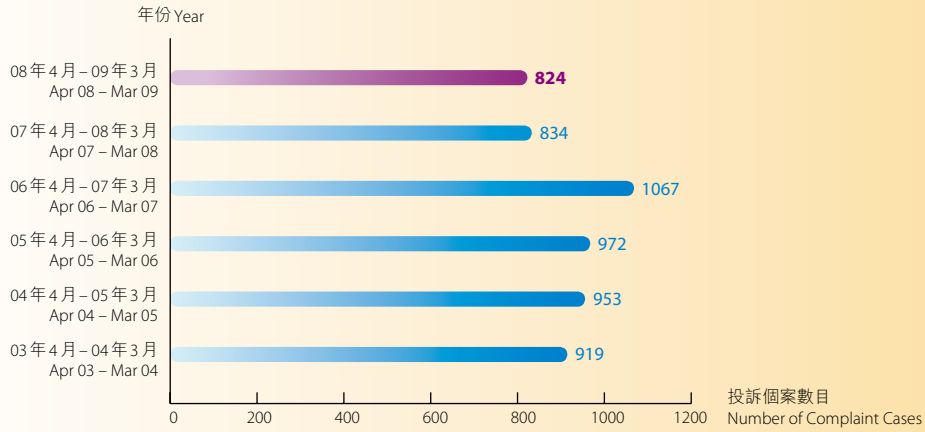
Participation in the PCPD's investigation work gave me enormous satisfaction and made me realize the mission of my work. I will keep on carrying out my duties to protect personal data privacy conscientiously. I hope that both complainants and parties complained against could handle personal data carefully to avoid unnecessary disputes or losses.

Agnes Ching
Assistant Personal Data Officer

在二零零八至零九年度接獲的投訴個案
Complaints Received during 2008-2009

圖表 FIGURE 1

每年的投訴個案
Annual Complaint Caseload

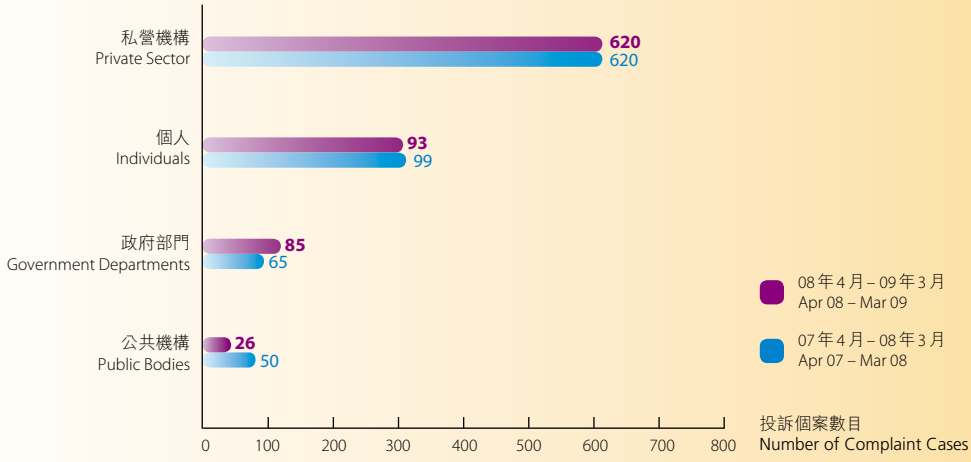


在二零零八至零九年度公署共接獲824宗投訴個案（較去年輕微下降了1%）。

A total of 824 complaint cases were received in 2008-2009 (a slight decrease of 1% on the previous year).

圖表 FIGURE 2

被投訴者的類別
Types of Party Complained Against

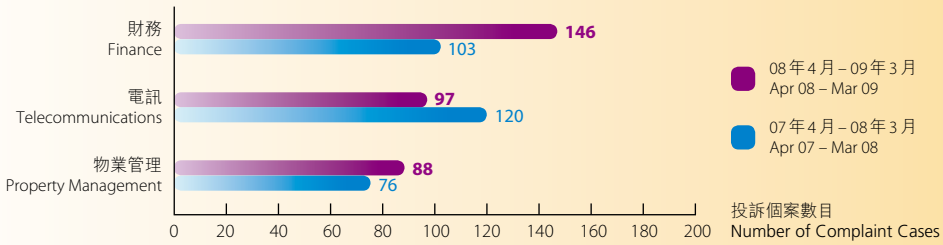


- 620宗（75%）個案投訴私營機構。
- 111宗（14%）個案投訴公營機構（即政府部門及其他公共機構）。
- 93宗（11%）個案投訴個人。

- 620 (75%) complaint cases were against private sector organizations.
- 111 (14%) complaint cases were against public sector organizations (i.e. government departments and other public bodies).
- 93 (11%) complaint cases were against individuals.

圖表 FIGURE 3

對私營機構的投訴
Complaints Against Private Sector Organizations

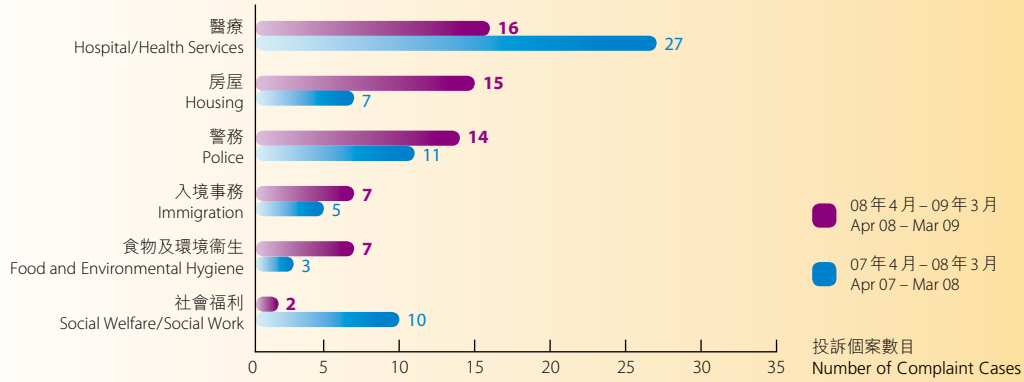


在投訴電訊業及財務機構的個案中，大部分被指非法使用或披露客戶的個人資料。在投訴私營機構的個案中，較上年度大幅上升的是指稱資料使用者持有不準確個人資料及不必要地保留個人資料（50%）、欠缺個人資料的保安措施（37%），及沒有依從查閱資料要求或改正資料要求（29%）的個案數目。

The majority of complaints against the telecommunications and financial sectors alleged the unlawful use or disclosure of customers' personal data. Among the complaints against private sector organizations, it is noted that there have been considerable increases in the numbers of allegations of inaccurate personal data held by the data users and unnecessary retention of personal data (50%); lack of security measures to protect personal data (37%) and non-compliance with data access or correction requests (29%) as compared with the previous year.

圖表 FIGURE 4

對公營機構的投訴
Complaints Against Public Sector Organizations



在投訴公營機構的個案中，大部分涉及被指：

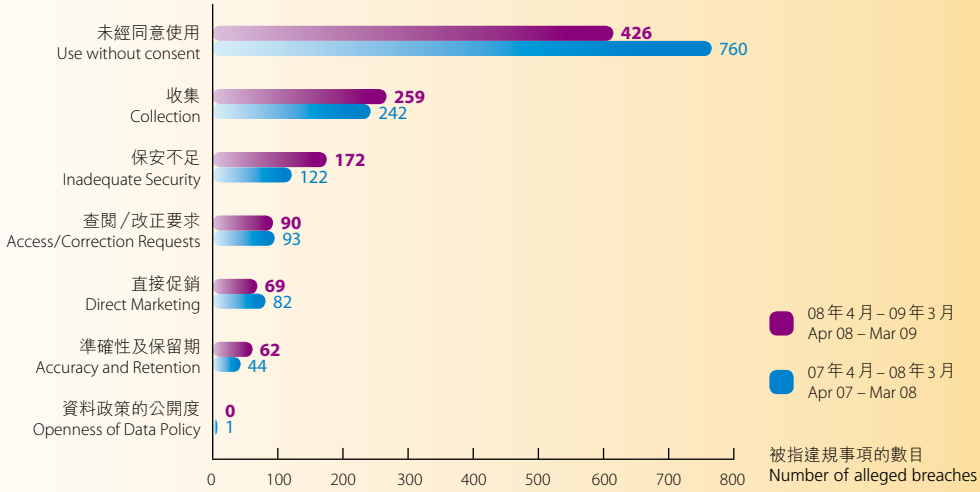
- 與不符收集目的及未取得當事人同意而使用或披露個人資料（31%）；
- 欠缺保障個人資料的保安措施（28%）；
- 過量或不公平收集個人資料（27%）；及
- 未能遵守查閱資料要求或改正資料要求（12%）。

The majority of complaints against public sector organizations involved allegations of:

- use or disclosure of personal data beyond the scope of collection purpose and without the consent of the individual (31%);
- lack of security measures to protect personal data (28%);
- excessive or unfair collection of personal data (27%); and
- non-compliance with data access or correction requests (12%).

圖表 FIGURE 5

投訴的性質
Nature of Complaints



二零零八至零九年度接獲的824宗投訴個案共涉及1,078項被指違反條例的規定。在這些事項中，919項（85%）被指違反保障資料原則的規定，以及159項（15%）被指違反條例的主體條文。

在919項被指違反保障資料原則的事項中，259項（28%）涉及過度或不公平收集投訴人的個人資料。在這類個案中，49項（19%）主要涉及財務機構或電訊公司被指從不明來源收集投訴人的個人資料作追收欠債或直接促銷用途。

有些投訴人對條例在收集個人資料方面的適用範圍有所誤解。一個常見的例子是，有些投訴人認為他們的個人資料只可以直接向他們收集、或在取得他們的同意後才可收集、或他們必須獲得知會。條例規定個人資料須以合法及在有關個案的所有情況下屬公平的方法收集。不過，條例並沒有規定資料使用者要得到資料當事人的同意才可向第三者收集他的個人資料，或將有關收集通知他。行政上訴委員會在一宗行政上訴個案中裁定，只是證明某人持有個人資料這點證據，不能證明他是用不公平或不合法的手段獲得該些資料。因此，單是從資料當事人以外的來源收集個人資料（資料當事人不知情或沒有給予同意），並不算違反條例的規定。此外，條例並無條文規定資料使用者需向資料當事人披露他取得個人資料的來源。

The 824 complaint cases received in 2008-2009 involved a total of 1,078 alleged breaches of the requirements of the Ordinance. Of these, 919 (85%) were alleged breaches of the data protection principles and 159 (15%) were alleged contraventions of the provisions in the main body of the Ordinance.

Of the 919 alleged breaches of the data protection principles, 259 (28%) concerned the alleged excessive or unfair collection of personal data of complainants. In this category, 49 cases (19%) involved allegations, most of them are against financial institutions or telecommunications companies, of collection of complainants' personal data from unknown sources for the recovery of debts or direct marketing purposes.

There is a misunderstanding among some complainants regarding the ambit of the Ordinance when applies to collection of personal data. A common example is that some complainants believe that their personal data can only be collected from them direct or after prior consent having been obtained from them or that they must be notified of it. The Ordinance provides that personal data shall be collected by means which are lawful and fair in the circumstances of the case. However, the Ordinance does not require a data user to obtain the consent of the data subject for collection from third party of his personal data or to notify him of the collection. In an administrative appeal case, the Administrative Appeals Board ruled that the mere evidence of the holding of personal data by a person could not prove that he had obtained the data by unfair or unlawful means. Accordingly, the collection of personal data from sources other than the data subject without his knowledge or consent, without more, does not suggest a contravention of the Ordinance. Moreover, there is no provision in the Ordinance that requires a data user to disclose to the data subject the source from which the data user obtained the personal data.

調查投訴
Complaint Investigations

圖表 FIGURE 6

二零零八至零九年度處理的投訴摘要
Summary of Complaints Handled in 2008-2009

	2005-06	2006-07	2007-08	2008-09
上年轉來的投訴 Complaints carried forward	195	188	188	**148**
接獲的投訴 Complaints received	972	1067	834	**824**
經處理的投訴的總數 Total complaints processed	1167	1255	1022	**972**
已完結的投訴 Complaints completed	979	1067	874	**799**
處理中的投訴 Complaints in process	188	188	148	**173**

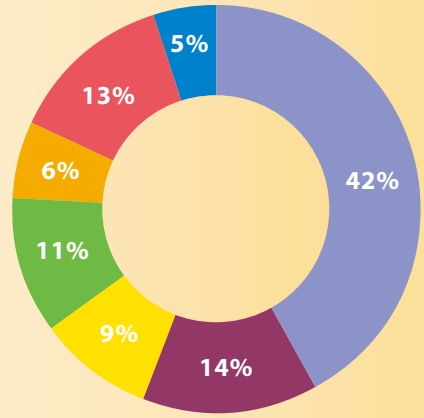
在本年報期開始時，公署正處理上年度帶下來的148宗投訴，加上新收到的824宗投訴，私隱專員在本年報期內共須處理972宗投訴。在這些個案中，799宗（82%）在本年報期內已經完結，而餘下的173宗（18%）在二零零九年三月三十一日時仍在處理中（圖表6）。

At the beginning of the reporting year, 148 complaints were being processed. With the 824 new complaints received, the Privacy Commissioner handled a total of 972 complaints during the reporting period. Of these, 799 (82%) cases were completed during the reporting year while the balance of 173 (18%) cases were still being processed on 31 March 2009 (Figure 6).

圖表 FIGURE 7

投訴結果
Outcome of Investigations

沒有表面證據 No *prima facie* case	42%
沒有管轄權 No jurisdiction	14%
證據不足 Unsubstantiated	9%
調解 Mediation	11%
撤回 Withdrawn	6%
沒回應/其他規管機構處理 No response/other authority	13%
正式調查 Formal investigation	5%



在本年報期內完結的799宗個案：

- 334宗（42%）沒有表面證據；
- 111宗(14%）不在條例的管轄範圍；
- 89宗（11%）透過調解得到解決；
- 37宗（5%）在進行正式調查後得到解決；
- 73宗（9%）在向被投訴者查詢後發現證據不足；
- 46宗（6%）在初步查詢期間由投訴人撤回；及
- 餘下的109宗（13%）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由其他規管機構，例如警方跟進。

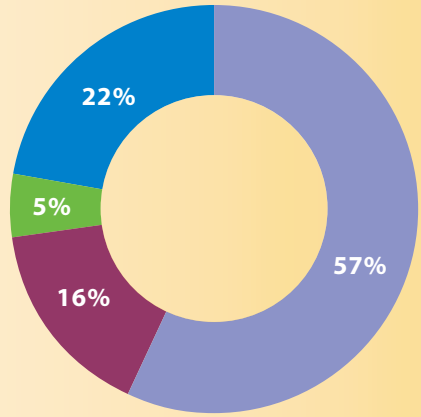
Of the 799 cases completed during the reporting period:

- 334 (42%) cases were found to have no *prima facie* case;
- 111 (14%) cases were outside the jurisdiction of the Ordinance;
- 89 (11%) cases were resolved through mediation;
- 37 (5%) cases were resolved after formal investigations;
- 73 (9%) cases were found to be unsubstantiated after enquiries with the parties being complained against;
- 46 (6%) cases were withdrawn by complainants during preliminary enquiries; and
- the remaining 109 (13%) cases involved mostly complaints where the complainants did not respond to the Commissioner's inquiries or where the matter had been transferred or reported to other authorities, e.g. the Hong Kong Police Force.

圖表 FIGURE 8

正式調查結果
Results of Formal Investigations

違反保障資料原則的規定 Contravention (Data Protection Principles)	57%
違反條例主體條文的規定 Contravention (Provisions)	16%
無違例 No contravention	5%
中止調查 Discontinued	22%

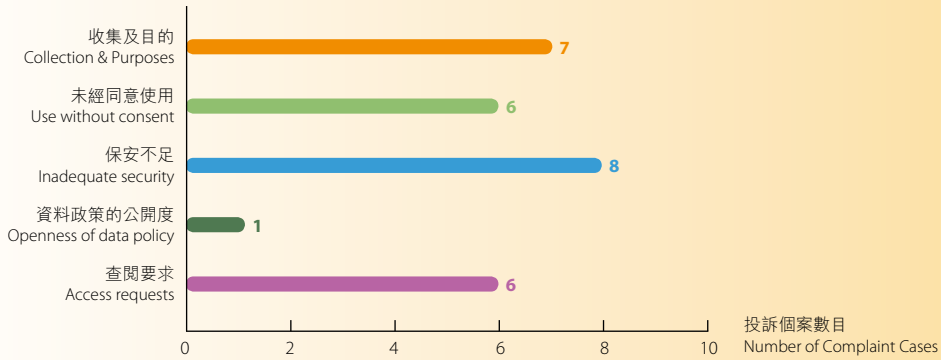


在本年報期內完成正式調查的37宗個案中，私隱專員發現其中27宗（73%）違反了條例的規定，2宗（5%）並無違例或因缺乏證據而無法證明有違例情況。餘下8宗（22%）則是因投訴人決定不再跟進有關事項而中止調查。

Of the 37 formal investigations completed during the reporting period, the Commissioner found contravention of the requirements of the Ordinance in 27 (73%) cases. In two (5%) cases, either no contravention was found or contravention was not established due to insufficient evidence. The eight (22%) remaining cases were discontinued as the complainant decided not to pursue the matter further.

圖表 FIGURE 9

違例事項的性質
Nature of Contravention

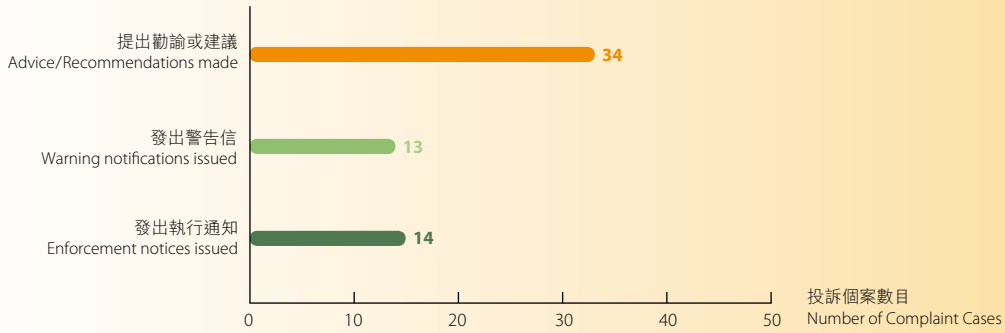


在被確定違反條例規定的27宗個案中，21宗違反一項或以上保障資料原則，其餘6宗違反了條例主體條文的規定，所涉及的違例事項與依從查閱資料要求有關（圖表9）。

Of the 27 cases where the requirements of the Ordinance were found to have been contravened, 21 cases involved contravention of one or more of the data protection principles. The remaining six cases involved contravention of the requirements of the main body of the Ordinance relating to compliance with data access requests (Figure 9).

圖表 FIGURE 10

根據調查結果採取的行動
Actions Taken as a Result of Investigation



在89宗透過調解得到解決的個案中，私隱專員向34間機構提出勸諭及／或建議，以協助它們在行事方式及程序上遵守保障資料原則及條例的其他規定。

在被確定違反條例規定的27宗個案中，私隱專員向被投訴的資料使用者發出14份執行通知，以防止它們繼續或重複違反規定。至於餘下的13宗個案，被投訴者已採取或書面承諾採取糾正措施，私隱專員因而毋須作出強制性行動，發出執行通知，而只是向有關資料使用者發出警告信。

In the 89 cases resolved through mediation, the Commissioner provided advice and/or recommendations to 34 organizations on their practices and procedures in order to assist them in complying with the data protection principles and other requirements of the Ordinance.

Of the 27 cases in which requirements of the Ordinance were found to have been contravened, the Commissioner issued enforcement notices on the parties complained against in 14 cases to prevent continuation or repetition of the contraventions. In the remaining 13 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 necessary, and warning notices were issued.

處理資料方面的改善
Improvements in Data Handling

以下是本年報期內的一些個案，闡明資料使用者在接獲投訴後迅速作出回應，並在私隱專員的指引下，實行改善保障個人資料私隱的措施。

The following cases in the reporting year illustrate how data users made prompt responses to complaints and implemented measures under the guidance of the Commissioner to improve personal data privacy protection.

收集犯事者的個人資料：不應為執法目的而收集超乎適度的個人資料—保障資料第1(1)原則

Collection of personal data of offenders: should not collect excessive personal data for the purpose of law enforcement action – Data Protection Principle ("DPP") 1(1)

投訴內容

投訴人因被指觸犯定額罰款罪行而被政府部門的人員截停。投訴人按要求向該人員提供其香港身份證，以便該人員填寫一份定額罰款罪行通知書（下稱「通知書」）。投訴人投訴該人員收集了他的出生日期。

The Complaint

The complainant was stopped by an officer of a government department for having committed an alleged fixed penalty offence. As requested by the officer, the complainant provided his Hong Kong Identity Card for the officer to complete a notice in relation to the alleged fixed penalty offence (the "Notice"). The complainant complained that the officer had collected his date of birth.

結果

該政府部門解釋，出生日期是用以計算犯事者的年齡，那是司法機構在有需要提起法律程序時所需的資料。

私隱專員認為就該執法目的而言，收集年齡（而非詳細出生日期）已足夠。該政府部門接納私隱專員的建議，停止收集犯事者的出生日期，並刪除以前所收集的有關資料。

Outcome

The government department explained that the date of birth was used for calculating the age of the offender that was required by the Judiciary for instituting court proceedings where necessary.

The Commissioner considered that the collection of the age, rather than the full date of birth, would be sufficient for the purpose of the enforcement action. The government department accepted the advice of the Commissioner by ceasing the practice of collecting offenders' dates of birth and deleting the data previously collected.

公司進行跨業直銷活動：給予夥伴公司的客戶個人資料只限於客戶的聯絡資料 — 保障資料第3原則

Company conducting cross-marketing activities: should limit customers' personal data to be passed to partner company to customers' contact information only – DPP 3

投訴內容

投訴人是A公司的客戶。為了訂購A公司的服務，投訴人向A公司提供其姓名、出生日期、香港身份證號碼及車輛登記文件的複本。投訴人其後收到B公司推廣汽車保險計劃的信件。該信夾附一份保險計劃報價單，載有投訴人的姓名、年齡及車輛資料（包括車牌號碼、車輛類別、型號及汽缸容量）。投訴人投訴A公司在沒有他的訂明同意下向B公司披露了他的個人資料，以作推廣用途。

The Complaint

The complainant was a customer of Company A. For the purpose of subscribing the services of Company A, the complainant had provided his name, date of birth, Hong Kong Identity Card number and a copy of his car registration document to Company A. The complainant subsequently received a letter from Company B, promoting motor vehicle insurance plan. The letter enclosed an insurance plan quotation containing the complainant's name, age and vehicle information (including vehicle number, vehicle class, model and cylinder capacity). The complainant complained that Company A had disclosed his personal data to Company B for marketing purpose without his prescribed consent.

結果

根據投訴人訂購A公司服務的申請資料及文件，私隱專員認為A公司可為推廣汽車保險計劃而把投訴人的個人資料移轉予B公司。不過，私隱專員認為，就進行直接促銷的目的而言，只可移轉那些讓B公司能聯絡投訴人的資料。該些資料應只限於投訴人的姓名、地址及電話號碼。因此，在個案的情況下，移轉投訴人的出生日期、香港身份證號碼、年齡及車輛資料是不必要的，及可能已違反保障資料第3原則的規定。

A公司接納私隱專員的意見，並承諾只向B公司移轉那些讓它能夠聯絡客戶的資料，例如姓名、地址及電話號碼。

Outcome

According to the information and documents relating to the complainant's subscription application for Company A's services, the Commissioner accepted that Company A may transfer the complainant's personal data to Company B for promoting motor vehicle insurance plan. However, the Commissioner is of the view that for the purpose of conducting direct marketing, only those data which would enable Company B to contact the complainant could be transferred. Such data should be limited to the complainant's name, address and phone number. The transfer of the complainant's date of birth, Hong Kong Identity Card number, age and vehicle information was therefore not necessary under the circumstances and might have contravened the requirement of DPP3.

Company A accepted the views of the Commissioner and undertook to transfer to Company B only those data which would enable Company B to contact the customers, e.g. name, address and telephone number.

機構准許員工於流動裝置內儲存個人資料：必須保障個人資料不受未獲准許或意外的查閱 — 保障資料第4原則

Organizations allowing storage of personal data in mobile devices: must protect personal data from unauthorized or accidental access – DPP4

投訴內容

一間慈善機構的一名義工（資料當事人）獲該慈善機構通知，該機構一名人員的手提電話在港鐵車廂內被盜，電話內載有該機構所有義工及客戶的個人資料，包括姓名、香港身份證號碼、聯絡地址及電話號碼（以下統稱「該等資料」）。

The Complaint

A volunteer (the data subject) of a charitable organization was informed by the charitable organization that a mobile phone containing personal data of all its volunteers and clients, including name, Hong Kong Identity Card number, correspondence address and telephone number (collectively the "Data"), was being stolen from an officer of the charitable organization in an MTR train.

結果

該慈善機構解釋，他們向其人員提供該手提電話，並授權該人員儲存該等資料，以作緊急聯絡及在有需要時提供支援之用。不過，他們沒有就保障儲存於手提電話內的該等資料制定任何政策或內部指引（例如規定人員把該等資料加密）。因此，遺失手提電話可能會引致電話內的該等資料外洩。結果，該慈善機構禁止其職員把該等資料儲存於手提電話或其他類似的儲存媒體內。

Outcome

The charitable organization explained that they provided the mobile phone to their officer and authorized her to store the Data for the purpose of emergency contact and providing support where necessary. However, they failed to devise any policy or internal guidelines on the protection of the Data stored in mobile phone (such as requiring the officer to encrypt such Data). As such, leakage of the Data stored in the mobile phone may be arisen from the loss of the mobile phone. As a result of the complaint, the charitable organization had forbidden its staff from storing such Data in mobile phone or other similar storage media.

財務機構收到客戶的查閱資料要求：必須在法定時限內依從有關要求 — 第 19(1) 條

Financial institution receiving customer's data access request: must comply with the request within statutory time limit – Section 19(1)

投訴內容

投訴人透過一間銀行購買了雷曼迷你債券及其他投資產品。其後，投訴人向該銀行提出兩項查閱資料要求(下稱「該等查閱資料要求」)，索取有關他購買投資產品的文件複本，例如他所簽署的合約及個人風險評估表格(以下統稱「要求資料」)。但該銀行沒有回應該等查閱資料要求。

The Complaint

The complainant subscribed Lehman Mini-bond and other investment products through a bank. Subsequently, the complainant submitted two data access requests (the "DARs") to the bank for copies of documents relating to his subscription of the investment products, such as his signed contract and personal risk evaluation form (collectively the "Requested Data"). However, the bank failed to respond to the DARs.

結果

該銀行解釋，事件是因處理該等查閱資料要求的職員失察，沒有把該等查閱資料要求交給相關部門處理而引起的。經公署查詢後，該銀行已向投訴人提供要求資料的複本。該銀行亦向全體員工發出通告，提醒他們妥善處理客戶的查閱資料要求。

Outcome

The bank explained that the incident was caused by the oversight of the staff member handling the DARs who failed to pass the DARs to the relevant department for processing. Upon enquiries of the PCPD, the bank had provided a copy of the Requested Data to the complainant. The bank also issued a notice to all staff reminding them to handle data access requests made by customers properly.

從投訴中學習
Lessons Learnt from Complaints

以下投訴個案能舉例說明本年報期內一些資料使用者被確定違反條例規定的各種作為或行為。公署是基於有關事件的實況作出挑選，旨在述明受條例（包括保障資料原則）管限的行為之多樣性。

The following complaint cases illustrate some data users' 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 matters and demonstrate the wide variety of conducts that are subject to the provisions of the Ordinance, including those of the Data Protection Principles ("DPPs").

向顧客收集個人資料的商戶：必須確保所收集的資料屬足夠但不超乎適度 — 保障資料第1(1)原則

Shops collecting customers' personal data: must ensure that the data collected are adequate but not excessive – DPP1(1)

投訴內容

投訴人的家人於一間洗衣店磅洗枕袋及床單，當時店員在單據上記錄了投訴人的家人的姓氏及手提電話號碼。投訴人其後到該店欲領取衣物，卻未有帶備該店發出的單據。店員表示如投訴人未能出示單據，便須記錄身分證資料。投訴人提議以她講出其家人的姓氏及電話號碼代替登記身分證資料，但該店員不接受。投訴人遂向公署投訴該店收集她的身分證號碼。

該店解釋是根據由私隱專員發出的《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段所准許的情況，即「為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」，而收集投訴人的身

The Complaint

When a family member of the Complainant gave pillowcases and bedspreads to a laundry shop for washing, the staff of the laundry shop recorded the surname and mobile phone number of the family member on the invoice. Later, the Complainant went to the shop to pick up the laundry, but she had not brought along the invoice. The staff told the Complainant that if no invoice were presented, identity card information would be recorded. The Complainant suggested to inform the staff the surname and mobile phone number of the family member as a substitute, but the suggestion was rejected. The Complainant then lodged a complaint with the PCPD complaining collection of her identity card number by the laundry shop.

The shop explained that it collected the Complainant's identity card number under section 2.3.3.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers ("the Code") issued by the Commissioner, i.e. "to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances".

投訴內容 *(續)*

分證號碼。該店續解釋，為保障顧客及該店本身的利益，以及避免顧客的衣物被他人冒領，他們會要求未能出示單據的顧客，報案並向他們提供報案紀錄紙；或如顧客同意的話，讓他們記錄其姓名及身分證號碼，才會發放衣物。不過，該店承認自1990年開業以來，從未因顧客的衣物被他人冒領而作出任何賠償。此外，該店的店員確認投訴人為他們的常客，並經常在未有出示單據的情況下領取衣物。

The Complaint *(continued)*

The shop further explained that to protect the interest of customers and the shop, and to avoid fraudulent claims of laundry, customers without invoices would be requested to report the case to the police and present the police's acknowledgment slip to it; or if they agree to do so, let it record their names and identity card numbers, before releasing the laundry. However, the shop admitted that it had not paid any compensation for any fraudulent claim of laundry since its opening in 1990. Moreover, the staff of the shop recognized that the Complainant was the shop's frequent customer, who often collected laundry without presenting invoice.

結果

根據私隱專員的調查結果顯示，該店收集顧客身分證號碼的目的，是為了在遇到有冒領衣物的情況時，該店可以將所收集的身分證號碼交予警方偵測罪案。至於上述該店所表示是根據實務守則第2.3.3.3段的情況而收集身分證號碼，店長未能提供任何資料以顯示其收集身分證號碼的做法如何可防止他們受到超過輕微程度的損害或損失。

雖然實務守則第2.3.2.2段准許資料使用者為了防止或偵測罪行等情況，收集身分證號碼，但私隱專員認為只可在有實際需要收集身分證號碼的真實情況下，才引用實務守則第2.3.2.2段。案中該店從沒有就冒領衣物情況報警求助或得到警方的指示提供顧客身分證號碼以協助調查。該店不可單從他們認為冒領情況可能發生或警方可能會要求他們提供顧客身分證號碼，而收集顧客的身分證號碼。至於就確定投訴人是否真正代表有關顧客（即其家人）領取衣物，私隱專員認為，有效的辦法是要求投訴人講出有關顧客留下作紀錄的名稱及/或電話號碼及詳述清洗衣物的日期、種類、款式、數量及顏色等作核對。如該店仍有懷疑的話，他們更可以致電有關顧客作查詢或要求該顧客親身前來領取。

私隱專員認為，該店收集顧客身分證號碼的做法是不必要及超乎適度的，並向該店發出執行通知，指示該店終止有關做法，及銷毀所收集得的身分證號碼記錄。

Outcome

The Commissioner found that the shop's purpose of collecting customers' identity card numbers was to provide the identity card numbers to the police in the event of fraudulent claims of laundry. Regarding the collection of identity card numbers under section 2.3.3.3 of the Code, the shop had not provided any information to show how the collection of identity card numbers could prevent it from suffering damage or loss which was more than trivial.

Though section 2.3.2.2 of the Code allows data users to collect identity card numbers for the prevention or detection of crime, the Commissioner considers that section 2.3.2.2 of the Code can only be invoked when there is actual need to collect identity card numbers. In this case, the shop had never sought assistance from the police; nor received any direction from the police to provide identity card numbers for investigation of any fraudulent claim of laundry. The shop could not collect customers' identity card numbers solely because there might be fraudulent claims or it might be required by the police to provide identity card numbers. On the question of how to confirm whether it was true that the Complainant collected the laundry on behalf of the relevant customer (i.e. her family member), the Commissioner considered that the effective way was to ask the Complainant to give the name and/or mobile phone number of the relevant customer before; and to state the date, type, style, quantity and colour of the laundry for verification. If the shop still had doubt, it could call the relevant customer for enquiry or request the customer to collect the laundry in person.

The Commissioner was of the view that the collection of identity card numbers by the shop was unnecessary and excessive. An enforcement notice was served on the shop directing it to cease such act and destroy all the identity card numbers so collected.

僱主向其他職員披露僱員的個人資料：必須確保只在「有需要知道」的基礎下披露個人資料 — 保障資料第3原則

Employer disclosing employee's personal data to other staff members : must ensure that the personal data are disclosed only on a "need-to-know" basis – DPP3

投訴內容

投訴人是一間大學某學系（下稱「該學系」）的行政級人員，同時亦擔任該學系內某管理委員會（下稱「該委員會」）的秘書(是最高級的非教學委員)。投訴人需要向該學系的系主任（下稱「X先生」）匯報其工作，並要管理該委員會的一般行政及運作。此外，投訴人的上司（即X先生）亦擔任該委員會的主席。

由於X先生對投訴人的工作表現不滿，因此向投訴人發出一封警告電郵，並在沒有投訴人的同意下，把該警告電郵的全部內容抄送給該委員會的所有委員，部分委員是投訴人的下屬。

The Complaint

The Complainant was an executive staff of an academic department in a university (the "Department"). At all material times, the Complainant also served as the secretary (the most senior non-academic member) of a specific management committee within the Department (the "Committee"). The Complainant needed to report her duties to the head of the Department ("Mr. X") and to oversee the general administration and operation of the Committee. On the other hand, the Complainant's supervisor, i.e. Mr. X also acted as the chairman of the Committee.

Since Mr. X was dissatisfied with the Complainant's working performance, he sent a warning email to the Complainant and, without the Complainant's consent, copied the full contents of the warning email to all members of the Committee, some of them were the Complainant's subordinates.

結果

保障資料第3原則訂明，如無有關的資料當事人的訂明同意，個人資料不得用於（包括披露或移轉）下列目的以外的目的：(i)在收集該等資料時會將其使用於的目的；或(ii)直接與前述(i)項所提及的目的有關的目的。公署得悉撰寫該警告電郵的目的是檢討投訴人的工作表現。該大學解釋，向該委員會所有委員披露該

Outcome

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used (including disclosed or transferred) for any purpose other than (i) the purpose for which the data were to be used at the time of collection of the data; or (ii) a purpose directly related to the purpose referred to in the aforesaid item (i). It was noted that the warning email was compiled for the purpose of reviewing the work performance

結果 (續)

警告電郵是必需的，因為該委員會的其中一項職權是就「人力及其他資源調配」提供意見，而披露該警告電郵可讓各委員確定投訴人工作表現的不足。

私隱專員的調查顯示，沒有足夠證據證明各委員獲賦權檢討投訴人的工作表現。此外，私隱專員注意到X先生只是把該警告電郵抄送給各委員，並無要求他們就投訴人的表現提供建議或意見。因此，很難令私隱專員相信，電郵接收者是知道他們需要就該警告電郵的內容給予意見，以檢討投訴人的工作表現。

基於以上所述，私隱專員認為該大學並非基於「有需要知道」的準則向該委員會的各委員發送該警告電郵，從而披露了投訴人的個人資料，而且有關披露的目的並不是與收集目的相同或與之直接有關。因此，私隱專員認為該大學違反了保障資料第3原則的規定。

公署向該大學送達執行通知，要求它採取步驟，通知其獲賦權向員工發出書面警告的職員，不要向第三者披露警告的內容，除非有關披露的目的是與收集目的相同或與之直接有關，或已取得資料當事人的訂明同意。

Outcome *(continued)*

of the Complainant. The university explained that the disclosure of the warning email to all members of the Committee was necessary because one of the purviews of the Committee was to give advice on "deployment of human and other resources" and the disclosure of the warning email enabled the Committee members to ascertain the deficiency found on the Complainant's work performance.

According to the findings of the Commissioner, there was insufficient evidence to support that the Committee members were empowered to review the work performance of the Complainant. In addition, the Commissioner noted that Mr. X merely forwarded the warning email to the Committee members without requesting the recipients to render their advice or views on the Complainant's performance. It was therefore hardly to convince the Commissioner that the email recipients could acknowledge that they were assumed to give views on the contents of the warning email for the purpose of reviewing the Complainant's working performance.

On the basis of the above, the Commissioner considered that the university's disclosure of the Complainant's personal data by forwarding the warning email to the members of the Committee was not on a "need to know" basis and such disclosure was not for the same purpose as or a purpose directly related to the purpose of collection of the data. Accordingly, the Commissioner found that the university had contravened the requirement of DPP3.

An enforcement notice was served on the university requiring it to take steps to notify its supervising staff who were empowered to give written warnings to staff members not to disclose the contents of the warnings to any third party unless the disclosure was for the same purpose as or a purpose directly related to the purpose of collection; or the prescribed consent has been obtained from the data subject.

僱主對員工進行監察：必須以公平的方法進行並預先告知員工有關的監察行動 — 保障資料第 1(2) 及 5 原則

Employers monitoring employees' activities: must be by fair means and inform employees of the monitoring exercise in advance – DPP1(2) and DPP5

投訴內容

投訴人的工作性質需要使用電腦，故此她的僱主（下稱「該機構」）為她安排工作枱上設有一台可以收發電郵及使用互聯網的電腦（下稱「該電腦」）。為保安理由，投訴人獲分配一個用戶名稱及自設密碼（下稱「該密碼」），以用作登入該機構的電腦系統。投訴人的上司曾多次以該機構要求「緊急之用」為理由，要求她提供該密碼，她最終亦將該密碼告知上司。

The Complaint

The Complainant needed to use computer in her work, so her employer ("the organization") arranged for her a computer ("the computer") which could access to email and Internet service. For security purpose, the Complainant was assigned a user name and a password that was set by herself ("the password") to log in the computer system of the organization. The supervisor of the Complainant had asked her several times for the password for "emergency use" of the organization. She finally disclosed the password to her supervisor.

投訴內容 *(續)*

投訴人其後被上司發現於辦公時間使用該電腦進行網上遊戲活動。就此，投訴人的上司在取得該機構的同意下，在投訴人下班後，使用投訴人較早前提供的該密碼登入該電腦收集她瀏覽網站的資料（即儲存在電腦內的cookies資料，下稱「該些cookies資料」）。投訴人得悉事件後向公署投訴該機構在她不知情的情況下登入該電腦收集該些cookies資料。

該機構表示該電腦屬其財物，只供投訴人公事上使用。故此，該電腦內所儲存的資料也應屬該機構所擁有，因而該機構有權進入該電腦並查閱所儲存的資料。此外，該機構認為投訴人的上司查閱該電腦內的資料並非為收集投訴人的「個人資料」，而該些cookies資料亦非投訴人的個人資料。不過，在公署調查案件期間，該機構已刪除該些cookies資料。

The Complaint *(continued)*

The Complainant's supervisor later found that the Complainant had played online games on the computer during office hours. In this connection, the Complainant's supervisor, with the consent of the organization, logged into the computer with the password provided by the Complainant when the Complainant was off duty and collected information about her browsing activities (i.e. the cookie data stored in the computer ("the cookies"). After realizing the incident, the Complainant complained to the PCPD that the organization logged in the computer and collected the cookies without notifying her.

The organization said that the computer belonged to the organization and was only provided to the Complainant for business use. Therefore, the data stored in the computer were also owned by it. Thus, it had the right to log into the computer and access the data stored therein. Moreover, the organization believed that the Complainant's supervisor did not mean to collect the Complainant's "personal data" when accessing the data in the computer, and the cookies were not the personal data of the Complainant. During the PCPD's investigation, the organization had deleted the cookies.

結果

由於cookies只是關於某台電腦曾瀏覽網站的資料，如cookies並不包含任何可識辨個別人士身份的資料（例如有關使用者的姓名），單只cookies本身便不符合個人資料的定義。換句話說，cookies在某一個案中是否屬個人資料，須視乎個案中的cookies是否包含可識辨個別人士身份的資料，或是否連同其他可識辨個別人士身份的資料而被持有或使用。

鑑於該些cookies資料載有可識辨投訴人身份的英文名，加上該些cookies資料是投訴人的上司為針對投訴人的涉嫌違規行為而建立的記錄，私隱專員認為有關做法構成收集投訴人的個人資料。

私隱專員調查發現，該機構並沒有採取實際措施去阻止或禁止投訴人使用該電腦作私人用途或儲存私人資料。另外，該機構容許各僱員自行更改電腦密碼，而沒有規定僱員必須向同事提供電腦密碼，或於每次更改電腦密碼後即時通知其他同事。案中亦無證據顯示除投訴人的上司外，其他職員亦知悉投訴人的電腦密碼。私隱專員認為在一般的情況下，投訴人是該電腦的唯一使用者，其他職員應不會在投訴人不知情下使用該電腦。

Outcome

As cookies are the browsing data of a computer, if a cookie does not contain any data that could identify an individual (e.g. the name of the user), the cookie alone does not satisfy the definition of personal data. In other words, the question of whether cookies in a particular case are personal data would depends on whether the cookies contain any data that can identify an individual, or whether they are held or used together with other data that can identify an individual.

As the cookies contained English names that could identify the Complainant and that the cookies were the records gathered by the Complainant's supervisor to deal with the suspected misconduct of the Complainant, the Commissioner considered that the act of the organization constituted collection of the Complainant's personal data.

The Commissioner found that the organization had not taken any practical measures to stop or prohibit the Complainant from using the computer for private purpose or storage of private data. In addition, the organization allowed its employees to change passwords themselves, without requiring them to provide their passwords to their colleagues, or to inform other colleagues of their passwords upon each change. There was no evidence in the case showing that apart from the Complaint's supervisor, other staff members also had knowledge of the Complainant's password. The Commissioner found that in normal circumstances, the Complainant was the sole user of the computer and other staff members would not use the computer without notifying the Complainant.

結果 *(續)*

投訴人的上司使用投訴人提供的該密碼登入該電腦收集該些cookies資料，明顯與當初要求投訴人提供該密碼時所述的目的並不一致，而他向投訴人索取電腦密碼時所指的工作需要或「該機構要求」的目的卻又太過籠統。由於該些cookies資料與投訴人的日常工作並無直接關係，即使投訴人可能會預期她的上司會登入該電腦找尋工作所需的資料，亦不會合理地預期她的上司會在她下班後使用她提供的該密碼登入該電腦以收集該些cookies資料。

根據個案所得的資料，私隱專員認為該機構如此收集該些cookies資料並不符合投訴人使用該電腦的合理私隱期望。

另一方面，私隱專員認為除非有相關特殊情況的理據支持，資料使用者不應以隱蔽方式收集個人資料，因為此舉嚴重侵犯個人私隱。假若投訴人的上司於辦公時間內在投訴人面前登入該電腦，應不會損害有關檢查該電腦的目的。個案中並無資料顯示該機構曾研究採用其他私隱侵犯程度較低的替代方案。

Outcome *(continued)*

It was apparent that the act of the Complainant's supervisor using the password provided by the Complainant to log into the computer for collecting the cookies was inconsistent with the purpose as stated by the supervisor when asking for the password from the Complainant. The stated purpose of working need or "the organization's request" was too general. As the cookies were not directly related to the Complainant's daily work, even if the Complainant might expect that her supervisor would log into the computer to look for data which were job related, she would not have reasonably expected that her supervisor would log into the computer with her password to collect the cookies when she was off duty.

Having regard to the information available, the Commissioner considered that the collection of the cookies by the organization was not consistent with the reasonable expectation of privacy of the Complainant in using the computer.

On the other hand, the Commissioner took the view that unless justified by the special circumstances of the case, data users should not collect personal data by covert means because this would seriously intrude an individual's privacy. If the Complainant's supervisor logged into the computer in the presence of the Complainant during office hours, such act should not affect the purpose of checking the computer. There was no evidence showing that the organization had considered using other less privacy intrusive alternatives.

結果 *(續)*

私隱專員認為投訴人的上司使用當初為「該機構要求」而取得的電腦密碼，在投訴人不在場的情況下，登入該電腦查閱她瀏覽網站的資料（即該些cookies資料），屬以不公平的方法收集個人資料，該機構因而違反了保障資料第1(2)原則的規定。

在個案發生時，該機構只制定了一份內容簡單的通告，提及該機構的電腦只供僱員公事上使用等，但通告沒有指明會利用僱員的電腦密碼進入其電腦收集其上網記錄。再者，沒有資料顯示該機構曾於投訴人入職時向她發出有關通告。就此，私隱專員認為該機構未曾向投訴人清楚指出進行僱員監察的目的；可能進行監察的情況；或收集資料的用途，故該機構並沒有根據《保障個人資料私隱指引：僱主監察僱員工作活動須知》第3.2.4及3.3.1段採取步驟確保投訴人能夠知悉政策內容。

Outcome *(continued)*

The Commissioner was of the view that the act of the Complainant's supervisor in logging into the computer with the password obtained at "the organization's request" to obtain the in the absence of the Complainant amounted to collection of personal data by unfair means and thus the organization had contravened DPP1 (2).

When the incident occurred, the organization had only formulated one brief notice stating that the computers of the organization could only be used for business by staff, with no mention of the policy that the organization would log into employees' computers with their passwords to collect their browsing activity data. Furthermore, there was no information showing that the organization had issued the notice to the Complainant upon entering into employment. In this connection, the Commissioner considered that the organization had not clearly notified the Complainant of the purpose of conducting employee monitoring, the circumstances under which monitoring might be conducted, or the use of the data so collected. Therefore, the organization had not taken steps under paragraphs 3.2.4 and 3.3.1 of "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" to ensure that the Complainant be informed of its employee monitoring policy.

結果 *(續)*

考慮到個案的所有情況，私隱專員認為該機構並無採取所有切實可行的步驟，令投訴人確定或得悉該機構有關記錄僱員使用該機構電腦瀏覽網頁方面的政策及實務，因而違反了保障資料第5原則的規定。

就該機構違反保障資料第1(2)原則方面，私隱專員向該機構發出執行通知，指示該機構停止利用僱員提供的電腦密碼，登入電腦查閱該僱員所瀏覽的網站記錄，除非事先獲得該名僱員的同意。

此外，該機構已制訂有關的監察及保安政策，並已提示僱員注意有關政策，私隱專員認為該機構已採取相應的措施，令僱員能確定或得悉該機構有關監察僱員使用電腦瀏覽互聯網的政策，故毋須就保障資料第5原則方面向該機構發出執行通知。

Outcome *(continued)*

After considering all the circumstances of the case, the Commissioner opined that the organization had not taken all practicable steps to ensure that the Complainant could ascertain or be informed of the policy and practices of the organization in relation to recording employees' activities of browsing the Internet by using the organization's computer. The organization thus contravened DPP5.

Regarding the organization's contravention of DPP1(2), an enforcement notice was issued to the organization directing it to stop using passwords obtained from employees to log into their computers and access their browsing activity data, unless their prior consent was obtained.

The organization had put in place its monitoring and security policies and had reminded its employees of the policies. The Commissioner considered that the organization had taken appropriate measures to ensure that its employees could ascertain or be informed of the policy of the organization on monitoring employees' use of its computer in Internet browsing. Therefore, there was no need to issue an enforcement notice in respect of the contravention of DPP5.

資料使用者依從索取醫療記錄的查閱資料要求：應提供記錄中所載個人資料的複本，而不是給予醫療報告 — 第19條

Data user complying with data access request for medical records : should supply a copy of the personal data contained in the records rather than giving a medical report – Section 19

投訴內容

投訴人在一間機構接受牙科治療後，向牙醫管理委員會投訴該機構所聘任的牙醫，指控他專業失當。牙醫管理委員會為了調查該投訴，要求投訴人提供相關的牙科記錄。因此，投訴人向該機構提出查閱資料要求（下稱「該查閱資料要求」），索取其牙科記錄的複本。該機構向投訴人表示可向投訴人提供一份牙科報告，收費400港元。投訴人投訴該機構沒有依從她的查閱資料要求。

該機構認為牙科記錄不單載有投訴人的個人資料，亦載有主診牙醫的觀察及診斷，且該機構的政策是病人的記錄只會給予執法機構。該機構進一步表示，投訴人不應以查閱資料要求作為工具，為訴訟找尋資料，或協助她向其他規管機構提出投訴。該機構補充，他們只會直接向牙醫管理委員會提交投訴人的牙科記錄。

The Complaint

After receiving dental treatment provided by an organization, the Complainant lodged a complaint to the Dental Council against the dentist employed by the organization, accusing him of professional misconduct. In order to investigate the complaint, the Dental Council requested the Complainant to provide the relevant dental records, the Complainant thus made a data access request (the "DAR") to the organization for a copy of her dental records. The organization replied to the Complainant that they would furnish the Complainant with a dental report at a fee of HKD400. The Complainant complained against the organization for failing to comply with her DAR.

The organization was of the view that the dental records contained not only the Complainant's personal particulars, but also the observations and diagnosis of the dentist-in-charge and it was their policy to release patients' records only to law enforcement agencies. The organization further stated that DAR should not be used as a tool for the Complainant to locate information for litigation or assist her to lodge complaint to other regulatory bodies. The organization further added that they would only submit the Complainant's dental records to the Dental Council direct.

結果

根據條例第2條，「資料」指在任何文件中資訊的任何陳述（包括意見表達）。因此，毫無疑問，投訴人的牙科記錄所載的資料，包括牙醫對投訴人的診斷及觀察，均屬於投訴人的個人資料。該機構同意向投訴人提供的牙科報告是有別於該查閱資料要求所要求的牙科記錄。雖然牙科報告是根據牙科記錄而撰寫，或牙科報告可能包括牙科記錄中投訴人的部分個人資料，但向投訴人提供牙科報告是不足以依從該查閱資料要求（除非牙科報告包括牙科記錄中投訴人的全部個人資料的複本，情況如是的話，就依從該查閱資料要求而收取400港元看來是超乎適度）。

因此，私隱專員認為該機構沒有在收到該查閱資料要求後40日內向投訴人提供牙科記錄中投訴人的個人資料複本，違反了條例第19(1)條的規定。

私隱專員向該機構送達執行通知，指令它向投訴人提供牙科記錄中投訴人的個人資料複本。

Outcome

"Data" is defined under section 2 of the Ordinance as any representation of information (including an expression of opinion) in any document. Thus there was no doubt that the data contained in the Complainant's dental records, including in particular the dentist's diagnosis and observations about the Complainant, amounted to the Complainant's personal data. The dental report which the organization agreed to provide to the Complainant was different from the dental records requested in the DAR. Although the dental report was written based on the dental records or the dental report might include some of the Complainant's personal data as contained in the dental records, the furnishing of the dental report to the Complainant was not sufficient for complying with the DAR (unless the dental report includes a copy of all the Complainant's personal data in the dental records, in which case the charge of HKD400 for complying with the DAR would seem excessive).

The Commissioner was therefore of the view that the organization had contravened section 19(1) of the Ordinance for failing to provide a copy of the Complainant's personal data contained in the dental records to the Complainant within 40 days after receiving the DAR.

An enforcement notice was served on the organization directing it to provide the Complainant with a copy of the Complainant's personal data contained in the dental records.

拒絕查閱資料要求：必須小心考慮條例的第20條及其他豁免情況是否真正適用 — 第19、20及59條

Refusal of data access request: must carefully consider whether section 20 and other exemptions of the Ordinance really apply – sections 19, 20 and 59

投訴內容

投訴人任職一政府部門（下稱「該部門」）。由於投訴人曾放取超過90日病假，故此她在該部門的安排下，出席醫事委員會（下稱「醫委會」）為評估她的健康而在醫院管理局轄下的一間醫院（下稱「該醫院」）召開的醫委會會議（下稱「該會議」），協助該部門評估她是否適宜執行其正常職務的事宜。

其後，投訴人向該部門遞交了一份「個人資料（私隱）條例查閱資料要求表格」（下稱「有關要求」），要求該部門向她提供醫委會就該會議發出的醫委會報告（下稱「該報告」）的副本。但該部門致函投訴

The Complaint

The Complainant worked in a government department ("the department"). As the Complainant had taken sick leave over 90 days, the department asked her to attend a meeting ("the meeting") held by the Medical Board at a hospital ("the hospital") under the Hospital Authority for the purpose of assessing her health condition so as to assist the department to evaluate whether she was fit for her normal duties.

Later, the Complainant submitted a "Personal Data (Privacy) Ordinance Data Access Request Form" ("the request") to the department requesting for a copy of the Medical Board report ("the report") issued in respect of the meeting by the Medical Board. However, the department

投訴內容 *(續)*

人，通知她有關要求遭拒絕。投訴人不滿該部門拒絕依從她的有關要求，遂向公署作出投訴。

該部門解釋個案屬條例第20(3)(d)條所述的情況，即該醫院有權控制該報告的使用，並禁止該部門依從有關要求；及該報告與投訴人的身體健康或精神健康有關，獲條例第59條豁免。

The Complaint *(continued)*

informed the Complainant in writing that the request was refused. Dissatisfied with that the department's refusal, the Complainant lodged a complaint with the PCPD.

The department explained that the situation mentioned in section 20(3)(d) of the Ordinance applied to the case, i.e. the hospital was entitled to controlled the use of the report and prohibited the department from complying with the request; and also that the report was related to the physical or mental health of the Complainant and thus exempt from section 59 of the Ordinance.

結果

私隱專員調查發現，該部門於收到有關要求時，該醫院已把該報告寄給該部門。該部門在收到投訴人的有關要求後，曾向該醫院查詢是否反對該部門向投訴人提供該報告的副本。該醫院回覆該部門表示不適宜向投訴人提供該報告，但該醫院並無禁止該部門向投訴人提供該報告的副本，而該報告的內容亦沒有禁止該部門使用該報告的字句。即使在該部門回覆投訴人的信中，也沒有表示他們是基於條例第20(3)(d)的情況而拒絕依從有關要求。因此，該部門指他們是根據條例第20(3)(d)條拒絕依從有關要求的理據不能成立。

至於條例第59條豁免方面，該部門與該醫院間的通信記錄顯示，該部門在拒絕有關要求前，從沒有跟該醫院談及如果提供該報告的副本，會否損害投訴人的身體健康或精神健康，或者談及條例第59條是否適用。該部門在拒絕依從有關要求時，亦沒有表示有關要求遭拒絕的

Outcome

The investigation of the Commissioner found that when the department received the request, the hospital had already sent the report to the department. After receipt of the request, the department had asked the hospital if it objected to the release of a copy of the report to the Complainant. The hospital replied that it was not appropriate to provide the Complainant with the report, but the hospital did not prohibit it. Further, there was no wording in the report prohibiting the department from using the report. Even in the department's reply letter to the Complainant, the department had not mentioned that it refused the request under section 20(3)(d) of the Ordinance. Therefore, the grounds of the department in refusing to comply with the request under section 20(3)(d) could not be established.

Regarding the exemption of section 59 of the Ordinance, the correspondence between the department and the hospital revealed that before rejecting the request, the department had never discussed with the hospital whether the provision of a copy of the report would cause harm to the physical or mental health of the Complainant, or whether section 59 of the Ordinance was applicable. When the department refused to comply with

結果 *(續)*

理由是該報告獲條例第59條豁免。即使其後在該部門致投訴人的補充信件中，該部門也沒有向投訴人透露這一點。故此，私隱專員認為該部門在拒絕依從有關要求時，實際上並無考慮條例第59條的豁免情況，他們當時亦沒有任何客觀證據，證明提供該報告的副本便相當可能會對投訴人或其他人士的身體健康或精神健康造成嚴重損害。

由於該部門並未有在收到投訴人的有關要求後的40日內依從有關要求，因此違反了條例第19(1)條的規定。私隱專員向該部門發出執行通知，指示該部門在符合條例第20(1)(b)條及第20(2)條的規定下(即在向投訴人提供資料之前，刪除資料中可識辨其他人士身份的詳情，除非該等人士已同意向投訴人披露他們的個人資料)，依從投訴人的有關要求，向她提供該報告內屬其個人資料的複本。

Outcome *(continued)*

the request, it had not said that it was because the report was exempt from section 59 of the Ordinance. Even in its further letter to the Complainant, the department had not mentioned this. Therefore, the Commissioner found that when the department refused to comply with the request, it had not actually considered the exemption of section 59 of the Ordinance. Besides, at that time the department had no evidence showing that the provision of a copy of the report would likely cause serious harm to the physical or mental health of the Complainant or other persons.

As the department did not comply with the request within 40 days after receiving it, the department had contravened the requirement of section 19(1) of the Ordinance. The Commissioner issued an enforcement notice to the department, directing it to comply with the Complainant's request by providing her with a copy of her personal data in the report subject to the requirements under sections 20(1)(b) and 20(2) of the Ordinance (i.e. before providing the data to the Complainant, identifying particulars of other individuals had to be deleted, unless they had consented to the disclosure of their personal data).

根據《個人資料(私隱)條例》第48(2)條發表的報告
Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance

條例第48(2)條訂明，私隱專員在完成一項調查後，如認為如此行事是符合公眾利益的，可發表報告(下稱「報告」)，列明該項調查的結果及由該項調查引致的、私隱專員認為適合作出的任何建議或其他評論。

在本年報期內，私隱專員發表了兩份報告，分別關於(i)一間醫院沒有採取所有切實可行的步驟，保障病人的個人資料；及(ii)一所大學沒有依從查閱資料要求。

Under section 48(2) of the Ordinance, the Commissioner may, after completing an investigation and if he opines that it is in the public interest to do so, publish a report ("Report") setting out the investigation results and any recommendations or comments arising from the investigation that he sees fit.

During the reporting year, the Commissioner published two Reports regarding (i) failure to take all practicable steps to safeguard patients' personal data by a hospital; and (ii) failure to comply with data access request by a university respectively.

醫院須採取所有切實可行的步驟，保障病人的個人資料

2008年12月24日，私隱專員發表一份報告，公布私隱專員就一名病人(下稱「投訴人」)投訴一間醫院遺失其個人資料所作出的調查結果。

背景

該醫院的一名護士(下稱「該護士」)被派駐不同地點工作，並獲提供一個USB閃存驅動器(下稱「該USB」)，用以儲存醫療資料、將病人的登記資料傳送回辦公室，及把有關資料輸入總電腦檔案中。該護士其後發現該USB的密碼保護區損壞了，且無法存取資料，因此她把由她處理的26名病人(包括投訴人)的登記資料複製至該USB的非密碼保護區，並繼續使用該USB，而沒有向其上司報告此事。其後，該護士發現遺失了該USB。她曾作出搜尋，但未能尋獲該USB，她約於3個月後向其上司報告遺失事件。該USB載有26名病人的個人資料(例如姓名、香港身份證號碼及聯絡電話號碼)。

事件發生後，該醫院採取連串補救措施，其中包括向提供與該護士相同的服務的護士收回所有發放給他們的USB，並刪除內存的所有病人資料；通過利用內聯網電郵戶口及傳真以儲存及傳送病人的個人資料；以及發出內部通告，加強保護病人個人資料的保安措施，及指示職員遇有遺失載有病人個人資料的電子儲存儀器，必須立即報告。

Hospital to Take All Practicable Steps to Safeguard Patients' Personal Data

On 24 December 2008, the Commissioner published a Report in respect of an investigation into the loss of personal data of a patient (the "complainant") by a hospital as complained by the complainant.

Background

A nurse (the "Nurse") of the hospital was assigned to work in different working places and was provided with a USB flash drive (the "USB Drive") for storage of clinical notes and transmitting patients' registration data back to her office and inputting such data into the master computer file. The Nurse later found that the password protected zone of the USB Drive was defective and could not be accessed, so she copied the registration data of 26 patients (including the complainant) handled by her to the non password protected zone and continued to use the USB Drive without reporting the incident to her supervisor. Later on, the Nurse found that the USB Drive had been lost. She made vain attempts to search for the USB Drive and reported the loss to her supervisor about 3 months later. The USB Drive contained personal data (such as name, Hong Kong Identity Card number and contact telephone number) of the 26 patients.

After occurrence of the incident, the hospital had taken a series of remedial actions including, among other things, recalled all USB Drives given to nurses who offered services same as the Nurse and deleted all patients' data inside the USB Drives; passed a motion to replace USB Drive with intranet email account and facsimile for storing and transmitting patients' personal data; and issued internal circulars to enhance security measures on the protection of patients' personal data and direct staff to immediately report loss of electronic storage devices containing patients' personal data.

調查

該醫院作為公營醫療服務提供者，所處理的病人個人資料的數量十分龐大，而有關資料亦屬高敏感度。為了裁決該醫院是否違反了保障資料第4原則，沒有採取所有切實可行的步驟，以確保有關資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，私隱專員必須考慮該醫院在提供USB予其職員處理及儲存病人個人資料時，是否已採取足夠的保護措施，例如(i)是否已有合適的政策及指引通知其職員在使用USB時保護有關資料；及(ii)是否已實行措施確保其職員遵守有關政策及指引。

私隱專員的調查結果

在考慮個案的所有情況後，尤其是該醫院沒有制定任何有關使用電子儀器(例如USB)的詳細指引或應用程序，供其職員遵守；該護士沒有需要將已傳送至總電腦檔案的病人登記資料保留在該USB內；以及該護士沒有向該醫院報告該USB的密碼保護區損壞及遺失一事，私隱專員認為該醫院違反了保障資料第4原則的規定。

由於該醫院已停止使用USB儲存及傳送病人的個人資料，因此無需就調查發出執行通知。

調查引致的建議

USB的用途十分廣泛，而且方便攜帶，醫護人員在使用前應考慮是否真正有需要使用USB、是否有其他代替方法，以及小心衡量使用USB的潛在風險。如醫護人員經審慎考慮後，認為使用USB儲存病人個人資料是必須的，則須採取有效的措施，以保護個人資料免受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，例如儲存於USB的個人資料應被加密處理，並在使用後立即刪除，以及當發現遺失載有病人個人資料的USB時，應該立即向有關方面報告。

The Investigation

As a public medical service provider, the hospital handles huge amount of patients' personal data which are of sensitive nature. In order to determine whether the hospital was in contravention of DPP4 for failing to take all practicable steps to ensure that such data were protected against unauthorized or accidental access, processing, erasure or other use, the Commissioner had to consider whether sufficient safeguards had been taken when the hospital provided its staff with USB Drives for handling and storage of patients' personal data, such as whether (i) appropriate policies and guidelines were in place to inform its staff to protect such data when using USB Drives; and (ii) measures had been implemented to ensure compliance with such policies and guidelines by its staff.

The Commissioner's Findings

Having considered all the circumstances of the case, including in particular that the hospital did not have in place any detailed instructions and application procedures on the use of electronic device such as USB Drive for compliance by its staff; the Nurse had no need to keep in the USB Drive the patients' registration data which had been transmitted to the master computer file; and the Nurse had failed to report to the hospital the defect of the password protected zone of the USB Drive as well as the loss of the same, the Commissioner found that the hospital was in contravention of DPP4.

As the hospital had stopped using USB Drive to store and transmit patients' personal data, no enforcement notice was issued in consequence of the investigation.

Recommendations Arising from the Investigation

While USB Drive offers a wide range of uses and is portable, medical staff should, before using it, consider if there is any actual need to use it or there is any other substitute, and ponder the potential risk of using USB Drive. If after careful consideration, it is still necessary to use USB Drive to store patients' personal data, effective measures shall be adopted to protect the personal data against unauthorized or accidental access, processing, erasure or other use, for example, personal data stored in USB Drive should be encrypted and deleted immediately after use and USB Drive containing personal data found missing should be immediately reported to the relevant parties.

學校須依從學生有關考試評分的查閱資料要求

2009年1月19日，私隱專員發表另一份報告，公布私隱專員就一名學生投訴一所大學拒絕依從其查閱資料要求所作出的調查結果。

背景

一名學生向一間大學提出查閱資料要求，要求索取他曾修讀的四個學科的考試答案、錄音帶、作業及上述各項的有關評語。該大學回覆表示，由於當時正籍該學生的學科評級覆核申請的上訴程序期間，故該大學不能處理該查閱資料要求以提供所要求的資料，只同意向該學生提供他要求的錄影帶複本。該學生因而投訴該大學在收到其查閱資料要求後40日內沒有依從該要求。

調查

為了裁定該大學是否違反條例第19(1)條的規定，沒有依從該查閱資料要求，私隱專員必須考慮該查閱資料要求所要求的資料是否屬該學生的個人資料，及該大學在個案的情況下有否收集該學生的個人資料。此外，由於該大學聲稱根據條例第55(2)(a)(i)(D)及(ii)條獲豁免依從該查閱資料要求（即所要求的資料屬「有關程序」的標的物，該大學在有關程序下為決定授予或應否延續學術資格而考慮該等資料），私隱專員亦需要考慮該大學可否獲得第55條的豁免。

私隱專員的調查結果

毫無疑問，學生在考試中的表現評估是該學生的個人資料。私隱專員認為載於計分紙上的分數及評卷員的評語（與預先印備的項目一併考慮），以及評卷員的評閱連同有關的答題卷，屬於評卷員對該學生在考試及作業中表現的評估或評語，因此構成該學生的個人資料。

School to comply with students' data access request in relation to examination marking

On 19 January 2009, the Commissioner published another Report in respect of an investigation arising out of a complaint made by a student against a university that the university refused to comply with the student's data access request ("DAR").

Background

A student of a university made a DAR to the university requesting for copies of the examination answers, audio-tapes, coursework and related comments thereof in respect of 4 courses that he had attended. The university replied that as it was within the period of the appeal process regarding the student's request for review of course grades, the university could not look into the DAR to supply the requested data save that they were prepared to provide the student with a copy of the requested video tape. The student therefore complained that the university had failed to comply with his DAR within 40 days after receiving it.

The Investigation

In order to determine whether the university was in breach of section 19(1) of the Ordinance for failing to comply with the DAR, the Commissioner has to consider if the data requested under the DAR constitute personal data of the student and that the university had collected the student's personal data in the circumstances of the case. Moreover, as the university claimed exemption from complying with the DAR under section 55(2)(a)(i)(D) and (ii) of the Ordinance (i.e. the requested data were subject of a "relevant process" whereby such data were considered by the university for determining the awarding of academic qualification or whether any academic qualification should be continued), the Commissioner also needed to consider if section 55 exemption was available to the university.

The Commissioner's Findings

There is no doubt that evaluation of the performance of a student in an examination constitute personal data of that student. The Commissioner considered that the scores and examiners' remarks (read together with the printed items) contained in the marking sheets, and the examiners' markings together with the answer scripts, being the examiners' evaluation or comments on the student's performance in his examination and coursework, constitute the student's personal data.

至於收集個人資料方面，私隱專員認為該大學在收集載於計分紙及其他試卷/作業的該學生的個人資料時，一定已知悉該學生的身份，以及視該等資料為與該學生有關的重要資訊。故此，該大學在收集該等資料時，是在編製關於該學生的資訊。因此，該大學在考試及作業中收集了該學生的個人資料。

With regard to collection of personal data, the Commissioner found that the identity of the student was no doubt known to the university when it collected the student's personal data in the marking sheets and other examination/coursework papers. Further, such data should be regarded by the university as an important item of information relating to the student. Thus the university was compiling information about the student when collecting such data, hence there was collection of the student's personal data in the examination and coursework exercise.

私隱專員認為該大學沒有在收到該學生的查閱資料要求後40日內依從該要求，違反了條例第19(1)條的規定。在考慮到(i)該大學當時並不是為了決定是否向該學生授予或繼續給予學術資格而考慮該等資料；(ii)當該大學回覆該查閱資料要求時，該學生提出的學科評級正式覆核已經完成，而上訴程序只於其後進行；及(iii)該大學進行的上訴程序不應被視為「有關程序」，因為根據該大學的上訴程序規則，研究院院長的決定是最終的決定，而根據條例第55(2)(b)條，如在某程序中，針對該等決定提出上訴是不獲容許的，則「有關程序」不包括該等程序，因此私隱專員認為該大學在本個案中不能獲得條例第55條的豁免。

The Commissioner found that the university had contravened the requirement of section 19(1) of the Ordinance for failing to comply with the DAR made by the student within 40 days after receiving it. Taking into consideration that (i) it was found that the University was not considering the data for determining whether to give or continue to provide an academic qualification to the student at the material time; (ii) when the university replied to the DAR, the formal review of course grades requested by the student had already been completed and the appeal process only took place thereafter; and (iii) the appeal process conducted by the university should not be regarded as a "relevant process" because according to the appeal process regulations of the university, the decision of the Dean of Graduate Studies was considered final while under section 55(2)(b) of the Ordinance, "relevant process" does not include any process where no appeal may be made against such determination, the Commissioner was of the view that section 55 exemption under the Ordinance was not available to the university in this case.

調查引致的建議

考生要求查閱其載有分數及評卷員評語的試卷、作業及/或答題簿，以及要求覆核，這情況並不罕見。考試機構如有意援引條例第55條的豁免，必須小心考慮所要求查閱的資料是否真正屬於「有關程序」的標的物。

Comments arising from the Investigation

It is not uncommon that students would request access to their examination scripts; coursework and/or answer books with scores and examiners' written comments contained therein and ask for a review. Examination bodies which seek to rely on the exemption provisions in section 55 of the Ordinance must carefully consider whether the requested data are indeed the subject of a "relevant process".

另一方面，私隱專員提醒考生，如試卷、作業及/或答題簿本身沒有包含與考生個人有關的資料，它們並不構成條例下的「個人資料」，因此條例下的查閱資料要求之有關規定並不適用，考試機構不依從要求查閱該些資料不構成違反條例。

On the other hand, the Commissioner advised students that if examination scripts, coursework and/or answer books do not contain information relating to the students personally, they would not constitute "personal data" under the Ordinance and examination bodies would not be required to comply with the data access request provisions of the Ordinance in respect of such items.

報告可以在公署的辦事處（香港灣仔皇后大道東248號12樓）索取，亦可以從公署網站（http://www.pcpd.org.hk/chinese/publications/invest_report.html）下載。

Copies of the Reports are available from the PCPD at 12/F., 248 Queen's Road East, Wan Chai, Hong Kong. They are also available for download from the website of the PCPD (http://www.pcpd.org.hk/english/publications/invest_report.html).