Report Published under Section 48(2) of the

Personal Data (Privacy) Ordinance (Cap. 486)

根據《個人資料（私隱）條例》（第 486 章）第 48（2）條發表的報告

Report Number: R06-2599 **報告編號：R06-2599**

Date issued: 26 October 2006 **發表日期：2006 年 10 月 26 日**

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

聘用外判承辦商時必須
採取保安措施以保障個人資料

案件編號：200602599

本報告乃有關本人根據《個人資料(私隱)條例》（第 486 章）(下稱「條例」)第 38 條對投訴警方獨立監察委員會進行的調查，並根據條例第 VII 部行使本人獲賦予的權力而發表。條例第 48(2)條訂明「*...專員在完成一項調查後，如認爲如此行事是符合公眾利益的，可—*

(a) 發表列明以下事項的報告—

(i) 該項調查的結果；

(ii) 由該項調查引致的、專員認爲是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文(尤其是各保障資料原則)的任何建議；及

(iii) 由該項調查引致的、專員認爲適合作出的任何其他評論；及

(b) 以他認爲合適的方式發表該報告。」

吳斌
個人資料私隱專員

目錄

第一章 1

簡介 1

引言 1

事件 2

涉及人士 3

第二章 4

調查方法 4

第三章 5

管理投訴警察個案的制度 5

警監會 5

警監會秘書處 5

投訴警察課 7

處理投訴警察個案的程序 8

第四章 10

警監會的資訊科技系統 10

投訴統計數字 10

電腦統計系統的開發 11

第一次提升計劃 12

配對程式 12

第二次提升計劃 12

維修合約 12

第五章 14

保安及私隱政策 14

保安政策 14

私隱政策 14

第六章 16

引致互聯網上資料外洩的連串事件 16

引言 16

資料於 2000 年 5 月至 2003 年 5 月由警監會移轉予 EDPS 16

資料於 2003 年 5 月至 2006 年 3 月由警監會移轉予 EDPS 17

警監會及 EDPS 兩者所說的版本出現分歧 17
投訴人的個人資料在互聯網上外洩 19
其他證人 20

第七章 21
專員的調查結果 21
專員對警監會調查所得的結果 21
對事件中其他人士的評論 23
對投訴警察課的評論 23
對 EDPS 的評論 24
對 Y 先生的評論 24
對 X 女士及當時的上司的評論 25
對網站管理員的評論 26

第八章 27
警監會在資料外洩後採取的行動及專員作出的建議 27
警監會在資料外洩後採取的行動 27
執行通知 27
調查之後的建議 28
聘用外判承辦商或代理時須採取的措施 28
對資訊科技從業員的建議措施 29
對政府人員的指引 30

附件

附件 A – 警監會對於個人資料被泄之報告（二零零六年四月八日）
附件 B – 警監會第 37/98 號內部通告，標題爲「機密文件的處理」

（註：此乃中文翻譯本，一切以英文文本爲準。）

第一章

簡介

引言

1.1.1　本報告是個人資料私隱專員(下稱「專員」)依據《個人資料(私隱)條例》(第 486 章)(下稱「條例」)第 38 條就「投訴警方的公眾人士的個人資料於互聯網上外洩」一事(下稱「事件」)進行調查的結果。

1.1.2　專員決定對資料使用者展開調查後，共有 55 位投訴人向個人資料私隱專員公署（下稱「公署」）作出投訴。調查的對象是被投訴者—投訴警方獨立監察委員會(下稱「警監會」)。

1.1.3　條例附表 1 的保障資料第 4 原則與本個案有關，其內容如下：

> *「第 4 原則 – 個人資料的保安*
>
> *須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料(包括採用不能切實可行地予以查閱或處理的形式的資料)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，尤其須考慮—*
>
> *(a) 該等資料的種類及如該等事情發生便能造成的損害；*
> *(b) 儲存該等資料的地點；*
> *(c) 儲存該等資料的設備所包含(不論是藉自動化方法或其他方法)的保安措施；*
> *(d) 爲確保能查閱該等資料的人的良好操守、審慎態度及辦事能力而採取的措施；及*
> *(e) 爲確保在保安良好的情況下傳送該等資料而採取的措施。」*

事件

1.2.1　2006 年 3 月 10 日，一份本地報紙刊登了題目爲「粗心大意令二萬人私隱曝光，隨時惹禍上身」的報導。該報導透露公眾可透過網站 www.china2easy.com(下稱「該網站」)查閱一個看來是警監會的資料庫，內裏載有投訴警察課的投訴資料，包括投訴人的姓名、地址及身份證號碼。當日在該報接觸該網站的註冊經營者之後，有關資料已從網站移除。

1.2.2　專員在收到正式投訴前，已決定採取即時行動。2006 年 3 月 10 日，即該報導刊登當日，公署迅即向警監會作出書面查詢。2006 年 3 月 11 日，專員聯絡警監會主席，取得一些初步資料，並安排與警監會的高層會面。2006 年 3 月 13 日，專員與警監會主席及一名副主席會面。同日，專員亦率領公署的高級人員與警監會的高層會面。2006 年 3 月 15 日，專員根據條例第 38(b)條展開正式調查。

1.2.3　警監會於 2006 年 4 月 8 日就事件發表報告。該報告的副本見附件 A。與此同時，專員收到多名受事件影響的人士投訴。公署在核實投訴人的身份，並信納其個人資料在互聯網上外洩後，便根據條例第 38(a)條對投訴進行調查。

1.2.4　下表列出截至撰寫本報告時公署接獲的投訴數目：

日期	接獲的投訴數目
2006 年 3 月 13 日 – 2006 年 3 月 19 日	9
2006 年 3 月 20 日 – 2006 年 3 月 26 日	3
2006 年 3 月 27 日 – 2006 年 4 月 2 日	7
2006 年 4 月 3 日 – 2006 年 4 月 9 日	2
2006 年 4 月 10 日 – 2006 年 4 月 16 日	6
2006 年 4 月 17 日 – 2006 年 4 月 23 日	2
2006 年 4 月 24 日 – 2006 年 4 月 30 日	2
2006 年 5 月 1 日 – 2006 年 5 月 7 日	2
2006 年 5 月 8 日 – 2006 年 5 月 14 日	6
2006 年 5 月 15 日 – 2006 年 5 月 21 日	6
2006 年 5 月 22 日 – 2006 年 5 月 28 日	5
2006 年 5 月 29 日 – 2006 年 9 月 18 日	5
總數：	55

涉及人士

1.3.1　被投訴違反條例規定的一方是警監會。

1.3.2　在調查過程中，專員發現事件涉及其他人士。儘管他們並非被投訴的一方，但專員認爲就有關個人資料評論他們的角色及行爲是恰當的。

1.3.3　這些人士包括：

(i)　投訴警察課，
(ii)　警監會資訊科技承辦商 EDPS Systems Ltd. (下稱「EDPS」)，
(iii)　EDPS 分判商 Y 先生，
(iv)　警監會人員 X 女士，
(v)　X 女士當時的上司(下稱「當時的上司」)，以及
(vi)　負責該網站的網站管理員(下稱「網站管理員」)。

第二章

調查方法

2.1 調查方法包括到訪警監會辦事處、到訪投訴警察課、會見有關人員、審查涉及人士持有的文件記錄和作出的書面陳述，以及會見由專員根據條例第 44 條傳召的有關人士。

2.2 公署人員於 2006 年 3 月 13 日及 2006 年 4 月 24 日到訪警監會辦事處。警監會於 2006 年 3 月 13 日、2006 年 3 月 14 日、2006 年 4 月 8 日、2006 年 4 月 27 日、2006 年 4 月 29 日、2006 年 5 月 2 日、2006 年 5 月 11 日及 2006 年 5 月 20 日提交書面陳述，以回應公署的查詢。公署人員亦於 2006 年 4 月 24 日到訪投訴警察課，並於 2006 年 5 月 8 日及 2006 年 5 月 11 日取得其書面陳述。同時，EDPS 於 2006 年 3 月 22 日、2006 年 4 月 4 日、2006 年 4 月 11 日及 2006 年 5 月 16 日向公署提交書面陳述。

2.3 此外，專員及/或其人員曾會見或以傳召的方式訊問下列人士：

(i) 警監會主席，
(ii) 警監會副主席，
(iii) 警監會秘書長，
(iv) 警監會副秘書長，
(v) 當時的上司，
(vi) X 女士，
(vii) 兩名警監會辦公室助理員，
(viii) EDPS 總裁，
(ix) EDPS 總經理，
(x) Y 先生，
(xi) Y 先生的業務夥伴(下稱「Y 先生的夥伴」)，
(xii) 網站管理員，
(xiii) 投訴警察課前統計主任，以及
(xiv) 警察資訊系統部資訊科技主任(下稱「警方程序編製主任」)。

第三章

管理投訴警察個案的制度

警監會

3.1.1　警監會源自行政立法兩局非官守議員警方投訴事宜常務小組。1986年，當時的總督把常務小組改組爲一個非法定但獨立的投訴警方事宜監察委員會。1994 年 12 月 30 日，投訴警方事宜監察委員會改稱爲投訴警方獨立監察委員會(警監會)。警監會現時的成員包括由行政長官委任的一名主席、三名副主席和 14 名委員。

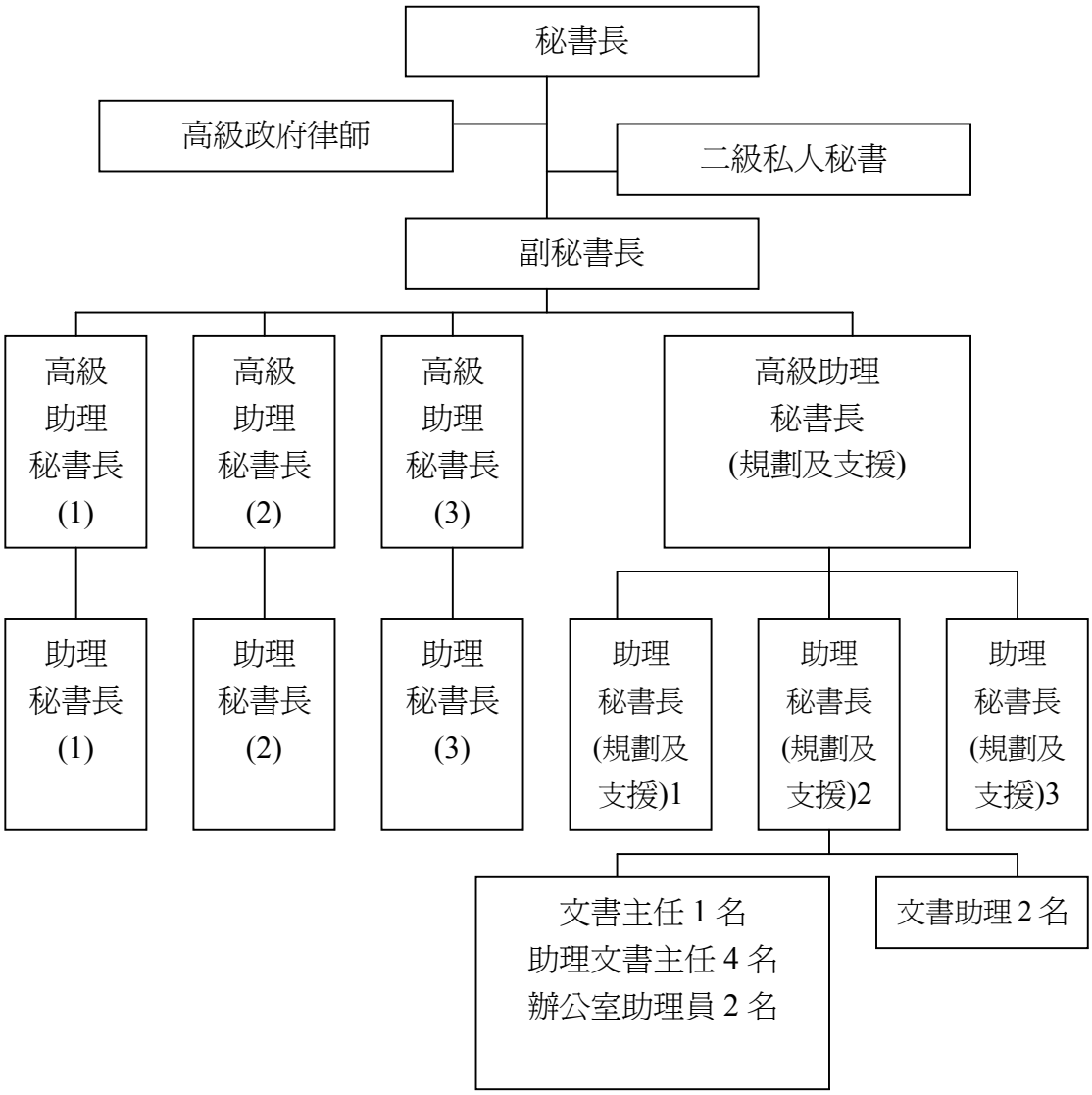
3.1.2　警監會的主要職能，是監察和覆檢投訴警察課就市民投訴警察個案而進行的調查工作。警監會的職權範圍如下：

(i)　監察警方處理市民投訴的方法，並於適當時加以覆檢；
(ii)　經常覆檢導致市民投訴警務人員的各類行爲的統計數字；
(iii)　覆檢警方的工作程序，找出引起投訴或可能引起投訴的不當之處；以及
(iv)　於適當時，向警務處處長，或在有需要時向行政長官提出建議。

警監會秘書處

3.2.1　警監會設有由公務員組成的全職秘書處(下稱「警監會秘書處」)，由一名首長級丙級政務官擔任秘書長，其下有 21 名一般職系人員和一名擔任警監會法律顧問的高級政府律師。警監會秘書處的主要職責，是仔細審閱投訴警察課提交的所有投訴調查報告，確保每宗個案都經過徹底而公正的調查，然後才向警監會委員建議通過報告。在秘書長和副秘書長(總行政主任)監察下，有三組人員專責審核投訴的調查工作。每組均有高級助理秘書長和助理秘書長各一名，分別屬高級行政主任和一級行政主任職級。第四組，即規劃及支援組，由一名高級助理秘書長和 12 名行政、文書和秘書職系人員組成，負責一般行政、研究、宣傳和其他支援服務，以及爲嚴重投訴個案委員會提供支援服務。

3.2.2　警監會秘書處的組織架構如下：

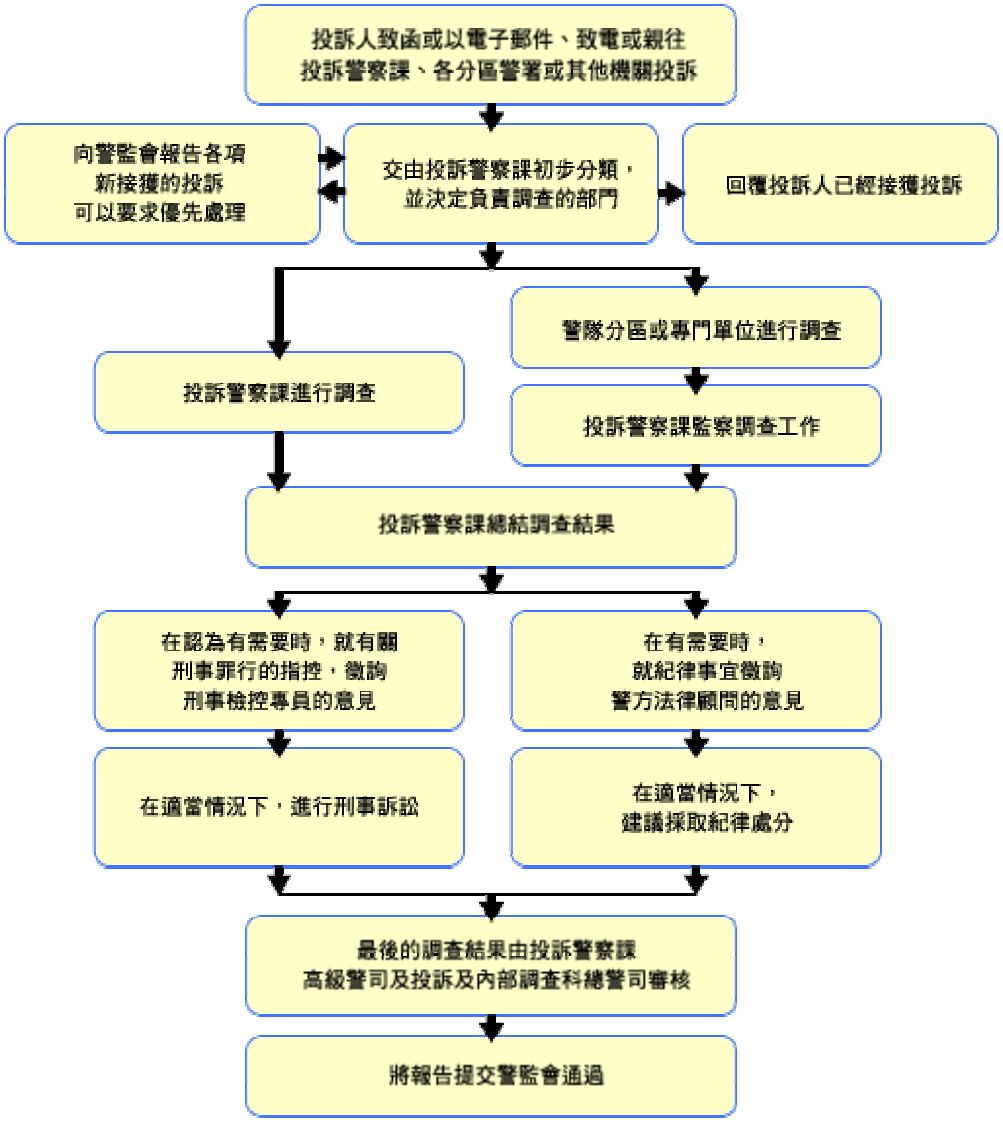


3.2.3　警監會委員可以就有關履行其職能及職責的事宜，向警監會秘書處發出指示或命令。警監會秘書處會執行有關指示或命令，只要有關指示或命令沒有違反公務員的規則或規例。但警監會委員無權決定警監會秘書處人事上的事宜，包括終止職員的聘任。除非是重要事宜或警監會委員要求，否則警監會秘書處是不會向警監會委員匯報其日常運作事宜。

投訴警察課

3.3.1　投訴警察課隸屬警務處投訴及內部調查科，向警務處處長負責，確保所有對警務人員或隸屬警隊的文職人員作出的行爲不檢投訴或刑事指控，均獲全面和公正的調查。不論來源，所有投訴都交由投訴警察課調查。完成調查後，投訴警察課會編寫報告，詳述所進行的調查及其結果，並提交警監會批簽通過。警監會專責監察所有投訴，確保所有投訴均獲得徹底及公正的調查。

3.3.2　以下的流程圖列出投訴警察課審核和調查投訴的程序。完成調查後，投訴警察課會按調查結果把投訴分類，並擬備報告提交警監會覆檢和通過。



處理投訴警察個案的程序

3.4.1　投訴警察課會把所有調查報告，連同有關的個案或罪案調查檔案提交警監會。警監會秘書處的行政主任會詳細審閱這些報告，並在有需要時向內部的高級政府律師徵詢法律意見。

3.4.2　投訴警察課的所有調查報告，包括回覆投訴人函件的擬稿，都會於警監會秘書長主持的每周個案會議上詳細討論。

3.4.3　會議之後，警監會秘書處會以書面向投訴警察課提出意見和查詢(如有的話)。在適當情況下，警監會秘書處也會促請該課注意警方的現行政策、工作程序或慣常做法的不足之處，並建議補救措施。

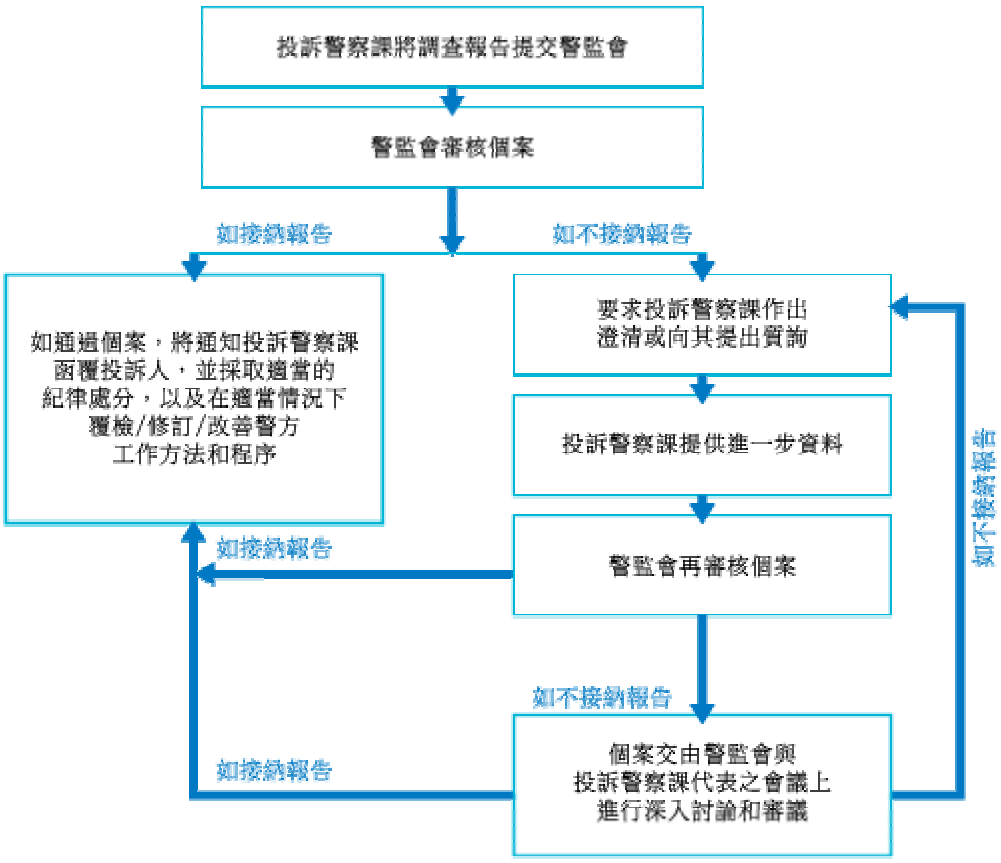
3.4.4　警監會秘書處會仔細審核投訴警察課的答覆，然後才擬備個案總結報告提交警監會委員審議。已審閱的個案會每星期分批呈交委員審議。

3.4.5　警監會委員分爲三組，分擔審議工作。每組均有一名副主席和五名委員。每宗個案均由有關組別的副主席及委員審議，而主席則審議所有嚴重個案，以及任何由警監會秘書長及/或副主席或委員轉介給他的個案。

3.4.6　遇有非常嚴重及複雜的個案，監察過程可能涉及成立特別覆檢小組、由警監會委員接見證人，以及徵詢醫學及/或法律意見。如有需要，警監會可能要求投訴警察課重新調查有關個案。

3.4.7　大部分個案是透過傳閱方式處理。至於涉及政策，或不能透過警監會秘書處與投訴警察課之間的文書往來解決的複雜個案，便會交由警監會/投訴警察課聯席會議處理。聯席會議的主席由警監會主席擔任。

3.4.8　下圖說明警監會如何監察投訴警察課完成對投訴警察個案的調查：



第四章

警監會的資訊科技系統

投訴統計數字

4.1.1　為了經常覆檢導致或可能導致市民投訴警務人員的各類行為的統計數字，警監會必須保持投訴統計數字，以供年度審核及內部進行有關投訴警察個案的研究之用。

4.1.2　在程序方面，警監會得到投訴統計數字的過程如下：警監會批簽通過投訴個案後，警監會的案件主任會根據投訴警察課報告檔案內的資料，為每個檔案編碼。編碼要考慮的因素包括指稱的性質、指稱的分類、事件的狀況、投訴人及被投訴者的詳細資料。要有效地收集分析投訴資料所需的統計數字，編碼的過程是必須的。在編碼之後，警監會的職員便會把資料輸入警監會的電腦統計系統。

4.1.3　投訴警察課擁有的電腦系統名為「投訴索引及統計系統」，負責管理投訴的統計數字。雖然投訴警察課與警監會是使用相同的代碼表，但統計結果有時會不同，因為兩者是各自編碼的。警監會與投訴警察課的人員可能會對同一個個案編配不同的代碼。因此，投訴警察課和警監會在採用投訴資料作內部用途(包括內部研究)或公開發放前，必須互相核對資料有沒有分歧。

4.1.4　由於警監會與投訴警察課分別保持兩個統計系統，因此警監會在 2000 年一個聯席會議中，曾詢問可否在警監會設立電腦終端機，直接連接投訴警察課的投訴索引及統計系統。雙方的電腦最終沒有直接連接，但投訴警察課會定期以電腦碟向警監會提供過去五年投訴索引及統計系統的摘錄資料。

4.1.5　根據安排，投訴警察課會定期以電腦碟向警監會提供投訴警察個案的統計資料(連同個別個案的詳細資料)，以供核實。警監會的電腦會擬備錯配代碼的報告。警監會會覆檢錯配資料，然後與投訴警察課作出修正。經修正的資料會併入警監會的電腦統計系統。

電腦統計系統的開發

4.2.1 1998 年，警監會以電腦統計系統管理所有投訴個案的數據及資料。爲了更妥善有效地管理資料，警監會有意開發一個新的系統。

4.2.2 新系統預計由 1999 年 1 月 1 日起在一部獨立的個人電腦中運作，並應該：

(i) 可以利用標準代碼建立、儲存及更新投訴記錄；
(ii) 可以增加、刪除及變更標準代碼；
(iii) 可以對投訴個案記錄進行搜尋/編輯/分類及統計查詢；
(iv) 可以列印統計報告；
(v) 具有保安措施，例如登入密碼；
(vi) 能夠進一步提升；
(vii) 符合 2000 年的系統要求；以及
(viii) 容易使用。

4.2.3 獲揀選開發電腦統計系統的承辦商須：

(i) 提供所需的程式設計服務；
(ii) 安裝及測試系統；
(iii) 製定能順利操作系統的電腦環境；
(iv) 爲使用者提供足夠的培訓；
(v) 爲警監會提供該系統的使用手冊；
(vi) 建議所需的硬件及軟件平台；
(vii) 將舊資料轉換，並由當時的資料庫(FoxBase+資料庫格式)輸入新的資料庫；
(viii) 提供約六個月的保證期；以及
(ix) 如有需要，按雙方同意的費用提供維修服務。

4.2.4 警監會邀請了六個承辦商報價，最後揀選了 EDPS 提供服務。警監會於 1998 年 12 月 24 日與 EDPS 正式簽約。

4.2.5 根據合約條款，EDPS 同意向警監會提供資料轉換程式，盡量將資料由舊系統轉換至新系統。EDPS 亦會爲警監會擬備使用手冊，作爲參考指引。最後，在應用軟件成功安裝並由警監會接受後，EDPS 會提供維修服務。

第一次提升計劃

4.3 自 1999 年 8 月起，警監會再聘任 EDPS 提升其電腦統計系統。1999 年進行的提升項目是爲系統加入特別列印及搜尋功能；2000 年則增加更多的資料欄位及列印功能。

配對程式

4.4 大約在 2001 年 4 月，警監會及投訴警察課用以儲存投訴統計數字的電腦系統在專門用語及分類方面出現輕微差異，需要花費相當多的時間進行修正。因此警監會決定開發新的電腦程式，以便更快捷地核實兩套統計資料。2001 年 5 月，EDPS 受聘開發一個電腦程式，以監察及核實投訴統計數字(下稱「配對程式」)。

第二次提升計劃

4.5 2003 年 5 月，由於投訴警察課的投訴索引及統計系統進行提升，加進新的代碼及修改當時的代碼，因此警監會必須修改其系統，以便投訴警察課的資料能夠轉換至警監會的系統，並可在系統內檢索。EDPS 於 2004 年 1 月再次受聘進行這個提升計劃(下稱「提升計劃」)。

維修合約

4.6.1 警監會亦聘任 EDPS 爲其電腦統計系統進行維修。警監會於 1999 年 11 月首次聘任 EDPS 負責維修其電腦系統，合約是每年續期的，而最後一份合約是在 2005 年 10 月簽訂(這些合約在本報告內統稱「維修合約」)。

4.6.2 上述所有合約並沒有一般的保密條款，亦沒有要求 EDPS 採取任何措施，保障他們所收到的機密資料或保障這些資料的用途。合約也沒有任何條款禁止 EDPS 把合約中的服務分判。

4.6.3 在有關時間內，EDPS 打算把所有從警監會承包的維修及提升工作分判給 Y 先生。1998 年，EDPS 就電腦統計系統的開發事宜在警監會辦事處首次與警監會職員會面，EDPS 總經理向警監會職員介紹 Y 先生爲項目經理。警監會職員收到一張 EDPS 的名片，上面印有 Y 先生的姓名及「項目經理」的職銜 (名片副本見附件 A 警監會報告內的附錄 V)。警監會並不知道 EDPS 與 Y 先生之間的分判關係。對於警監會而言，Y 先生是 EDPS 的僱員。

警監會及其職員自那時開始與 Y 先生接觸，但不知道他與 EDPS 之間存在分判關係。

第五章

保安及私隱政策

保安政策

5.1.1　警監會及投訴警察課是按香港特別行政區規例第 5 卷的保安規例(下稱「保安規例」)運作。保安規例規定，機密資料是按機密程度而分爲「絕對機密」、「高度機密」、「機密」和「限閱文件」。保安規例採取「有需要知道」的原則，只有符合業務有效運作的需要及獲授權的人士，才可接觸機密資料。這項原則必須應用於政府內部及政府以外的人士。

5.1.2　除了政府的保安規例之外，警監會於 1998 年向其員工發出標題爲「部門保安指示」的第 33/98 號內部通告(下稱「保安通告」)。保安通告的副本見附件 A 警監會報告內的附錄 IV。警監會每六個月便會向員工傳閱保安通告，希望藉此提醒員工在處理機密文件時依從通告所述的指引。保安通告的首段提醒警監會職員，警監會處理的檔案及調查報告性質敏感，這些文件及資料必須妥善保護，免受未獲准許的披露。

5.1.3　另一份標題爲「機密文件的處理」的第 37/98 號內部通告提醒警監會員工，所有用來記錄機密資料的物品，包括電腦碟必須視作機密文件。該內部通告的副本見本報告附件 B。除此之外，警監會並無就處理電腦碟或以電子方式傳遞資料的事宜，向員工發出具體的書面程序或指引。

5.1.4　投訴警察課把所有檔案列爲「限閱文件」。警監會認爲保安規例、保安通告及第 37/98 號內部通告所述的保安級別，同樣適用於投訴警察課提供的電腦碟所載的投訴資料。

私隱政策

5.2.1　除了上述的保安通告及第 37/98 號內部通告提供處理機密資料的一般指引外，警監會本身並沒有制定私隱政策，訂明警監會持有的個人資料類別、個人資料的使用目的、個人資料的保存期間、處理查閱及改正個人資料要求的指定職員等。

5.2.2　警監會表示，實際上，擔任當時的上司所持職位的職員是負責監督整體人員遵從條例的規定。警監會正積極研究制定政策文件的需要，全面列明保障個人資料私隱的措施，讓員工及公眾知悉。

第六章

引致互聯網上資料外洩的連串事件

引言

6.1.1　在調查過程中，專員及其人員廣泛地審核了涉及事件的各方所持有的文件，並會見了多名證人。

6.1.2　本章載述專員及其人員取得的主要資料。

資料於 2000 年 5 月至 2003 年 5 月由警監會移轉予 EDPS

6.2.1　投訴警察課於 2000 年開始向警監會提供載有投訴索引及統計系統真實資料的電腦碟。在或大約在 2000 年 5 月，警監會要求 Y 先生(他們相信是其資訊科技承辦商 EDPS 的僱員)讀取投訴警察課提供的電腦碟內的資料，但 Y 先生遇到困難。Y 先生於是建議警監會向投訴警察課索取另一張加入「分隔」 (有特別記號把不同欄位的資料分隔開來)的電腦碟。警監會的 X 女士於 2000 年 6 月 12 日向副秘書長及當時的上司報告：承辦商在讀取投訴警察課提供的電腦碟後向她表示讀取資料頗爲困難，因爲欄位沒有清楚分隔。2000 年 6 月 12 日警監會的檔案錄事可以爲證。按照 Y 先生的建議，警監會於 2000 年 6 月 26 日以書面要求投訴警察課另外提供一張加上欄位分隔的電腦碟。

6.2.2　在或大約在 2001 年 5 月，Y 先生曾就配對程式建議警監會要求投訴警察課提供最新的資料庫，以便進行資料轉換程序。X 女士於 2001 年 5 月 24 日擬備的書面記錄可以爲證。依據該建議，警監會於 2001 年 5 月 25 日致函投訴警察課，要求索取載有投訴索引及統計系統最新資料的電腦碟。在或大約在 2001 年 6 月，投訴警察課向警監會提供載有真實投訴資料的電腦碟。警監會於同日把該碟交給 Y 先生。X 女士於 2001 年 6 月 12 日擬備的書面記錄可以爲證。X 女士於 2001 年 6 月 19 日向副秘書長及當時的上司報告：投訴警察課提供的資料已由 Y 先生成功讀取。X 女士於 2001 年 6 月 19 日擬備的書面記錄可以爲證。

6.2.3　自 2001 年 5 月起開發配對程式以來，Y 先生曾以「假」資料進行測試。此事記錄於 2001 年 11 月 23 日的警監會高級職員會議記錄中。在完成以「假」資料進行的測試後，Y 先生在 2001 年底至 2002 年初期間，以真實資料再進行測試。此事記錄於 2002 年 1 月 18 日的警監會高級職員會議記錄中。

資料於 2003 年 5 月至 2006 年 3 月由警監會移轉予 EDPS

6.3.1　2003 年 5 月，投訴警察課開始提升其投訴索引及統計系統。X 女士因爲無法在警監會的電腦系統讀取投訴警察課提供的電腦碟內的資料，於是向 Y 先生求助。

6.3.2　Y 先生告知她，問題與投訴警察課的系統格式及編碼有關。X 女士於是安排 Y 先生聯絡投訴警察課的統計員。由於該統計員是資訊科技的門外漢，因此要求警方程序編製主任直接致電 Y 先生，協助解決問題。此事記錄於 2003 年 9 月 19 日的警監會高級職員會議記錄中。

6.3.3　Y 先生以電話聯絡警方程序編製主任超過一次。他要求警方程序編製主任把「不固定長度格式」轉換爲原來的「固定長度格式」，令警監會的系統可以讀取投訴警察課的資料。警方程序編製主任按要求辦妥。

6.3.4　在電話談話中，兩位資訊科技人員並沒有討論過測試環境及測試資料的問題。據警方程序編製主任所述，他只是闡述電腦程式中「不固定長度格式」和「固定長度格式」的分別。他本人從來沒有存取過投訴警察課的真實資料，該等資料是受權限及密碼保護的。

6.3.5　爲了解決問題及讓警監會的人員順利讀取資料，警監會把投訴索引及統計系統的最新真實資料交予 Y 先生作分析。此事記錄於 2003 年 11 月 14 日的警監會高級職員會議記錄中。

警監會及 EDPS 兩者所說的版本出現分歧

6.4.1　是次調查的關鍵是 X 女士及 Y 先生兩者所說的版本出現分歧。首先是 X 女士有否清楚告知 Y 先生，交給他的電腦碟內的資料是真實的機密資料；其次是 Y 先生是否知道資料的機密性質；第三是 Y 先生或 EDPS 有沒有明確要求警監會提供「測試資料」，以便讓警監會讀取投訴警察課提供的真實資料。

6.4.2　警監會 2001 年 4 月開發的配對程式、2003 年 5 月的第二次提升計劃，以及與 EDPS 每年簽訂的維修合約，X 女士都有參與。她堅稱並不知道 Y 先生是以 EDPS 的分判商身份提供服務。

6.4.3　X 女士記不起向 Y 先生提供電腦碟的次數和電腦碟的數目，但她肯定 Y 先生是清楚知道電腦碟內的資料性質。

6.4.4　EDPS 表示索取「測試資料」是口頭上的要求，而載有資料的電腦碟是放於警監會的接待處，待 EDPS 的職員拿取。電腦碟並無保護裝置或警告字眼，EDPS 的職員亦無須簽收或承諾小心處理該等資料。

6.4.5　X 女士記得，有一次 Y 先生要求她向投訴警察課索取一張各欄位之間有「分隔」、載有最新資料的電腦碟。因此，X 女士聲稱 Y 先生應該知道碟內所載的資料是投訴警察課的真實資料。

6.4.6　X 女士表示，她替 Y 先生安排的各項事情都有向上司報告。警監會持有的書面記錄至少可以證明以下事項：

6.4.6.1　在或大約在 2000 年 6 月，Y 先生要求投訴警察課提供載有資料的電腦碟，而該要求於 2000 年 6 月 26 日轉達投訴警察課；

6.4.6.2　在或大約在 2001 年 5 月，Y 先生要求索取投訴警察課最新的資料庫，以便進行資料轉換程序；

6.4.6.3　經 Y 先生要求，Y 先生在或大約在 2001 年 6 月收到一張載有真實資料的電腦碟，而資料其後由 Y 先生成功讀取；

6.4.6.4　在開發配對程式時，Y 先生以「假」資料進行測試。Y 先生在 2001 年底至 2002 年初期間，再以真實資料進行測試；

6.4.6.5　在或大約在 2003 年 9 月，Y 先生與投訴警察課，以及其後的警方程序編製主任直接商討投訴警察課向警監會提供的電腦碟內的資料格式；以及

6.4.6.6　在或大約在 2003 年 11 月，投訴索引及統計系統的最新真實資料被交予 Y 先生作分析。

6.4.7　Y 先生表示，他是在 2001 年開發配對程式期間首次注意到警監會處理的資料是與投訴警務人員有關。雖然他並不確切知道資料的內容，但是他注意到資料包含了個人資料，包括姓名、日期、年齡、地址等。

6.4.8　Y 先生聲稱他在 2001 年從警監會得到一張電腦碟。當 X 女士以電話通知 Y 先生該碟已備妥待領後，他便前往警監會。他表示，X 女士並無告訴他碟內所載的是甚麼資料。據他理解，該碟載有用作測試配對程式的資料。該碟並非由 X 女士直接交給他，而是由一名警監會職員在接待處交給他。該碟是放於一個政府信封內，封面沒有註明「機密」或「限閱文件」。

6.4.9　EDPS 在其書面陳述中表示：

> *「開發及測試過程是需要建立測試環境，並要求警監會提供測試資料。顧名思義，測試環境並不一定要完全沒有程式的錯誤或保安的缺陷。因此，測試資料通常是由電腦生成的「假資料」或「經處理」的資料。」*

6.4.10　EDPS 堅稱，他們對警監會提供的資料的機密性質並不知情。

6.4.11　有關「測試資料」的問題，以及 Y 先生是否知道警監會提供的電腦碟載有真實資料，而不是「假」資料的問題，將於本報告第七章進一步討論。

投訴人的個人資料在互聯網上外洩

6.5.1　根據 Y 先生所述，從 X 女士那裏取得的「測試資料」是儲存於他的筆記簿電腦及家中的電腦。在完成第二次提升計劃的測試之後，Y 先生於 2004 年初把程式安裝到警監會辦事處的電腦統計系統內。2004 年初的安裝完成之後，Y 先生把整個完成的源程序及所有資料，包括他用以開發警監會第二次提升計劃的「測試資料」，上載到一間名爲 China Motif Limited 的公司的伺服器內，該伺服器亦是該網站的主機。

6.5.2　該網站是由 Y 先生及 Y 先生的夥伴成立，目的是用作在香港出售來自中國的商品。該網站是以網站管理員的姓名註冊的。

6.5.3　網站管理員表示，Y 先生是他的舊同事，其後自組公司，並把一些兼職工作判給網站管理員。網站管理員爲 Y 先生設計及維修該網站。Y 先生獲准及能夠獨立地把資訊或資料上載到該網站的伺服器內。

6.5.4　根據網站管理員所述，警監會的資料外洩是由 Y 先生造成的，因爲 Y 先生把警監會的機密資料上載到伺服器一個其他人能夠進入的位置。Y 先生可能不知道把資料上載到伺服器的不同位置會有不同後果。Y 先生從來沒有詢問網站管理員哪個伺服器位置或子目錄可能會被其他人經互聯網進入，網站管理員亦沒有告知 Y 先生。

6.5.5　2006 年 3 月 10 日，一名公眾人士在互聯網進行搜尋，經該網站發現一些投訴人的姓名、地址及身份證號碼，警監會的資料於是曝光。

6.5.6　EDPS 就技術上的問題之立場如下：

> *「儘管測試資料是存儲於私人的伺服器、只作測試及內部用途、由用戶名稱及密碼保護，以及只限少數技術人員存取，正如我們現在所知，測試資料的存儲保障已被各種系統工具、搜尋器及互聯網所損壞。這個問題是技術性的，完全只限於測試環境。如果那些資料真的是測試資料，這問題其實是很容易補救，而不會有嚴重後果。」*

其他證人

當時的上司

6.6.1　當時的上司是 X 女士的直屬上司。他聲稱只知道警監會資訊科技程式的一些基本事項，但不知道詳情。在開發資訊科技程式的過程中，當時的上司並沒有收到上級的指示要向 EDPS 提供協助，而 X 女士亦無在這方面諮詢他。

Y 先生的夥伴

6.6.2　Y 先生的夥伴知道 Y 先生替警監會做了一些持續的維修工作，但 Y 先生沒有提及工作的詳情。Y 先生的夥伴並不知道 Y 先生把警監會的資料庫上載到該網站的伺服器內。

第七章

專員的調查結果

專員對警監會調查所得的結果

7.1.1　本報告第 1.1.3 段提及的保障資料第 4 原則，要求資料使用者對其持有的個人資料採取保障及預防措施。保安級別應反映資料的敏感程度及違反保安規定可引致的損害程度。

7.1.2　本個案涉及資料使用者(警監會)，把電腦資料庫系統的開發、提升及維修外判給承辦商(EDPS)，而承辦商在資料使用者(警監會)不知情的情況下，再把有關工作分給分判商(Y 先生)。一般預期承辦商(EDPS)會查看有關資料，並在將製成品交給資料使用者(警監會)之前以資料測試系統。

7.1.3　爲了進行外判的工作，Y 先生要求警監會提供有關資料。根據本人所得的證據，本人並不認爲警監會曾作出適當考慮，確保資料安全。

7.1.4　警監會在發給員工的保安通告中列明:「*鑑於警監會秘書處處理的投訴警察課個案檔案及調查報告數量龐大，性質敏感，這些文件/資料必須妥善保護，免受未獲准許的披露。*」警監會是清楚知道他們處理的資料是極爲敏感。資料外洩不單令受影響的人士嚴重焦慮，而且令他們極度擔心其人身安全。如果資料落入壞人手中，可能會被用於欺詐活動，例如冒充有關人士向財務機構申請信貸。由於資料極爲敏感，資料外洩引致的損害甚爲嚴重，因此警監會無論在甚麼情況下都應該小心謹慎，採取足夠的保障措施保護資料，尤其是要向第三者(例如事件中的承辦商)發放資料時。

7.1.5　EDPS 與警監會的合約關係可追溯至 1998 年。由於警監會是清楚知道外判給 EDPS 的工作性質及範圍，他們應該知道承辦商是需要資料進行系統測試的。從 X 女士於 2000 年 6 月 12 日、2001 年 6 月 12 日及 2001 年 6 月 19 日擬備的書面記錄副本及 2002 年 1 月 18 日的警監會高級職員會議記錄來看，很明顯警監會是清楚知道向 Y 先生發放的是投訴警察課個案的真實資料。

7.1.6　作爲負責人的 X 女士及/或其上司均沒有考慮他們應該向 Y 先生發放真實資料抑或「假」資料。X 女士看來是假定要向承辦商發放真實資料，所以沒有詢問 Y 先生使用「假」資料的可行性。在調查中，EDPS 及 Y 先生在回應本人的查問時，均表示他們並不需要以警監會的真實資料來測試程式。自從資料外洩之後，警監會亦同意當時是可以使用「假」資料測試 EDPS 負責的程式或提升的系統。如果警監會當時充分地考慮使用「假」資料，這次事件相信得以避免。

7.1.7　鑑於有關資料性質敏感，真實資料無須離開警監會的處所是最爲理想。不過，本人看不到任何證據顯示在向 Y 先生發放資料之前，X 女士或警監會的任何人士曾與他商討或考慮可否在警監會的處所內進行需使用真實資料的工作。

7.1.8　當時的上司聲稱，無人獲得准許把投訴警察課的機密資料帶離警監會辦事處，而 X 女士在閱讀保安通告之後應該明白這點。X 女士確認她曾閱讀保安通告，但她並不覺得通告的內容禁止她向承辦商發放真實資料。本人閱讀過保安通告後，同意她的看法。若按當時的上司所聲稱，警監會的政策是禁止任何人把投訴警察課的資料帶離辦事處，但本人卻看不到任何實質證據顯示警監會曾在這方面給予員工清晰的指示。

7.1.9　承辦商在某階段需要以個人資料作系統測試，是合理地預計得到的。但警監會並無發出任何實務指引，列明員工在承辦商要求索取個人資料時需要考慮的事宜。警監會亦無發出指引，提醒員工有關敏感資料離開警監會辦事處及其監控範圍所涉及的私隱風險。

7.1.10　本人同意，因應工作的複雜性及其他考慮(例如有關測試所要求的準確程度)，外判承辦商在開發及維修電腦資料庫系統時，可能需要使用真實資料。在這些情況下，可能需要把真實資料交給承辦商在資料使用者的處所以外的地方處理。在發放資料之前，資料使用者必須採取所有切實可行的預防措施，防止承辦商外洩資料。可是沒有證據顯示警監會曾採取切實可行的預防措施，防止 EDPS 或 Y 先生外洩資料。

7.1.11　在涉及外判承辦商處理個人資料的服務合約中，應該有條款規定承辦商有責任保障個人資料的安全，並爲資料保密。本人在警監會與 EDPS 簽訂的服務合約中找不到這樣的條款，亦找不到條款規定 EDPS 必須採取保安措施，保障警監會交託給他們的敏感個人資料。

7.1.12　保障資料第 4 原則規定，資料使用者必須採取措施，確保能查閱由他持有的個人資料之人士的良好操守、審慎態度及辦事能力。現有資料顯示，警監會的投訴資料外洩是 Y 先生的某作爲導致的。不論警監會在揀選 EDPS 爲其承辦商時是否盡了應盡的努力，警監會沒有在 EDPS 的服務合約中加入條款，禁止 EDPS 把服務分判，此舉做成危險，可能會導致敏感資料被發給操守、態度及辦事能力不爲警監會認識、行爲不受警監會監管的人士。

7.1.13　經考慮上述所有情況後，本人認爲警監會把投訴警察課提供的個人資料發放給 Y 先生之前，首先沒有考慮過是否必需這樣做。有關資料的性質高度敏感，但警監會向 Y 先生發放資料時，卻沒有採取任何預防措施(不論是否在合約上作出的)，保障資料免受未獲准許或意外的查閱。此外，警監會在事件中並無採取任何切實可行的步驟，確保可以查閱該等資料的人士的良好操守、審慎態度及辦事能力。

7.1.14　綜觀以上所述，本人認爲警監會違反保障資料第 4 原則的規定。

對事件中其他人士的評論

7.2.　事件中，個人資料在互聯網上外洩是因爲 Y 先生把資料上載到該網站的主機伺服器。如果警監會在處理外判事宜時曾充分地遵從保障資料第 4 原則的規定，資料外洩可能得以避免。事件中亦涉及其他人士，公眾會期望本人也就有關個人資料評論他們及 Y 先生的角色及行爲。

對投訴警察課的評論

7.3.1　鑑於警監會的監察角色，投訴警察課是有責任向警監會提供投訴資料的。本人亦知道，爲了讓警監會有效地進行研究及擬備統計數字，警監會是需要以電子形式從投訴警察課取得全面的投訴資料。不過，爲了減低資料外洩及被濫用的風險，投訴警察課發放的電子資料應該只限於進行研究及擬備統計數字所需。

7.3.2　如果警監會及投訴警察課曾就資料的使用目的，檢討投訴警察課向警監會提供的資料類別，應該會是明智之舉。本人建議投訴警察課及警監會考慮(要是他們未有這樣做的話)，若是作研究或統計用途，投訴警察課是否需要把個別人士的識辨資料，如身份證號碼、警務人員編號、全名及詳細地址移轉予警監會。

對 EDPS 的評論

7.4.1 EDPS 確認其代表首次與 Y 先生到警監會辦事處爭取首份服務合約時，他們向警監會的職員提供了一張 EDPS 的名片，上面印有 Y 先生的姓名及「項目經理」的職銜。在這個場合中，EDPS 及 Y 先生都沒有告訴警監會，如果他們獲得工作，EDPS 只是承辦商，而 Y 先生則是負責實際工作的分判商。在那次會面中及其後的時間，EDPS 及 Y 先生可能是有意或無意令警監會認爲，交予 EDPS 的工作會由 Y 先生作爲 EDPS 的僱員承擔，以及有關工作只是由 EDPS 負責處理。雖然警監會並無禁止 EDPS 把警監會的合約分判給第三者，若 EDPS 一開始便清楚表明 Y 先生是其屬意的分判商，或是在獲得工作後把分判安排通知警監會，這會是良好的行事方式。從資料的保安方面來說，如果警監會知道有關項目是由分判商來進行，警監會可能會對由分判商處理敏感個人資料的保安問題作出適當考慮。

7.4.2 EDPS 聲稱他們只是向警監會要求「測試資料」，而 EDPS 不可能創造資料作測試項目之用。但 EDPS 沒有向警監會解釋，「測試資料」的意思是「假」或「經處理」的資料。雖然 EDPS 聲稱資訊科技專業人員應該對「測試資料」一詞的理解沒有困難，但是他們沒有採取任何步驟，確保非資訊科技專業人員的 X 女士明白這個術語。

7.4.3 根據 Y 先生所述，EDPS 就資料保安而向他提供的指引，只限於一些要把客戶的資料保密的口頭指示。關於對客戶資料保密的責任，EDPS 聲稱他們與 Y 先生之間是有共識的，並已列於與 Y 先生簽訂的合約內。當公署要求 EDPS 提供該合約的副本時，EDPS 卻無法提供。本人並不相信 EDPS 有就處理警監會的資料向 Y 先生提供足夠的指引，亦不相信 EDPS 有就交還或銷毀資料(不論是否「測試資料」)而制定任何政策或程序。

對 Y 先生的評論

7.5.1 Y 先生應該知道警監會誤以爲他是 EDPS 的職員，而非獨立的分判商。但很明顯 Y 先生沒有採取任何行動，糾正這個錯誤印象。

7.5.2 正如 EDPS 的陳述一樣，Y 先生聲稱他只是向 X 女士要求「測試資料」，而「測試資料」一詞在資訊科技界是指不真實的資料。X 女士表示，她在讀取投訴警察課的電腦碟遇上困難時，會向 Y 先生求助。既然她在讀

取電腦碟方面有困難，便不能期望她在技術上能夠以提升了的投訴索引及統計系統格式，向 Y 先生提供「假」或「經處理」的資料。Y 先生或 EDPS 不能合理地期望，在沒有他們的指導或協助下，可以從 X 女士或警監會取得「假」或「經處理」的資料。由於 Y 先生是與一個非資訊科技專業人員接觸，一個較爲審慎的人應該會關注對方是否完全明白那個術語，以及是否需要加以解釋或討論，確保沒有誤解。

7.5.3 在整個調查中，本人對 Y 先生處理警監會資料的態度感到不安。首先，他從 X 女士或警監會收取電腦碟或資料後，沒有向警監會發出任何收據。其次，本人看不到 Y 先生有保存任何記錄，記載他從 X 女士或警監會收取電腦碟或資料。第三，本人看不到任何關於他把資料上載到公司伺服器的書面記錄。第四，Y 先生與 X 女士並沒有討論過電腦碟或資料在 Y 先生使用完之後的交還或銷毀事宜。第五，本人看不到任何有關 Y 先生銷毀電腦碟或資料的記錄。最後，Y 先生並沒有給予警監會任何告知或確認銷毀電腦碟或資料的書面通知。

7.5.4 儘管 EDPS 及 Y 先生聲稱他們視警監會的資料爲「測試資料」，但本人在聆聽所有證供及陳詞之後，並不相信 Y 先生是不知道警監會提供的資料屬於投訴警察課個案的真實資料。即使他真的不知道，但是他把資料儲存於連接互聯網的伺服器內，公眾人士得以進入，似乎是沒有採取任何步驟，保障資料(不論是否「測試資料」)免受未獲准許的或意外的查閱。明顯地，Y 先生沒有考慮過他把該些資料存放於該伺服器內的後果或效果。

對 X 女士及當時的上司的評論

7.6.1 警監會的書面記錄顯示，不熟悉資訊科技事宜及未受有關訓練的 X 女士，習慣向當時的上司及其他高級人員報告如何處理投訴警察課的資料；記錄亦顯示投訴警察課的真實資料曾多次交予 Y 先生。根據這些記錄及 X 女士經宣誓後的證供，本人相信她對於與 Y 先生接觸過程而作出的陳述。

7.6.2 根據警監會的一貫做法(見本報告第 5.2.2 段)，當時的上司是負責監督整體人員遵從條例的規定。作爲 X 女士的直屬上司，當時的上司聲稱，他並不知道 X 女士處理電腦項目外判的詳情，而他對這些項目及資訊科技系統的知識僅限於一些基本事項，本人對此感到非常驚訝。儘管多年來 X 女士已將項目的處理情況記錄存檔，並在會議上報告，當時的上司卻不知道項目的進度，本人對此作爲並不認同。此外，當時的上司沒有致力確保：

(i) 把電腦碟及資料交給 Y 先生或 EDPS 後，向他們索取收據；
(ii) 每次向 Y 先生或 EDPS 移轉資料均記錄存檔；
(iii) 向 Y 先生或 EDPS 發出書面指示，要求他們保障資料的保安，並爲資料保密；
(iv) 就電腦碟或資料在 Y 先生或 EDPS 使用完之後應否交還或銷毀而作出商討及適當考慮；
(v) Y 先生或 EDPS 必須在指定時間內交還或銷毀電腦碟或資料；
(vi) 如電腦碟或資料由 Y 先生或 EDPS 銷毀，在銷毀之後，Y 先生或 EDPS 即須提交確認書或報告，載列銷毀詳情。

當時的上司作爲 X 女士的直屬上司及警監會內負責個人資料事宜的人員，有關表現並不理想。

7.6.3 X 女士在警監會幾乎是單獨地處理這些電腦項目，沒有得到多少指導及監督。本人認爲造成問題的部分原因是在整個過程中，當時的上司及警監會管理層對 X 女士的監督不足，以及 X 女士在處理敏感的個人資料及在資訊科技知識兩方面都欠缺適當的培訓和支援。

對網站管理員的評論

7.7 網站管理員是由 Y 先生及 Y 先生的夥伴聘請，爲 Y 先生的公司建立支援該網站及電腦系統的伺服器。網站管理員相信資料外洩是因爲 Y 先生把警監會的機密資料上載到伺服器內一個公眾能夠查閱的位置。很明顯這是 Y 先生在事前不知道的。可以爭論的是，如果網站管理員曾提醒 Y 先生，把資料上載到伺服器內某些位置是很容易被公眾查閱的，那麼資料外洩或許得以避免。網站管理員沒有把如此重要的伺服器特點告知其用戶 Y 先生，本人對此表示關注。

第八章

警監會在資料外洩後採取的行動及專員作出的建議

警監會在資料外洩後採取的行動

8.1 在資料外洩之後，警監會採取了一些措施，其中包括：

(i) 主席於 2006 年 3 月 11 及 17 日公開向公眾道歉；
(ii) 設立電話熱線，回答公眾對事件的查詢；
(iii) 成立三個委員會，由主席及兩名副主席率領，接見關注事件的公眾人士；
(iv) 向受資料外洩影響的人士發出道歉信；
(v) 繼續與警方商業罪案調查科進行網絡巡邏，阻止外洩資料在互聯網上遭濫用；
(vi) 要求谷歌(Google)及其他搜尋器公司刪除儲存在快取記憶體的外洩資料，以阻止資料在互聯網上流傳；
(vii) 提升其電腦系統，以支援加強的保安功能；
(viii) 聘任一名全職的資訊科技人員，監控系統資料的保安及相關事宜；以及
(ix) 著手聘任獨立顧問爲電腦系統進行資訊科技保安的風險評估。

執行通知

8.2.1 依據條例第 50 條及因應本人的調查，如有關資料使用者被發現正在違反條例下的規定，或已違反條例下的規定，而違反情況令到違反行爲將持續或重複發生是相當可能的，則本人可向資料使用者送達執行通知，指示資料使用者採取特定的步驟，防止違反情況在日後重複發生。

8.2.2 雖然警監會已經採取上述補救措施，但本人認爲警監會違反保障資料第 4 原則的情況很可能會持續或重複發生。本人的意見是根據下述事實而作出的：對於員工處理外判承辦商或代理索取投訴資料的要求時需要考慮的事宜，警監會並沒有制定實際的政策或指引讓員工依從；如投訴資料必須發放予外判承辦商或代理，警監會亦沒有訂立必須採取的預防措施；也沒有措

施確保在外判安排中可能查閱該等資料的人士的良好操守、審慎態度及辦事能力。

8.2.3 本人在根據條例第 50 條行使權力時，亦考慮到事件對個人資料在互聯網上外洩的人士造成損害或困擾。因此，本人向警監會發出執行通知，指示他們：

(i) 制定所需政策及實務指引，規定與外判承辦商或代理接觸時，須妥善處理及保障投訴資料；
(ii) 實施有效的措施，確保員工遵從這些政策及指引；以及
(iii) 檢討現時的外判合約，盡量在合約中加入條款，訂明承辦商須採取的措施，保障警監會交給他們的投訴資料。

調查之後的建議

8.3.1 事件反映資料使用者及受託處理敏感個人資料的資訊科技從業員對保護個人資料的意識不足。機構把電腦系統的開發或維修外判，經常涉及將員工或顧客的個人資料移轉予外判承辦商或代理，這個慣常做法亦令本人關注。

8.3.2 這件不幸事件令人得知，如資料使用者必須向外判承辦商或代理發放載有個人資料的資料庫，採取預防措施是非常重要的。此外，我們需要付出更多的努力，提高資訊科技從業員及政府人員對保護個人資料的意識。

聘用外判承辦商或代理時須採取的措施

8.4.1 向外判承辦商或代理發放個人資料之前，應該先考慮以下各點：

(i) 個人資料的敏感程度和資料外洩可能引致的損害；
(ii) 向外判承辦商或代理查詢及商討可否改用「假」資料，了解使用「真實」個人資料的必要性；
(iii) 發放個人資料所涉及的風險；以及
(iv) 如承辦商或代理必須使用「真實」個人資料，在機構的處所內進行所需程序是否可行。

8.4.2　如決定必須向外判承辦商或代理發放「真實」個人資料，應該採取以下預防措施：

(i)　揀選信譽良好、能保證個人資料保安的承辦商或代理；
(ii)　在服務合約中加入下列條款：
　(a)　除了受聘進行的目的之外，承辦商或代理不得爲其他目的而使用或披露該等個人資料；
　(b)　列明承辦商或代理須採取的保安措施，保障他們收到的個人資料，以及承辦商或代理有責任遵從條例下的保障資料原則，保障該等個人資料；
　(c)　承辦商或代理不再需要該等個人資料進行受聘的目的時，須適時交還；
　(d)　絕對或有限制禁止把有關服務分判；
　(e)　承辦商或代理必須即時報告任何不尋常徵兆或保安違規情況；以及
　(f)　列明承辦商或代理必須採取的措施，以確保處理個人資料的員工會執行保安措施，並履行服務合約中有關處理個人資料的責任；
(iii)　不時審核承辦商或代理，以確定他們有否執行所需的保安措施及責任；
(iv)　爲交給承辦商或代理的所有個人資料保存適當的記錄；
(v)　就個人資料的使用、傳送、儲存及銷毀向承辦商或代理發出清晰的指示；以及
(vi)　向外判承辦商或代理發放載有個人資料的資料庫之前，先徵得機構高層的批准。

對資訊科技從業員的建議措施

8.5.1　爲了提高資訊科技從業員在工作中保障個人資料的意識，並爲他們提供指引，本人認爲有需要制定實際指引，概述資訊科技從業員的專業職責，並爲其他人士提供使用資訊科技系統(其系統載有個人資料或將會用作處理個人資料)的指引。公署與主要的資訊科技機構將會發出一份名爲「資訊科技從業員處理個人資料的建議程序」的指引。

8.5.2 指引建議資訊科技從業員在處理個人資料時採取下列措施：

(i) 列明各級資訊科技人員在保障個人資料方面的職責。例如：系統開發人員應確保個人資料不會用於系統診斷或錯誤追蹤，而資料庫管理人員應把所有在資料庫存取個人資料的應用程序記錄存檔；
(ii) 凡進出載有個人資料的資料庫、複製資料庫複本/備份，以及從資料庫輸出圖樣，都應獲得授權、受到監察及作出解釋，而有關這些資料庫運作的報告應定期編製及審查；
(iii) 每當終端用戶進入載有個人資料的資訊科技系統時，系統應發出顯眼的通知。除非獲得正式批准，否則資訊科技系統終端用戶不應由系統輸出或儲存任何個人資料；
(iv) 輸出個人資料應獲得授權。輸出的個人資料如儲存於可移動媒體，例如：軟磁碟、光碟、通用串列匯流排驅動器，應加上適當的標籤。載有個人資料的電腦列印複本應包含適當的標籤。載有個人資料的電子郵件內容應加密及加上適當的標籤；
(v) 銷毀不會再使用的個人資料。如個人資料存於個人電腦，電腦的硬碟應清除乾淨；如個人資料存於伺服器，伺服器的硬碟應清除乾淨；所有備份複本及印刷複本應予以銷毀，而銷毀記錄應適當地保存；以及
(vi) 在電子媒體建立、存取、修改及銷毀個人資料，應不時進行審核。

8.5.3 除了公布指引外，會舉行研討會，讓資訊科技從業員分享保障資料的良好行事方式及經驗；亦會呼籲本地所有高等教育機構把資料私隱加入資訊科技課程中。

對政府人員的指引

8.6.1 政府部門持有大量公眾人士的個人資料，本人特別關注他們處理個人資料的情況。本人建議所有政府部門在員工的定期培訓中加入有關條例規定的課題，並爲遵從條例規定而提供實務指引。

8.6.2 爲了進一步加強政府部門對保障資料的意識，公署與民政事務局正籌劃研討會，與政府人員討論如何遵從條例的規定。